COURSE TECHNOLOGY
CENGAGE Learning

EC-Council | Press

Network Defense
Perimeter Defense Mechanisms

This title maps to

EC-Council | Network Security Administrator

COURSE TECHNOLOGY
CENGAGE Learning™

Perimeter Defense Mechanisms
EC-Council | Press

Course Technology/Cengage Learning Staff:

Vice President, Career and Professional Editorial: Dave Garza

Director of Learning Solutions: Matthew Kane

Executive Editor: Stephen Helba

Managing Editor: Marah Bellegarde

Editorial Assistant: Meghan Orvis

Vice President, Career and Professional Marketing: Jennifer Ann Baker

Marketing Director: Deborah Yarnell

Marketing Manager: Erin Coffin

Marketing Coordinator: Shanna Gibbs

Production Director: Carolyn Miller

Production Manager: Andrew Crouth

Content Project Manager: Brooke Greenhouse

Senior Art Director: Jack Pendleton

EC-Council:

President | EC-Council: Sanjay Bavisi

Sr. Director US | EC-Council: Steven Graham

Library of Congress Control Number: 2010924350

ISBN-13: 978-1-4354-8357-6

ISBN-10: 1-4354-8357-X

Cengage Learning
5 Maxwell Drive
Clifton Park, NY 12065-2919
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at: **international.cengage.com/region**

Cengage Learning products are represented in Canada by Nelson Education, Ltd.

For more learning solutions, please visit our corporate website at **www.cengage.com**

NOTICE TO THE READER

Cengage Learning and EC-Council do not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Cengage Learning and EC-Council do not assume, and expressly disclaim, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. Cengage Learning and EC-Council make no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and Cengage Learning and EC-Council take no responsibility with respect to such material. Cengage Learning and EC-Council shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Printed in the United States of America
1 2 3 4 5 6 7 13 12 11 10

Chapter 1

Hardening Physical Security

Objectives

After completing this chapter, you should be able to:

- Understand the need for physical security
- Understand the factors that affect network security
- Recognize specific physical security threats
- Implement premises security
- Apply biometrics in physical security
- Implement workplace security
- Secure network devices
- Understand the challenges in ensuring physical security
- Implement physical security measures
- Develop a physical security checklist

Key Terms

Faraday cage a metallic enclosure or cage that prevents the entry or escape of an electromagnetic field by having a fine-mesh copper screening embedded into the walls or system container

Script kiddies unskilled hackers who generally use downloaded applications to break into systems

Introduction to Hardening Physical Security

In addition to securing the network from external software attacks, the physical security of assets must be ensured. The following parts of the network must be physically secure:

- Servers
- Workstations
- Devices that enable access to the network, such as routers, switches, bridges, and hubs
- Network wiring

- Access points
- Laptops
- IT financial assets and credentials

This chapter will familiarize you with physical security as well as the steps that need to be taken in order to increase that security.

Understanding the Need for Physical Security

There are many different physical attack threats to a network; however, most fall into one of the following three categories, based on the specific way in which the attack occurs:

1. Forced entry threats
2. Ballistic threats
3. Explosive blast threats

Each of the three categories covers specific types of attacks, such as sabotage and burglary. In many cases security can be completely compromised if physical access is achieved. Attackers can disable, reconfigure, replace, and/or steal systems with relative ease once physical security is breached.

Statistics

- According to the CSI/FBI Computer Crime Security Survey 2005, nearly 40% of victims fail to report computer intrusions.
- According to Nationwide Mutual Insurance, 16% of debit card attack victims bear the total cost, or a part of the cost, of fraudulent purchases up to $4,000.
- According to Nationwide Mutual Insurance, one-third of consumers report their online banking IDs becoming compromised. Hackers gained 21% of this compromised bank account information through the victims' homes, cars, mailboxes, trash, wallets, or other physical means.
- The Global State of Information Security 2005 survey revealed that 37% of those surveyed had an information security strategy and that 24% of respondents are still developing a process for securing their bank account information.

Internet Security

The network manager will follow different network policies depending upon whether the network is trusted, untrusted, or unknown.

Trusted Networks

Trusted networks are inside the network security perimeter, so every computer in the network is behind a common firewall. This also includes VPNs. Firewalls are arranged to specify the location where the network packets originated so a server can authenticate the location.

Untrusted Networks

These are external networks outside the security perimeter. They are not under the complete control of the network administrator or the security policies.

Unknown Networks

Unknown networks are networks that are neither trusted nor untrusted, because the firewall is not aware of them.

Physical Security Breach Incidents

Any breach of security is a serious concern. Physical security breaches are a serious offense under the law and there have been many incidents of people being prosecuted for such breaches, including the following:

- In 2001, Yasuo Takei, chairman of Japan's biggest consumer lender, Takefuji, was arrested on charges of wiretapping. Metropolitan Police Department investigators suspected Takei of ordering former Takefuji

official Kazuhiro Nakagawa to wiretap a journalist and others to protect his son. In addition, Nakagawa confessed to police that he had also wiretapped the communications of a former branch head of the company.

- In 2003, a laptop containing the names, addresses, and Social Security numbers of approximately 43,000 customers was stolen from the principal data-processing provider of Bank Rhode Island, Fiserv.
- On December 15, 2003, Jesus C. Diaz, who once worked as an AS/400 programmer for Hellmann Worldwide Logistics, was sentenced to a one-year imprisonment for accessing the company's computer system remotely and deleting critical OS/400 applications. Diaz caused more than $80,000 in damage. As a result of his actions, Hellmann Worldwide Logistics' AS/400 systems were down for 48 hours.

Who Is Accountable for Physical Security?

Each employee is responsible for the systems that he or she handles. To strengthen the physical security of a company, the following personnel should be made accountable for physical and information security:

- The physical location's security officer
  - Responsible for any physical security breach
  - Responsible for educating the rest of the employees and guards on duty
  - Responsible for manually checking the firm's physical security periodically
- Safety officer
  - Responsible for fire protection
  - Responsible for educating employees and other staff on safety
- Information systems analyst or security administrator
  - Looks into network security and related issues
- Chief information officer
  - Heads the committee that frames security policies

Understanding the Factors That Affect Network Security

Vandalism

Disgruntled or former employees may try to compromise the system. Also, in any case where a disaster causes panic, systems may be mishandled.

Theft

Lack of proper security may result in equipment theft. A guard on the premises can help prevent this.

Natural Factors

Earthquakes

Even minor earthquakes may cause dust and debris to fall on computer equipment. Plastic sheets should be readily available in the system room. Covering computing assets in an emergency may mitigate damage. Magnetic tapes should be covered to prevent wear and tear. Operators should be trained on how to properly cover the equipment.

Fire and Smoke

Fire alarms and extinguishers should be placed well within the reach of employees, and they should be checked regularly to ensure proper functioning. Smoke detectors should be placed throughout the building. The designated smoking area should be as far as possible from computer systems.

Flood

Periodic inspections under the floors must be conducted to check for water seepage, especially during times of heavy precipitation. Water detectors must also be checked periodically. Administrators should be aware of proper shutdown procedures, and exercise drills must be performed regularly.

Lightning and Thunder

All computer systems should have a UPS (uninterruptible power supply) so that voltage fluctuations, sudden power surges, and outages will not affect them. These incidents can cause significant damage to computer hardware, particularly the memory.

Dust

Dust that naturally accumulates on hardware hinders its performance. Dust can seriously hinder a PC's ability to cool down. Even if the computer's case has never been opened, dust can still get in through the drive openings. An effective way to remove dust from the inside of a CPU is with compressed air, which can be used to blow dust away from the motherboard and other components.

Water

PCs should not be placed near water sources or near windows. PCs should be placed in an environment where humidity is controlled.

Explosion

Chemicals should be isolated and kept away from computers.

Types of Attackers

While attackers differ in their intentions and procedures, their common aim is to identify technical flaws in security policies and take advantage of them.

The Explorer

Purely out of curiosity, the explorer exploits security vulnerabilities and ends up breaking security policies. He or she browses through all sites, simply exploring and trying to figure out how things work. He or she tries to crack passwords, as well as alter or delete file settings and network configurations, but does not have any intention to cause real harm.

The Discontented Worker

Ex-employees and current, dissatisfied employees can attempt to harm the company's resources. They can effectively attack the integrity, privacy, and accessibility of assets. Because they are familiar with the weaknesses of the security policies and the location of confidential information, they try to damage and dismantle assets with knowledge of the best places to attack.

The Spy

Spies could be from intelligence agencies that attempt to obtain critical and confidential information. They could also be from rival companies, committing crimes for financial gain and reputation.

The Terrorist

Terrorists use the Internet to carry out their plans. Terrorists might use information that isn't critical to a company and is less secured.

The Thief

Thieves' primary concern is monetary gain. They try to acquire credit card information and reroute money offshore. They will often use social engineering to accomplish their goals.

The Hacktivist

Hacktivists protest governments and try to destroy public assets. Examples of hacktivist activities include:

- DDoS attacks
- Web page defacements of government sites
- Antiglobalization protests

The Script Kiddies

Unskilled hackers known as ***script kiddies*** use downloaded scripts and other automated attack tools to break into sites. They are often ignorant of what happens when they have access to sites and assets. Some hackers hire these script kiddies to perform DDoS attacks and to compromise the computers on a network.

