PHYSICAL DESIGN

PHYSICAL DESIGN: Security Technology - IDS, Scanning and Analysis Tools -Cryptography - Access Control Devices - Physical Security - Security and Personnel issues.

5.1 SECURITY TECHNOLOGY

Security

- "Quality or state of being secure—to be free from danger"
- A successful organization should have multiple layers of security in place:
  - Physical security
  - Personal security
  - Operations security
  - Communications security
  - Network security
  - Information security

Physical Design

- Physical design of an information security program is made up of two parts:
  1. Security technologies
  2. Physical security
- Physical design process:
  - Identifies complete technical solutions based on these technologies (deployment, operations and maintenance elements)
  - Design physical security measures to support the technical solution.

Firewalls

- A firewall in an information security program is similar to a building's firewall in that it prevents specific types of information from moving between the outside world, known as the untrusted network (for example, the Internet), and the inside world, known as the trusted network.
- The firewall may be a separate computer system, a software service running on an existing router or server, or a separate network containing a number of supporting devices.
- A software or hardware component that restricts network communication between two computers or networks.
  - In buildings, a firewall is a fireproof wall that restricts the spread of a fire.

  - Network firewall prevents threats from spreading from one network to another.
- Prevent specific types of information from moving between the outside world (untrusted networks) and the inside world (trusted networks)
- Firewalls can be categorized by processing mode, development era, or structure.

Firewall Processing Modes

- Firewalls fall into five major processing-mode categories:
  1. Packet-filtering firewalls,
  2. Application gateways,
  3. Circuit gateways,
  4. MAC layer firewalls, and
  5. Hybrids.
- Hybrid firewalls use a combination of the other four modes,

1. Packet filtering:

- Examine the header information of data packets that come into a network.
- a packet filtering firewall installed on TCP/IP based network and determine whether to drop a packet or forward it to the next network connection based on the rules programmed in the firewall.
- Packet filtering firewalls scan network data packets looking for violation of the rules of the firewalls database.
- Filtering firewall inspect packets on at the network layers.
- If the device finds a packet that matches a restriction it stops the packet from traveling from network to another.
- Filters packet-by-packet, decides to Accept/Deny/Discard packet based on certain/configurable criteria – Filter Rule sets.
- Typically stateless: do not keep a table of the connection state of the various traffic that flows through them
  - Not dynamic enough to be considered true firewalls.
  - Usually located at the boundary of a network.
  - Their main strength points: Speed and Flexibility.

There are three subsets of packet filtering firewalls:

1. Static filtering
2. Dynamic filtering
3. stateful inspection

Static filtering:

- Requires that the filtering rules covering how the firewall decides which packets are allowed and which are denied.
- This type of filtering is common in network routers and gateways.

Dynamic filtering

- Allows the firewall to create rules to deal with event.
- This reaction could be positive as in allowing an internal user to engage in a specific activity upon request or negative as in dropping all packets from a particular address

Stateful inspection

- Keep track of each network connection between internal and external systems using a state table.
- A state table tracks the state and context of each packet in the conversation by recording which station send, what packet and when.
- More complex than their constituent component firewalls
- Nearly all modern firewalls in the market today are stateful

Basic Weaknesses Associated with Packet Filters\ Stateful

- They cannot prevent attacks that employ application-specific functions.
- Logging functionality present in packet filter firewalls is limited vulnerabilities or
- Most packet filter firewalls do not support advanced user authentication schemes.
- Vulnerable to attacks and exploits that take advantage of problems within the
- TCP/IP specification and protocol stack, such as network layer address spoofing.
- Susceptible to security breaches caused by improper configurations.

Advantages:

- One packet filter can protect an entire network
- Efficient (requires little CPU)
- Supported by most routers

Disadvantages:

- Difficult to configure correctly
- Must consider rule set in its entirety
  - Difficult to test completely
  - Performance penalty for complex rulesets
- Stateful packet filtering much more expensive
  - Enforces ACLs at layer 3 + 4, without knowing any application details

2. Application Gateways

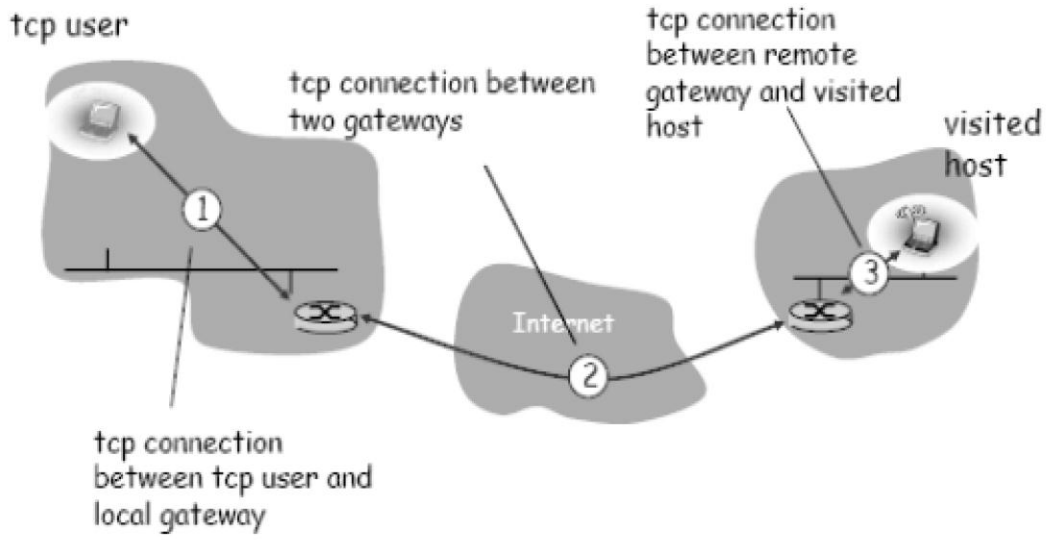
- The application gateway, also known as an application-level firewall or application firewall, is frequently installed on a dedicated computer, separate from the filtering router, but is commonly used in conjunction with a filtering router.
- It is also known as proxy server since it runs special software that acts as a proxy for a service request.
- One common example of proxy server is a firewall that blocks or requests for and responses to request for organization. web pages and services from the internal computers of an
- The primary disadvantage of application level firewalls is that they are designed for a specific protocols and cannot easily be reconfigured to protect against attacks in other protocols.
- Application firewalls work at the application layer.
- Filters packets on application data as well as on IP/TCP/UDP fields.
- The interaction is controlled at the application layer.
- A proxy server is an application that mediates traffic between two network segments.
- With the proxy acting as mediator, the source and destination systems never actually “connect”.
- Filtering Hostile Code: Proxies can analyse the payload of a packet of data and make decision as to whether this packet should be passed or dropped.

3. Circuit gateways:

- Operates at the transport layer.
- Connections are authorized based on addresses, they prevent direct connections between network and another.
- They accomplish this prevention by creating channels connecting specific systems on each side of the firewall and then allow only authorized traffic.
- Relays two TCP connections (session layer)

- Imposes security by limiting which such connections are allowed
- Once created usually relays traffic without examining