Hacker for Hire

There are two types of hackers for hire:

- The sneaker, also known as an ethical hacker, attempts to determine vulnerabilities and alert the owners of those vulnerabilities before any damage can be done.
- Mercenary hackers exploit the vulnerabilities of a company's Web site and sell the information to the highest bidder.

The Competition

Competition between companies can lead to corporate espionage, in which one company spies on another or sabotages its computer systems.

Enemy Countries

Rival countries regularly attack each others' information security.

Physical Security Threats to Networks

Threat is defined as any event that can cause damage to an asset. The purpose of physical security is to ensure the confidentiality, integrity, and availability of assets, including the safety of all personnel.

Physical security is perhaps the most overlooked aspect of security. Generally, threats to physical security are categorized into the following types:

- Natural/environmental
- Human-made
- Supply system
- Political events

Natural/Environmental

This type of threat includes the results of naturally occurring events, including:

- Flood
- Fire
- Earthquakes

Flood

Floods commonly occur due to heavy rains or the melting of ice. This increases the level of water beyond the carrying capacity of a nearby river, resulting in a flood. Some types of floods increase slowly, taking days to pose a threat. On the other hand, flash floods come quickly without any sign of rain. In addition to water, this can cause rocks and mud to enter the area.

Earthquakes, mass movements above or below water, volcanic eruptions and other underwater explosions, landslides, large meteorite impacts, and weapons testing at sea all have the potential to generate a tsunami.

Preventive Measures The following preventive measures can help guard against flood damage on a global scale (though carefully choosing the site location is often the best solution):

- Constructing flood control dams
- Building dikes and levees beside rivers to prevent them from overflowing
- Building canals to leave room for extra water
- Regulating flood plain development and urbanization

- Preventing soil from eroding
- Planting many trees, treating slopes, and building reservoirs to catch sediment and debris
- Diverting rivers and streams away from populated areas

Fire

Computers can be secured against fire threats by ensuring that there is good fire extinguishing equipment nearby and that personnel are trained to use it. A full sprinkler system should be installed in the building. The wiring should be protected, in addition to the computers. The organization should install smoke detectors and sprinkler heads that are appropriately positioned to cover wires and wiring closets.

Earthquakes

Personnel should pay careful attention to the location of shelves and bookcases. They should avoid placing computers on high surfaces or near windows and avoid placing heavy objects on shelves near computers where they may fall onto the equipment. Computers should be placed on strong tables. Also, those involved in physical security concerns should consider physically attaching computers to surfaces.

Human-Made Threats

The biggest threat to the physical components of an organization and its network are from human-made errors, be they intentional or unintentional. Human error includes hitting the wrong button, unplugging the wrong cord, and so on.

Terrorism

Terrorist activities include the following:

- Assassinations
- Bombings
- Random killings
- Hijackings

War

Wars destroy the major buildings, industries, and infrastructures of a particular country. Pollution can spread due to bombs and expelled gases. War also changes the economic conditions of many countries.

Dumpster Diving

Dumpster diving involves searching the garbage of the targeted company in order to acquire important information. Attackers search for information such as phone numbers, credit card numbers, and other information commonly thrown away. Discarded storage media such as floppy disks, CDs, and tapes can also be used to obtain important information.

To prevent losses from dumpster diving, an organization should consider these countermeasures:

- Create a well-defined policy to handle important security-related information. This policy states how to deal with sensitive information, including how to store, delete, and edit the information. All employees must be trained in this policy.
- A strong magnet can be used to completely delete the data on magnetic storage devices, such as floppy disks, tapes, and hard drives.
- Documents containing confidential information must be shredded when they are no longer needed. Dumpsters should be locked and well lit to ensure that no unauthorized person tries to access them.
- Secure network configuration files from unauthorized access by keeping track of equipment information.
- Avoid sticking notes on monitors, routers, and network devices. Notes containing router information and locations of systems and devices provide an easy map to an attacker.
- Printouts of user logs must be shredded.
- All systems should be password protected.

Political Events

Bombings, strikes, terrorism, riots, espionage, wars, and so on can affect the security of an organization and its normal operations. This falls under the basic need to avoid allowing physical access by any unauthorized persons.

Detecting Physical Hazards

A safety program always starts with hazard detection, which involves the deliberate search and identification of unsafe conditions in a work place. This requires a good knowledge of acceptable standards, codes, regulations, and safe work practices.

Hazard detection involves the following:

- Physical inspection
- Accident investigation
- Accident analysis

Physical Inspection

A physical inspection can be formal or informal. Regular inspections help personnel detect unsafe conditions.

Accident Investigation

Once an accident occurs, it must be investigated based on all facts, statements, opinions, and related information. This includes recommending corrective actions to prevent the accident from reoccurring.

Accident Analysis

An accident analysis is a collection of data taken from different accident information. If an accident is reported and investigated, the information from the investigation is included in this analysis to detect unsafe conditions and hazards.

Workplace Security

Employees manage and store the confidential information on desktops, laptops, and portable storage devices for both their office and home facilities. Facility managers must be equipped to determine who has entered the premises, as well as what information they have accessed. These managers should use technologies such as smart cards, encryption keys, digital signatures, and biometrics in preventing unauthorized access.

Implementing Premises Security

The premises are the physical area where computer hardware is located. The premises range from a limited space to a complete building. The location of the computers has to be decided after considering various conditions and security issues. The amount of hardware being used determines the space needed for the equipment. The cost and sensitivity of the devices are also considered when deciding on the location of the hardware.

Security Considerations

- When necessary services are unavailable, the flow of business operations is negatively affected.
- Sudden damages to physical assets endanger business functions.
- Unauthorized access to systems leads to theft and damage of resources.
- Fire, floods, and failure of air conditioners can lead to damage of physical resources.
- Unauthorized visitors can access and corrupt unsecured information.

Office Security

Some unsecured places where office information can be found are workstations, work areas, dustbins, and monitors. If an attacker can access such work areas in an office, he or she can gain information about

passwords, user accounts, physical devices, and other security features. Locations vulnerable to displaying secure information include the following:

- Employees might fix sticky notes with password or account details to the computer monitor.
- Employees might leave sensitive information in desks, drawers, display boards, notebooks, and recycle bins next to printers, phones, or fax machines.
- Attackers may easily guess the system ID from the user ID and password.
- If an attacker gains access to a notebook with a list of passwords or user IDs, he or she can often guess the rest.
- If the list of telephone numbers is available to the hacker, he or she can gain information through social engineering.
- If the attacker knows the security policies adopted by the organization, he or she can more easily hide applications from the organization's security tools.
- From memos, the attacker can obtain network configurations, services, access privileges, etc.
- The attacker can obtain the internal manuals of the organization that explain the operations of different departments, which can show the hacker potential vulnerabilities.
- The attacker can determine the best time to attack if the calendar of events is accessible.

Reception Area

In the reception area, outsiders entering the company must be observed. If they are strangers, their behavior should be recorded. Their intensions have to be noted. Extra attention should be paid to the following:

- Solicitors
- Charity organizations
- Ex-employees
- Movers

Smart Cards

A smart card is a credit card–sized plastic device that contains a computer chip and memory. It can store, process, and output data securely. Smart cards commonly store cryptographic keys, digital certificates, identification credentials, and other information. They provide strong two-factor authentication using a PIN.

The International Organization for Standardization (ISO) uses the term *integrated circuit card* (ICC) instead of *smart card*.

Benefits of Smart Cards

There are many benefits of smart cards, including the following:

- Lower administrative costs
- Reduced losses and liabilities
- Increased convenience
- Provides additional functionality, such as credential storage
- Provides strong two-factor authentication, with the possibility of a third, by using a fingerprint reader on the smart card itself
- Uses public-key cryptography without storing the key on a computer
- Can store multiple passwords
- Can be used anywhere inside or outside the building

Smart Card Uses

One of the important factors behind smart card use is the fact that multiple applications are involved in the use of a smart card. A smart card provides portable secure storage for digital certificates. The smart card can also be used for many applications, such as the following:

- Logon/logoff authentication to an operating system
- Authentication to a Web site

- Sending/receiving e-mail
- Encryption of data files

Types of Smart Cards

There are three types of smart cards:

- Stored-value cards
- Cryptographic coprocessor cards
- Optical-memory cards

Stored-Value Cards (SVCs) The stored-value card is the most common and least expensive of the smart cards. It stores data much like a magstripe card.

Cryptographic Coprocessor Cards Cryptographic coprocessor cards, or crypto cards, have specialized processors on board with specific support for cryptographic operations, such as digital signing and encryption.

Optical-Memory Cards An optical-memory card is a plastic card that stores information using lasers. These cards look somewhat like a credit card with a piece of a CD-ROM glued on top of the card. Because information is actually burned into the material during the write cycle, the medium is a write-once read-many (WORM) medium, and the data are nonvolatile (not lost when power is removed).

Smart Card Components

Every manufacturer of smart cards has its own international design and proprietary systems. Nearly all smart cards have the same components. These common components include a CPU, memory, and an interface pad. The CPU is the brain of the smart card, much like the CPU of a PC. It contains the interface pads that provide access to the smart card. The smart card memory is in different forms based on the design. It uses random access memory (RAM), read-only memory (ROM), and electrically erasable programmable read-only memory (EEPROM), which is read and write capable.

Contact and Contactless Cards

Contact cards have an electric contact on the card, while contactless cards use wireless technology to communicate. The distance covered by a contactless card can range from a few inches to a few meters, to enable the transmission of data or commands. Contactless cards generally have an onboard battery, and both reader and card have an internal antenna for secure communication.

Smart Card Operating Systems

Because a smart card is a small computer, it has an onboard operating system designed to manage microprocessor tasks. These tasks include the following:

- Data transmission over the serial terminal interface
- Loading, operating, and managing applications
- Execution control and instruction processing
- Protected access to data
- Memory management
- File management
- Cryptographic algorithm execution

Three common and basic operating systems are found on smart cards:

- JavaCard operating system is developed by Sun Microsystems and promoted via the JavaCard forum. It is used for Java-based smart cards.
- MULTOS is a smart card operating system developed by a consortium led by MasterCard and Mondex. It is a multiapplication smart card operating system designed with high security for financial transactions.
- Windows for Smart Cards is a smart card operating system developed by Microsoft and designed for multiple applications.

Proximity Cards or RFID Cards

Several companies are using proximity cards to control physical access. These proximity or RFID cards contain an internal antenna. When using this card, the employee holds his or her card within a few inches of the reader. The card reader receives a unique ID string from the card and transmits it to the central computer, which then tells the reader whether or not to open the door.

Combi Proximity Cards

These cards integrate photo ID, proximity, magnetic stripe, and even smart card technology into a single card, so multiple cards for each function are not needed.

Hybrid Smart Cards

A hybrid smart card has two chips embedded into the card's surface—one contact and one contactless—each with its own interface.

Combi Smart Cards

Combi smart cards allow a single smart chip to securely interface with both contact and contactless readers.

Applying Biometrics in Physical Security

In information technology, biometrics is the measurement and analysis of human fingerprints, irises, retinas, voices, faces, and hands. These measurements and their associated analyses are used in the process of authenticating individuals.

The implementation of biometrics can increase the overall security of an organization by removing reliance on passwords and the use of tokens that could be lost or shared. It also increases convenience, because users do not need to remember passwords or keep track of access cards.

Biometric Process

There are two different parts of the biometric process, integrated into the same device and system. One of these parts is the biometric enrollment process, and the other is the biometric verification process. The following steps occur during the enrollment process:

1. The user provides the required nonbiometric data. This may include full name, address, account information, username, and password.
2. The user presents the raw biometric data. This may be through a scanning device, a camera, a microphone, or whatever acquisition device the biometric system is using.
3. The biometric device captures an image of the biometric data.
4. The biometric system processes the raw data and creates an enrollment template.
5. The enrollment template is stored with the required nonbiometric data for this user's account.

Once the user is registered in the system, the following steps can be taken to verify the identity of the user:

1. The user presents the raw biometric data.
2. The biometric device captures the biometric data.
3. The biometric system processes the raw data and creates a verification template.
4. The verification template is matched against the enrollment template.
5. The biometric system scores the degree of similarity between the enrollment and verification templates.
6. The biometric system checks to see if the score is above or below a defined threshold.
7. If the score is above the threshold, a match decision is made. If the score is below, a nonmatch decision is made.

Accuracy of Biometrics

Accuracy of biometrics concerns the following three primary issues:

1. False match rate (FMR)

2. False nonmatch rate (FNMR)
3. Failure to enroll (FTE)

False Match Rate (FMR)

This is the chance that the biometric scanner will falsely identify an unauthorized user as another, valid user.

False Nonmatch Rate (FNMR)

This is the chance that the user's credentials provided at the time of authentication fail to match the data stored in the system. This is usually caused by the system having a greater detail of information than what is actually provided by the user.

Failure to Enroll (FTE)

There is a chance that a user cannot enroll his or her biometric details into the system. There are several reasons for this, including an injured finger in fingerprint biometrics, a cataract in retinal scanning, and a sore throat in voice recognition.

Biometrics Applications

The following are the some applications of biometrics:

- PC or network access
- Physical access
- Retail or ATM
- Criminal identification
- Citizen identification programs
- E-commerce

Fingerprint Scanning

This is a popular technology related to biometrics. Many people associate the biometric technology of fingerprint scanning with that of the criminal fingerprint identification system, which can make them hesitant to enroll.

In the criminal fingerprint system, the entire fingerprint image is obtained and stored in a database and is printed when it is required. Biometric fingerprint scanning systems do not store a full image of a fingerprint in a database. Only a small template created from the fingerprint is stored. Fingerprint scanning devices can either be standalone devices or built into laptops, keyboards, or mice.

Fingerprint Scanning Method

Fingerprint scanners are of two types: optical and capacitance. Optical scanners use a charged coupled device (CCD), which is the same as the light sensor used in some digital cameras and camcorders. CCD uses an array of specialized light-sensitive diodes called a *photosite*. When the scanner detects a finger, the CCD camera takes the picture.

A capacitance scanner is also used to capture an image of a fingerprint. But this scanner, instead of using light and a camera, uses electrical current to generate an image. This scanner contains tiny cells that house conductor plates. Each plate is smaller than the width of the single ridge of a fingerprint.

Hand Geometry

Hand geometry is a biometric technique used to identify a user by the shape of his or her hand. It is a simple and accurate procedure. The use of this technique requires special hardware and can integrate into any system or device.

Hand Geometric Process

The user places his or her hand on a metal surface. The device then verifies the user details in its database. This process takes less than 5 seconds.

Voice Scanning

Scanning the human voice is one of the most common biometric technologies. This system uses voice recognition software to allow a user to interact with a computer by issuing commands verbally instead of using an input device such as a mouse.

Voice Scanning Process

The voice scanning process is similar to other biometric technology. In this system, the raw biometric data is the sound waves produced by voice. This raw data is captured by different devices specifically made for voice scanning. The sound waves are converted from analog to digital early in the process. A microphone, landline telephone, cellular telephone, or any other device that can capture the human voice is suitable.

Retinal Scanning

Even identical twins have different retinal patterns. The retina is a thin layer of nerves (about 0.5 mm thick) found on the back of the eye. The retina transmits impulses through the optic nerves to the brain.

Retinal scanning is difficult compared to other scanning in biometric technology. To present raw biometric data, users must move their head into position, with their eye very close (within an inch) to the scanner for it to read the retina through the pupil. During the scan process, the user focuses on a light in the scanner. After generating the template, this technique provides excellent matching.

Iris Scanning

As with the retina, even twins also have different iris patterns. Some iris features include ligaments, furrows, striations, ridges, and zigzags. Iris scanning technology measures 247 independent variables in an iris. One of the most important applications of iris scanning is its use in bank ATMs for authentication.

Similar to fingerprint scanning, it also requires a device to capture the image and software to process the image. A camera uses infrared light to capture a high-resolution image. After capturing the image, the system locates the border between the pupil and the iris, which can be difficult for users with very dark irises. After noting the border, the system will convert the data to a grayscale image. The grayscale image is used to identify the unique features of the iris.

One example of an iris scanner is the Panasonic DT120, shown in Figure 1-1.

Facial Scanning

Facial scanning or facial recognition is well known due to large-scale surveillance implementations. It works by picking out the unique characteristics of a human face and matching them against facial images in a database.

A facial scanning system looks at the following facial characteristics:

- Size of eyes
- Distance between the eyes

Source: http://www.eyenetwatch.com/iris/panasonic-authenticam.htm. Accessed 2004.

Figure 1-1 The Panasonic DT120 is a small iris scanner for desktop computers.

- Depth of the eye sockets
- Location of the nose
- Size of the nose
- Location of the chin
- Size of the chin
- Jaw line
- Size, position, and shape of the cheekbones

Facial Scanning Process

The facial scanning process starts with the acquisition of the raw biometric data: an image of a human face. This image can be acquired using any imaging source. The image should be of as high resolution as possible.

Once the system identifies the face, it will narrow in on the face and then record the image. After that, the image is scaled and rotated in order to align it with the processing software. The system will remove all extra data from the image such as hair, background images, and head so that the system can isolate only the face in the image.

After capturing the isolated facial image, the system will create a face print of that image. The face print is the template for the system.

Implementing Workplace Security

It is common for both large and small companies to have areas where the majority of employees use computers at work. Sometimes, each of these employees has a cubicle for an office. Employees may like to personalize their workstations as well as their PCs, but they need to be educated on how to secure this personal space. People sometimes scribble their passwords, personal information, IP addresses, or telephone numbers on whiteboards, sticky notes, pads, or pieces of paper. This should be discouraged, since attackers can easily obtain this information, as well as critical information regarding the LAN and the company, by going through dumpsters or through other means. Address books, company policies, reminders, user IDs, etc., should be kept away from the reach of others.

The workstation can be physically secured in the following ways:

- CCTV cameras with monitored screens and video recorders can be used to monitor the movements of employees and visitors.
- Unmanned/unattended terminal screens should be locked to prevent unauthorized access.
- Workstation cubicles should be designed in such a way that employees cannot see each other's terminal screens.
- PCs should be locked down to prevent any physical movement.
- Removable media drives should be avoided as much as possible. Only one workstation per row should have such drives, and that particular workstation should not be used for any other purpose.

Desktop Security

Managing desktop security includes people, processes, and technology factors.

People

Education and Awareness Users must be reminded of ways to avoid vulnerabilities. Threats faced by desktop users include:

- Programs that send clear (unencrypted) passwords
- Social-engineering attacks
- Virus attacks
- Unsolicited e-mail attachments
- Unattended desktops

- Packet sniffing
- Bad desktop management with no antivirus software, outdated virus signatures, and/or no backups

Some examples of education and awareness programs include:

- Regular seminars and road shows of security awareness
- Placing weekly posters on a bulletin board

Enforcement Security policies must be efficiently managed. Certain evidences must be present to properly claim a violation of policies, such as producing audit trails. If there is a serious security breach, efficient action must be taken with legal support.

Processes

Strict adherence to the following processes set by the organization is essential to ensure desktop security:

- *IT security council*: The IT security council enables and designs the security policies and regularly checks the security process.
- *Policies*: Policies must be in place for things such as designing controls of application systems, developing user access controls, performing risk analysis, and conducting computer crime investigations.
- *Baselines*: These make sure systems are configured to security standards.
- *Procedures*: This is a detailed structure of the processes that go into completing a task.
- *User classification*: Dividing the users into different groups based on security needs allows administrators to have finer control and to manage user security in a more convenient and efficient way.
- *Reviews*: Security audits must be performed frequently by arranging seminars and reviews, so the user can correct errors before they are exploited.
- *Penetration testing*: Desktop security should be tested through penetration testing that involves various hacking techniques.

Technology

The technologies involved in managing desktop security include:

- *Centralized management*: Client applications are not installed on the desktop. The user will be provided with only the data available on the desktop.
- *Password protection*: Passwords must be designed to be difficult to guess.
- *Single sign-on*: When an application contains multiple security features, there is a possibility that many passwords are available for a single user. This should be eliminated.
- *Desktop lock*: An attacker can view confidential files on an unlocked machine. A user should not leave the desktop unattended without locking it first.
- *Virus detection*: Antivirus software must be installed and regularly updated.
- *File encryption*: Encryption causes files to be inaccessible to unauthorized persons.
- *Personal firewall*: A firewall installed on a desktop PC increases security.

Laptop Security

According to a survey conducted by the FBI in 2004, medium- and large-sized companies lose an average of 11.65 notebook computers a year by theft. If a laptop is lost, an organization should ask the following questions:

- What information of a strategic nature would be disclosed?
- What information of a tactical nature would be disclosed?
- What information about the company's network or computing infrastructure would be revealed that would facilitate an electronic attack?

Laptop Security Measures

The following are some common laptop security measures:

- Encrypt sensitive data
- Back up everything on the laptop
- Trace the stolen laptop's location, if possible
- Set a BIOS password on the laptop
- Consider laptop PC insurance
- Add third-party privacy protection for highly sensitive data
- Use physical Kensington locks
- Use strong hardware-based security

Laptop Lockers

Laptops can be secured with physical devices when they are stationary. This includes steel cable locks and tie-down bracelets.

Portable Laptop Carts

Portable laptop carts provide mobility in school classrooms. It is easy to move the carts from classroom to classroom. Electrical units allow notebooks to be recharged while in the carts. The carts can be closed and locked to prevent unauthorized access to the laptops.

Antitheft Tags

Antitheft tags affixed to laptops assist authorities in tracing stolen laptops found anywhere in the world.

Tracking and Recovery Systems

Lost or stolen laptops can be recovered through a variety of tracking and recovery techniques.

XTool Computer Tracker XTool Computer Tracker offers portability and traceability. A software-based transmitter sends a signal to the Signal Control Center by means of a telephone or an Internet connection. This signal can track the location of the stolen piece of equipment. The signal enables the user to reboot the system when it starts and when the IP address changes. The user also has the ability to delete files remotely, even if the system is mobilized. Every signal holds the telephone number or the IP address that is used by the transmitted signal.

XTool Computer Tracker's features include the following:

- Supports Windows and Macintosh platforms
- Undetectable, even by some antivirus programs
- Can be upgraded or downgraded as needed without affecting the computer's security
- Adaptable to new environments or configurations
- Worldwide monitoring and recovery services

zTrace Gold zTrace Gold is an invisible software security application that traces the location of missing laptops. It is undetectable and cannot be erased. The computer completes a handshake with the zServer at every Internet connection. If the laptop is reported missing, the zTrace Recovery Team identifies the computer's exact physical location. The team then coordinates with local law enforcement for a completely outsourced recovery solution. For enterprises, zTrace Gold can be managed internally by an organization's own internal security department or outsourced to the zTrace Recovery Team.

CyberAngel Using its secure password entry system, the CyberAngel Windows software will alert registered users of any unauthorized access to that protected computer and lock the communication ports to prevent unauthorized users from accessing any outside networks. CyberAngel will also lock the sensitive data stored on that computer with some of the strongest encryption algorithms currently available. Protected files will be rendered invisible to the unauthorized user. When the client notifies the Security Monitoring Center that a registered

computer has been stolen, the center can then locate the computer when it next reports an unauthorized access to the Security Monitoring Center.

ComputracePlus ComputracePlus provides detailed tracking reports for any computer with an Internet connection.

Securing Network Devices

Server Security

The server is the most important component of any network, so it should be given a higher level of security. The server room should be well lit. A high-end configuration should be used for servers so that they can sustain the load caused by continuous uptime.

The server can be secured using the following means:

- Servers should not be used to perform day-to-day activities.
- Servers should be enclosed and locked to prevent any physical movement.
- Booting from floppy and CD-ROM drives on the server should be disabled and, if possible, these drives should not even be on the server.
- Some system administrators have a habit of labeling the server and other systems in the server room. These labels sometimes have the operating system's name and the server hardware specifications written on them. This is not advised, because anyone who passes through the server room can get details about the server and other devices. If an attacker sees this information, he or she does not have to go through the process of footprinting.
- Unnecessary services and subsystems should be removed.
- Server software should be updated regularly.

Securing Backup Devices

When securing a network, data integrity is sometimes overlooked. It is important to maintain data integrity in systems and backups, which is the best defense against natural disasters, viruses, and hackers.

Physical Access to the Boot CD-ROM and Floppy Drives

Physical access to a floppy drive or a CD-ROM on a domain controller or member server invites intrusion during the booting processes. Malicious users can use boot disks to completely delete data or even gain system access. The intruder can access the system and abort installation processes from the MS-DOS prompt.

Removable Media

People use removable media in the workplace to store and move corporate information. Documents, databases, graphics, music, and video can be moved between computers using removable media, which are highly portable; thus, the security implications and risks of removable media need to be seriously assessed. Many high-security organizations like the military will prohibit the use or possession of removable media at their secure sites, often removing the availability of USB ports, floppy drives, and DVD/CD devices.

Fax

It is important to apply great care when accepting a fax as genuine because its integrity is questionable; there is no data validation or authentication between sender and receiver. Every fax machine can use the Calling Station Identifier (CSID) if required, while some software can check the names of CSID during the transmission. Faxes should not be used for secret information.

Personnel Security Practices and Procedures

The following procedures are involved in personnel security:

- A screening process is established to determine an employee's background. The background check includes criminal and financial screening. Education, past experience, and other qualifications are verified during screening.

- An employee access card is used to allow authorized persons into the office.
- An employee should complete access agreements before accessing any system. They may include confidentiality/nondisclosure agreements, acceptable-use agreements, user rules of behavior, and conflict-of-interest agreements.
- A formal sanction process has to be planned for personnel failing to act in accordance with established information security policies and procedures. The process should be in agreement with related federal laws, directives, policies, regulations, standards, and guidance.
- IT personnel security requirements for third-party providers should be established. Third-party providers include the following:
  - Service bureaus
  - Contractors
  - Information technology services
  - Outsourced applications
  - Network and security management

Position Sensitivity

Before a person is given a sensitive position, a security investigation is performed and then the person is granted the applicable clearance level. The following are the appropriate codes for position sensitivity names:

- Nonsensitive
- Noncritical sensitive
- Critical sensitive
- Special sensitive
- Moderate risk
- High risk

Employee Clearance

The following are the steps to relieve an employee of his or her responsibilities:

- An employee has to submit a resignation or retirement letter to the department head with a copy to the HR (Human Resources) Department. The department head will forward that resignation letter to the central leave coordinator.
- After receiving the resignation letter from an employee, the department head will set the last working date of that employee.
- The employee should fill out the clearance form and also have a meeting with the central leave coordinator from the HR Department to provide a plan for the last working days.
- After having a chat with that employee, the HR department will send a notice to obtain clearance from all the departments specified in the clearance form.
- After receiving the notice from the HR Department, all departments will send the due certificates to the central leave coordinator.
- The employee should contact the central leave coordinator during the last day in order to complete the clearance process.
- After verifying all the clearance certificates from all the departments, the central leave coordinator will clear the employee through a clearance form.
- After getting all the clearance certificates, the central leave coordinator will provide the employee with the following forms:
  - W-2 change of address form
  - Insurance form
  - Exit interview form (optional)
- The central leave coordinator will sign the clearance form, which depends on the clearance certificates from all the departments.

Access Authorization

Access authorization allows an employee to enter the office only with the appropriate access card. This is meant to protect important data and the entire building from unauthorized physical access. It also protects the equipment from unauthorized physical access, tampering, and theft. The employee must give his or her access card back to the head of the department or to HR when leaving.

The following are the advantages of access authorization:

- Does not allow access to unauthorized persons
- Provides details about employees who have entered the office
- Prevents data loss from physical access

Systems Maintenance Personnel

System maintenance requires both physical and logical access to the system. There are too many systems that have maintenance accounts. Companies preconfigure these accounts with specific and widely known passwords. The most common method hackers use to break into systems is through maintenance accounts that contain guessable passwords. IT personnel should change the password frequently and deactivate unused accounts. The developed procedure should allow only authorized maintenance personnel to access those accounts.

A maintenance manual assists in defining the characteristics and responsibilities of system maintenance personnel. It also provides maintenance personnel with the information required to do their job. The administrator should monitor the maintenance personnel.

Support and operations include the following:

- User support
- Software support
- Configuration management
- Backups
- Media controls
- Documentation
- Maintenance

Maintenance includes the following:

- Managing time settings with automatic update, time zone, and daylight saving time
- Managing backup frequency, personal computer settings, and office safe settings
- Managing feature keys to provide other capabilities
- Providing tools to exhibit network diagnostic and advanced troubleshooting tools
- Giving directions to update systems
- Restarting with the following options:
  - Normal restart
  - Restart with factory defaults restored
  - Restart in safe mode

Contractors

Contractors should have an office identity card with photo and personal details, perhaps with a defined period of validity. All contractors should carry their ID cards at all times. Contractors must exhibit their ID cards clearly to the security officer. Contractors should return their ID cards when they are terminated or when they resign.

CCTV (Closed-Circuit Televisions)

CCTV cameras help analyze the events of the day, in case something suspicious happens. They provide real-time monitoring of the premises. Simply having them present and displayed can act as a deterrent. The only drawback of these cameras is that their usefulness depends on the personnel monitoring them.

Parking Area

The parking should be safe and secure. It should be surrounded by a boundary of some sort and should be guarded.

EPS (Electronic Physical Security)

EPS (electronic physical security) is the integrated application of a number of electronic security systems. This includes the following:

- Addressable fire detection systems
- Automatic gas suppression systems
- CCTV systems
- RFID, biometric, and smart card access control systems
- Intrusion detection systems
- Law enforcement systems and products
- Guarding equipment and a guarding plan

Understanding the Challenges in Ensuring Physical Security

Enforcing Physical Security Policy

Practical problems, such as inconveniences caused by the implementation of physical security policies, may raise security threats.

Social-Engineering Attempts

Social-engineering tricks may be attempted to trick personnel into divulging sensitive information. Such knowledge may prompt attackers to find ways to compromise security systems. Management should provide enough training to employees to make them aware of social-engineering attempts.

Restrictions for Sharing Experience and Knowledge

Access control policies may restrict personnel in one department from sharing their experiences and knowledge with other departments. Physical security ensures data security but may also restrict knowledge and experience sharing.

Cost and Time

Installing a physical security department in a company takes both time and money. Costs are incurred in the form of salaries, system installations, training, and more. Management can also outsource security functions to a firm that specializes in this area.

Sophisticated Technologies

Physical security personnel often counter problems with sophisticated technologies. Visitors may carry a spy camera with them to take pictures of the target company, voice recorders for eavesdropping, etc. Security personnel should be trained regularly on these technologies.

Physical Security Measures

Fences

Fences can be used as a deterrent. A high-security installation must contain two fences—an outer and inner fence, each between 15 and 30 feet high.

Guards

Guards can determine what action to take in each circumstance as it comes along and to make logical responses. Most guards have definite standard operating procedures (SOPs) that assist them in unknown situations.

Dogs

Dogs can be an important part of physical security if they are included in the plan appropriately and administered properly. Their keen senses of smell and hearing can identify breaches that human guards cannot.

Locks and Keys

In addition to standard mechanical locks, electromechanical locks can accept a range of inputs such as magnetic strips or ID cards, radio signals from name badges, PINs typed into a keypad, or a combination of these.

Manual locks are installed in doors and cannot be altered except by an expert locksmith. They are meant for restricting access to a single door. Programmable locks, on the other hand, can be changed after they have been used, without a locksmith.

Locking Down USB Ports

Sometimes, it may be necessary to lock or disable the USB ports on a system to prevent unauthorized use. If a USB storage device is not already installed on the computer, the administrator can assign the user or group "deny permission" via the following files:

- **%SystemRoot%\Inf\Usbstor.pnf**
- **%SystemRoot%\Inf\Usbstor.inf**

In order to do this, follow these steps:

1. Locate the **%SystemRoot%\Inf** folder.
2. Right-click the **Usbstor.pnf** file, and then click **Properties**.
3. Click the **Security** tab.
4. In the **Group** or **User names** list, click the user or group that you want to set "deny permission" for.
5. In the **Permissions for UserName or GroupName** list, check the **Deny** check box, and then click the **OK** button.

In addition, add the System account to the **Deny** list. Repeat the above steps for the **Usbstor.inf** file as well.

DeviceLock

DeviceLock is a device control solution designed to safeguard network computers against internal and external attacks. It is shown in Figure 1-2, and its features include the following:

- Network administrators can lock out unauthorized users from USB.
- Administrators can control access to any device such as floppies, serial and parallel ports, optical disc drives, and USB devices.
- Users can generate a report concerning the permissions that have been set.
- Provides a level of precision control over available device resources.
- Grants users temporary access to USB devices when there is no network connection.
- Allows the system to be controlled remotely using the centralized management console.
- Generates a report displaying the USB, FireWire, and PCMCIA devices.
- Sets devices in read-only mode.
- Gives a complete log of port and device activity, such as uploading and downloading, made by users and filenames in the standard Windows Event Log.

Trackstick GPS Tracking Device

The Trackstick GPS Tracking Device is a 1 MB memory stick that can store months of travel information. It has the capability to record the following:

- Time
- Date

Source: http://www.devicelock.com/. Accessed 2004.

Figure 1-2 DeviceLock can automatically lock devices.

- Speed
- Direction
- Altitude

The output comes in the following formats:

- RTF
- XLS
- HTML
- Google Earth KML

The Trackstick receives signals from 24 satellites orbiting Earth and works from anywhere on the planet. A specially designed algorithm can measure the time, even indoors. The Trackstick has the ability to map the time and location accurately. Each location can be pinpointed within 15 meters.

USB Tokens

In large organizations that have shared computers, USB tokens can be used to establish a VPN tunnel. There is no need to reconfigure the computers to set up a VPN tunnel if a USB token is used. A PIN has to be entered each time the device is plugged in.

TEMPEST

All electronic devices, including computers, have emanations that can be captured and monitored from a distance. In the case of computers, data flow could be compromised by simply intercepting these electromagnetic radiation (EMR) emanations. Thus, TEMPEST was born. At first it was a secret military project, and it is still illegal to possess TEMPEST-type monitoring devices. TEMPEST can be short for either Transient Electromagnetic Pulse Emanation Surveillance Technology or Telecommunication Electronics Protected from Emanating Spurious Transmissions, though there is no official definition or meaning. These emanations can be of electrical, mechanical, or acoustical energy, all of which can now, with modern technology, be captured. TEMPEST

monitoring can involve protecting against unauthorized eavesdropping or the capturing and interpretation of such information.

TEMPEST protection ensures that systems are placed in protected and secure areas, such as a ***Faraday cage*** (a metallic enclosure or cage that prevents the entry or escape of an electromagnetic field by having a fine-mesh copper screening embedded into the walls or system container), and implements other security measures, such as the elimination of windows. The vibrations resulting from conversations taking place inside a room can now be monitored by focusing a laser measuring device on the outside glass. There are a number of methods used to protect systems against these emanations and threats to physical security.

TEMPEST also refers to investigations and studies of compromising emanations (CE) that include unintentionally sent signals that, if intercepted and analyzed, disclose information that is transmitted, received, handled, or otherwise processed by any information processing equipment.

CE is electrical or acoustical energy emitted by any equipment or system. CE can also occur as:

- Electromagnetic fields emitted by elements of plaintext processing equipment
- Text-related signals coupled to cipher, power, signal, control, or other BLACK (normal unsecured circuits and equipment) lines through common circuit elements such as grounds and power supplies or inductive and capacitive coupling
- Sound waves from mechanical or electromechanical devices, or the human voice

Sources of TEMPEST Signals

The two basic sources of TEMPEST signals are functional sources and incidental sources. Functional sources generate electromagnetic energy, while incidental sources are not designed to generate electromagnetic energy.

The CE sources include all electromechanical and electronic equipment and systems. The extent of CE must be determined, and necessary countermeasures must be applied to the equipment.

Types of TEMPEST Signals

Electrical conductors connected to circuits having the same impedance and power source as equipment processing RED baseband signals can introduce RED baseband emanations. It can be introduced into escape media by capacitive or inductive coupling and by radiation with RED baseband signals of higher frequencies or data rates.

Modulated spurious carriers are the results of modulation arising in a carrier because of RED data. Impulsive emanations are caused by very fast digital signal transitions. Impulsive emanations can be radiated into space or coupled with the external conductors of the equipment under test.

Shielding

TEMPEST shielding helps protect devices from electromagnetic radiation. Corporations also use it to prevent information loss. To reduce TEMPEST emanations, most devices use newly designed microcomponents. Communication security provides low-cost service by reducing the shielded volume to the required size for the protection of RED equipment. The cost of the shielding solution is based on the type of system to be protected. Shielding volumes are classified into two types:

- Small volumes are known as shielded enclosures and do not require protection from the overall facility structure.
- Large volumes are known as shielded areas and are concentrated on the main part of the facility and mostly require integration into the structural design.

Grounding

Grounding supplies a low-resistance path that moves lightning, power transients, and emanations to the reference point. The system is made up of an earth electrode subsystem (EESS), a fault protection subsystem (FPSS), a signal reference subsystem, and a lightning protection subsystem:

- The earth electrode subsystem has a maximum resistance of 10 ohms.
- The fault protection subsystem (FPSS) is intended to shield personnel and equipment from electrical circuit faults.
- The lightning protection subsystem provides protection against lightning and other temporary voltages that may enter the building.
- The signal reference subsystem provides a common signal ground reference for the entire building.

By grounding RED/BLACK signals, signal grounds, EESS grounds, cable ladders, conduits, and ducts can be connected. An equipotential ground plane is frequently installed in secure facilities to minimize the results of compromising emanations. This consists of the following equipment:

- Distribution frames
- Patch panels
- RED/BLACK processing

Attenuation

EMI shielding is calculated in decibels of attenuation. Shielding is more effective as the dB of the attenuation increases. The signal strength is calculated as the ratio of the signal strength in the clear to the signal strength through the shield.

Banding

Banding refers to restricting information to a specific set of frequencies, thus protecting information from being hacked. If banding is not properly done, then there is a chance of impartial data loss.

Filtered Power

Filtered power filters out the redundant electromagnetic radiations from equipment. Generally, low-pass filters can prevent everything, excluding high-frequency signals. Low-pass filters are restricted under high-frequency signals. The core function of the TEMPEST filter is to prevent the radiation of RED signals. However, filters are not able to reduce unintended emissions to zero.

Cabling

The TEMPEST emission control standard for network cabling systems combined with data encryption and other security systems enable information security. Fiber optic cable radiates only heat emissions, but it is costlier than copper cable. According to TEMPEST standards, potential emanations are generally addressed by placing all cables inside a ferrous channel or tubing to block any electromagnetic radiation.

The shielded copper cable will provide an additional layer of security that reduces some emissions. Single overall shielded (FTP) cables, like the one pictured in Figure 1-3, do not eliminate the need for conduit and RED/BLACK separation in high-security environments. The separation distance is lower with shielded cables, decreasing the cost for pathways and spaces.

The Siemon's TERA end-to-end network cabling system uses S/FTP cable and fully shielded connectivity, and was the first copper network cabling system to pass NSA-certified TEMPEST security testing. In S/FTP cable, each pair is shielded separately and an overall braid shield surrounds all connectors. This shielding removes the potential security gap caused by single radiation or emission. The additional shielding that is combined into the outlets and plugs eliminates all potential emissions from the overall cabling system.

S/FTP shielded twisted-pair cabling consists of the following:

- Conductor
- Insulation

Source: www.siemon.com/shielded-twistedpair.asp. Accessed 2004.

Figure 1-3 This is a cross section of an S/FTP cabling system.

- Tinned copper braid
- Aluminum/polyester foil tape
- Outer jacket

Zoning

Zoning is a control method used when different protection levels are required. A damaged UPS and communication room should have a medium protection level area, such as 60 decibels, while a damaged control and computer room should have a high protection level area, perhaps 100 decibels. The zones can be used to show the main form and features of different areas. Generally, the weakest areas are located at the center, inside other areas.

Zones are categorized into the following areas:

- Zone 0 is for protected areas.
- Zone 1 is for the generator area.
- Zone 2 is for the UPS and communication area.
- Zone 3 is for complicated control rooms.

TEMPEST Separation

Isolators are used to isolate, through attenuation or insertion, loss between a source and a load. It works like a filter but its isolator characteristics are very high. Circuit isolation reaches its destination by using transformers, feedback amplifiers, or optical couplers. Isolators provide an open circuit to unwanted signals. An isolator should have a minimum of a 4-inch optically coupled path to meet TEMPEST requirements, subject to the stress isolators that are connected to the lines carrying lightning or EMP transients.

Encryption safeguards confidential information from being exposed. Unwanted emanations from RED equipment that occur due to interceptions cannot be prevented via encryption. There are several steps that equipment and facility designers can take to prevent information exposure through compromised emanations. All these techniques minimize the potential of a stray signal and involve hiding the sensitive content in the background electrical noise.

Fire Safety: Fire Suppression, Gaseous Emission Systems

Portable System

These are used when direct implementation of fire suppression is required. They are effective for smaller fires, and they prevent the activation of a building's sprinkler systems, which would likely cause water damage. Portable systems are rated by the type of fire they are designed to suppress:

- Class A interrupts the ability of the fuel to be ignited. This is best for fire caused by normal combustible fuels such as wood, paper, and textiles.
- Class B removes oxygen from the fire. This is best for fire caused by combustible liquids or gases. Carbon dioxide, multipurpose dry chemicals, and halon fire extinguishers are best suited for these types.
- Class C uses nonconducting agents. This is best for fire caused by powerful electrical equipment. They use nonconducting agents, such as carbon dioxide, multipurpose dry chemicals, and halon.
- Class D uses special agents for combustible metal fires, such as those involving magnesium, lithium, and sodium.

Gaseous System

Dry-Pipe System The dry-pipe system is intended to work in areas hosting electrical machinery. It contains pressurized air. This air keeps the valves closed and escapes through the sprinkler heads. This decreases the threat of accidental initiation of the system. It is the best solution for advanced computer environments.

Preaction System This system has a two-phase reaction to fire. When fire is detected, the first phase is triggered and valves allow water to enter the system. A difference between the preaction system and the deluge system is that, in the deluge system, valves are left open as soon as the first phase is triggered, without waiting for the second phase to begin.

Gaseous Emission Systems

Chemical gas systems that suppress fires have a supplementary agent. There are two major types of gaseous systems: carbon dioxide and halon. Carbon dioxide absorbs the oxygen supply to the fire. Halon is a cleaning agent that does not leave any filtrate when dry and also does not interfere with electronic equipment. Carbon dioxide has the dangerous side effect of possible suffocation, and halon can deplete the ozone layer.

The following are some alternative agents:

- *FM-200*: Identical to halon 1301 and safe in residential areas
- *Inergen*: Combination of nitrogen, argon, and carbon dioxide
- *FE-13*: A more recent and safer cleaning agent

Fire Detection

Fire detection systems are either manual or automatic. Manual systems consist of human reactions, such as calling the fire department, while automatic systems have physically activated alarms, such as sprinklers and gaseous systems.

Thermal Detection

Thermal detection systems contain an advanced heat detector that functions in either of two ways. The first is called fixed temperature. Here, the sensor recognizes when the environmental temperature reaches a preset level, perhaps around 135° Fahrenheit or 57° Celsius. The second is called rate of rise. Here, the sensor detects an abnormal increase in the environmental temperature within a short period of time.

Smoke Detection

This is a common way of detecting fire in residential as well as commercial buildings. Smoke detectors function in three ways. In the first, photoelectric sensors detect an infrared beam in an area. In the second, an ionization sensor contains a small quantity of injurious radioactive material inside a detection chamber. Air-aspirating detectors are very advanced and are used in high-sensitivity areas. They function by taking in air and passing it through a compartment containing a laser beam. If the laser beam is diverted by smoke, the system is initiated.

Flame Detector

This detects the infrared or UV light created by an open flame. Flame detectors need a direct line of sight with the flame. They match the flame signature against a database to determine whether to trigger the alarm and suppression systems.

Heating, Ventilation, and Air Conditioning

Temperature

Computer systems are liable to get damaged from abnormally high temperatures. At 175°F, hardware can be damaged or destroyed. At 32°F, media are vulnerable to cracking and the components can freeze.

Rapid fluctuations in temperature can generate short circuits or otherwise harm a system and its components. The optimal temperature for a computer is between 70°F and 74°F.

Humidity

High humidity levels lead to condensation problems, and low levels can increase the quantity of static electricity. This can short-circuit electrical equipment, and fungus can grow and rot paper.

Ventilation Shafts

In residences, the ductwork can be big enough for intruders to climb through. In many buildings, the shafts can be entirely outside the view of security personnel. In most buildings, the vents lead to separate rooms and are no larger than 12–24 inches. If the vents are much bigger, security can use wire mesh grids at different places.

Power Management and Conditioning

Grounding

Grounding guarantees that electric current is appropriately discharged to the ground. If a piece of electrical equipment is not properly grounded, any user touching that equipment might get an electric shock, and the equipment can be damaged. In rare cases, this can even lead to death. Electrical equipment installed in regions that have contact with water must be carefully grounded with GFCI equipment (ground fault circuit interruption). GFCI has the ability to rapidly identify and obstruct a ground defect. Power must also be provided in adequate amperage to sustain the required operations. Overburdening a circuit can overburden the power load on an electrical cable, possibly causing a fire.

Emergency Shutoff

Most computer rooms and wiring closets are built with an emergency power shutoff in the form of a large, obvious red button. Such devices are a last resort to prevent personal damage and machine damage during flooding or sprinkler activation.

Water Problems

Absence of water causes problems for fire suppression systems and cooling systems. On the other hand, too much water can be a major threat. Damage due to water can cause computers and other electrical equipment to fail. Therefore, flooding and leaks must be prevented, as they may cause damage to paper and electronic information storage.

Structural Collapse

Inescapable environmental factors cause buildings to collapse. Buildings are designed and built with definite load restrictions, and overloading the capacity can lead to structural failure. Regular inspections by expert civil engineers are necessary.

Uninterruptible Power Supplies

In incidents of power failure, a UPS acts as a backup for important computer systems.

Standby or Offline UPS

A standby or offline UPS is an offline battery backup that recognizes when power is no longer supplied from the electrical service. When this happens, the UPS transfers power from its batteries through a DC-to-AC converter until the power is recovered or the computer shuts down.

Ferroresonant Standby UPS

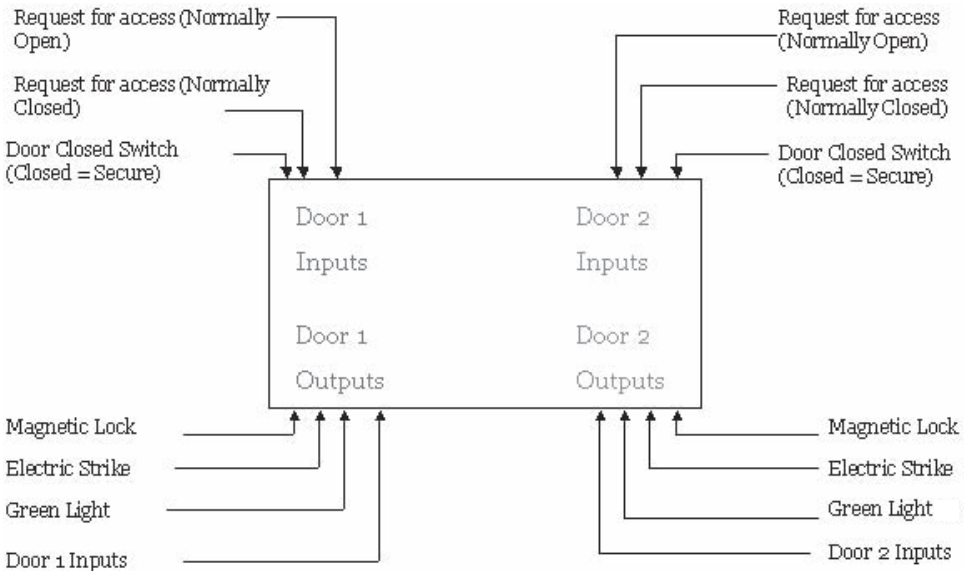
A ferroresonant standby UPS enhances the standard UPS design. The major difference is that it substitutes the UPS transfer switch. The transformer performs power conditioning and line filtering on the major power source, decreasing the effect of power problems. The transformer also stores energy in its coils, offering a buffer to fill the deficit between the break in the power supply and activation of the battery backup. This reduces the chances of system reset and data loss. These are best suited to a setting that demands a huge capacity of conditioned and genuine power, as they can go up to 14,000 VA.

Line-Interactive UPS

A line-interactive UPS has a considerably different design than the others. The inner components of the standby models are substituted with a pair of inverters and converters. Its major power source is from the main line, with the battery as the support. As soon as the power supply is stopped, the inverters and converters begin providing the power. Since the device is connected to the output, this model has a quicker response time and has built-in power conditioning and line filtering.

True-Online UPS

True-online UPS is the most expensive type. The process frequently changes from an AC to DC battery storage and continues to be AC fed, generating high quantities of heat. An advanced model resolves this problem by hosting a delta-conversion unit that permits some of the inward power to be fed directly to target computers,



Source: http://www.blackbox.co.uk/technical/manuals/D/Dortronics/4442%20INTERLOCK%20SHEET.PDF. Accessed 2004.

Figure 1-4 This is the programming logic for a mantrap system.

decreasing the quantity of energy wasted and heat produced. If the power supply ceases, the delta unit shuts off and batteries mechanically balance the high power needed, but the systems continue and do not recognize a fluctuation in voltage levels.

Mantrap

A mantrap offers alternate access to resources. It has two different doors with an airlock between them. A single door can be opened at a time, and authentication is required for both doors.

Mantraps restrict access to secure areas within a facility while providing an effective means to physically detain unauthorized persons until security provides clearance. Mantraps are typically manual swing doors forming a vestibule, but they can also use sliding doors or gates. Some mantraps make use of turnstiles or revolving doors.

Once a person gets into the first door, he or she is not allowed to enter the second door until the first one is closed.

This system offers protection in three ways:

- It is difficult to forcibly enter through a single door.
- It permits time to evaluate the person inside the mantrap prior to letting him or her enter the second door.
- It permits only one person to enter at a time.

In huge systems like those available in government installations and large financial institutions, many doors can be installed to create a massive mantrap system. Figure 1-4 shows the programming logic for a mantrap.

Developing a Physical Security Checklist

A physical security checklist defines the areas that need to be secured. It also describes the methods, technologies, and applications used to ensure that security.

Physical security protects:

- Stored information resources of the company
- Functions of the information systems

A security checklist should include the following steps:

1. Examine and analyze the buildings and boundaries that are problematic.
2. Install strong windows and locks on the doors, and ensure that the doors remain locked.
3. Place servers and other important assets in secured rooms without windows.
4. Set up proper air conditioners and fire detecting systems in the rooms where servers are located.
5. Keep important resources away from vents, pipes, toilets, radiators, and insecure zones.
6. Turn off monitor screens at night.
7. Maintain an inventory list, including memory, processors, serial numbers, locations, and purchase dates.
8. Label critical resources by using ultraviolet marking, which aids in the recovery of lost and stolen materials.
9. Maintain a backup of data and store it far from the source machines. Storing the backups off site is the best solution.
10. Distributing computers across multiple sites secures data from theft.
11. Physically lock equipment in open areas.
12. Carrying identification cards ensures that no outsider enters the organization without being noticed.
13. Ensure that visitors are genuine at the reception area.

Chapter Summary

- In addition to securing the network from external software attacks, the physical security of assets must be ensured.
- Both human (e.g., vandals, disgruntled employees, and attackers) and natural factors (e.g., earthquakes, floods, and electrical storms) affect the physical security of an organization.
- Some unsecured places where office information can be found are workstations, work areas, dustbins, and monitors.
- A smart card is a credit card–sized plastic device that contains a computer chip and memory. It can store, process, and output data securely.
- In information technology, biometrics is the measurement and analysis of human fingerprints, irises, retinas, voices, faces, and hands.
- Managing desktop security includes people, processes, and technology factors.
- Improving physical security involves both physical and technological solutions.

Review Questions

1. What is physical security?

_____

_____

_____

_____

2. Who is responsible for physical security?

_____

_____

_____

_____

3. What factors affect physical security?

4. What are the different types of attackers?

5. How do you implement premises security?

6. What are smart cards?

7. Explain the process of fingerprint scanning.

8. What are some laptop security procedures?

9. Explain the process of securing backups.

10. How does a mantrap work?

_____

_____

_____

_____

Hands-On Projects

1. Use 1st Security Agent to password-protect and secure Windows-based computers.
   - Navigate to Chapter 1 of the Student Resource Center.
   - Install and launch the 1st Security Agent program.
   - Click **Screen Lock** under User Restrictions, check the **Screen-lock Password** check box, and then click **Change**.
   - Change the password and click the **OK** button.
   - Go to the Control Panel option in User Restrictions, click **Add or Remove**, and check the **Disable Add/Remove Programs** check box.
   - Go to the Explorer option in User Restrictions, check the **Hide Drives in My Computer** check box, and select the drives to be hidden.
   - Go to the Start Menu option in User Restrictions and check the **Remove My Network Places from the Start Menu** check box.
   - Go to the Taskbar option in User Restrictions and check the **Hide the Taskbar Clock** check box.
   - Go to the Special Icons option in User Restrictions and check the **Hide My Computer Icon** check box.
   - Go to the menu bar, click **Apply Tree**, and click the **OK** button in the **Confirm** window to apply the settings.
   - To remove all restrictions, click **Clear Tree** in the menu bar and click the **OK** button in the **Confirm** window.
2. Use Access Lock to secure your desktop when you are away from your computer.
   - Navigate to Chapter 1 of the Student Resource Center.
   - Install and launch the Access Lock program.
   - Click the **Options** icon in the menu bar. A new window will be opened. Click the **Screen Saver** tab and check the **Lock screen** option.
   - Go to the **Security** tab in the Options window and check the check boxes as desired.
   - Click **Password** on the menu bar, type the desired password, and click the **OK** button to change the password.
   - Click **Activate** in the menu bar to make these settings active.
   - Click **Deactivate** in the menu bar to deactivate the settings.
3. Use Access Denied XP to safeguard your computer from unwanted access and protect the desktop and boot process.
   - Navigate to Chapter 1 of the Student Resource Center.
   - Install and launch the Access Denied XP program.
   - Click the plus icon in the menu bar to add a new user account.
   - Enter the user information in the Add User account window and click the **OK** button.

- Click the users icon in the menu bar, as shown in Figure 1-5, to manage user accounts.

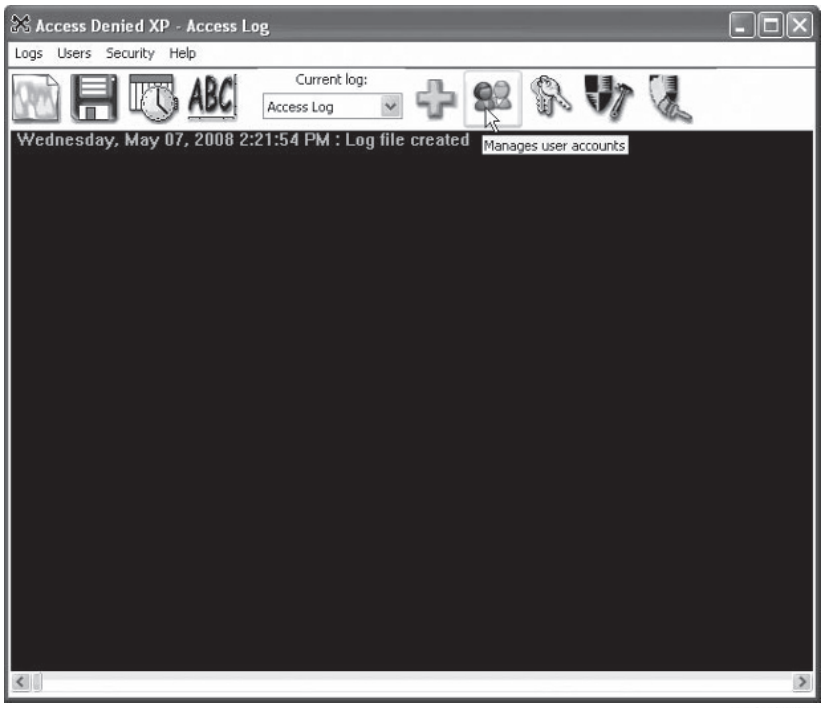


Figure 1-5 This is the users icon.

- Select the user account you wish to modify, type the user information, and click the **OK** button.
- Click the security icon, as shown in Figure 1-6, in the menu bar to set the security options.

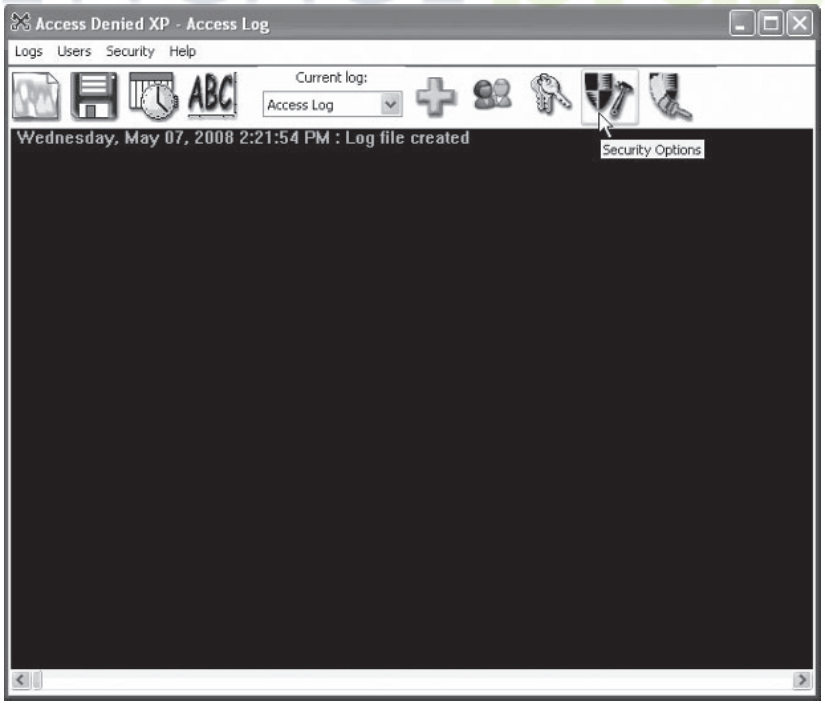


Figure 1-6 This is the security icon.

- Set the security settings as desired and click the **OK** button to activate.
- Click the boot messages icon, shown in Figure 1-7, in the menu bar to edit boot messages.

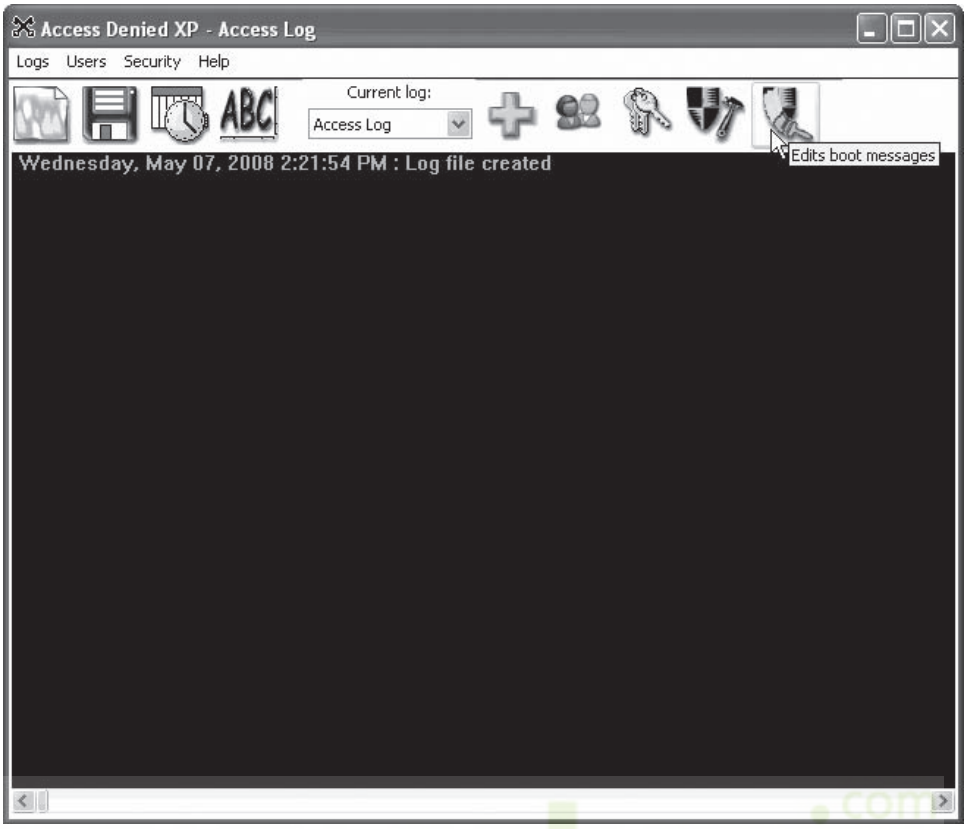


Figure 1-7 This is the boot messages icon.

- Set the settings in the **Edit Logon Access Messages** window and click **Test** to check the view of the login screen.

4. Use Desktop Lock to lock the PC and protect it from unauthorized access.
   - Navigate to Chapter 1 of the Student Resource Center.
   - Install and launch the Desktop Lock program.
   - To set the desktop lock settings, click **Configure**.
   - To set the Lock Mode settings, click the **Lock** tab and select the desired options.
   - To set the Unlock Mode settings, click the **Unlock** tab and select the desired options.
   - To set the display options while the system is locked, click the **Display** tab.
   - To set the advanced options, click the **Advanced** tab and select the desired options.
   - To set up the schedule items, click the **Schedule** tab and click **Setup**.
   - To set up the user mode settings, click the **Users** tab.
   - Click the **OK** button to apply the settings.
   - Click the **Lock Now** button to lock the desktop.
   - To create a virtual desktop, click **Virtual Screen** in the **Desktop Lock** window.
   - Click **Options** to set the virtual screen options in the **Virtual Screen** window.

- Click **Profiles Manager** to manage profiles.
- To add a profile name, click **Add** in the profiles manager of the **Virtual Screen** window.
- Enter the profile name in the **Input profile name** window and click the **OK** button.
- To change or set the password for the profile, click **Change** in the **Profile Settings** window.
- Enter the password and click the **OK** button in the **Set Password** window.
- Click **OK** in the **Profile Settings** window to apply the profile settings.
- To quit the application, click **Exit**.

5. Use Lockdown Plus PC to prevent users from deleting critical files and applications, making unauthorized changes to the desktop, saving unwanted programs, running disallowed programs, and downloading using Internet Explorer.
   - Navigate to Chapter 1 of the Student Resource Center.
   - Install and launch the Lockdown Plus PC program.
   - To protect files and folders, click the **Protect Files and Folders** option, and then start the wizard by clicking the **Wizard** button.
   - Select a desired option for securing the objects and click **Next**.
   - Click **Add Files** to add the files to be protected.
   - Browse the files in the location that you want to protect and click **Open**.
   - Click **Lock** to apply the protection.
   - Click **Unlock** to remove the file restrictions.
   - To protect the local hard disks, click **Protect Local Hard Disks**.
   - Select the drive you wish to lock, set the desired options, and click **Lock** to lock the hard drive.
   - Click **Unlock** to unlock the disk protection.
   - To restrict external drives, click **Restrict External Drives**.
   - Select the device name and click **Lock** to restrict access.
   - Click **Protect Window System** to select the settings for restricting access to the Windows system.
   - Click **Manage Accounts** to manage user accounts.
   - To change the password, click **Password**, enter the desired password, and click the **OK** button.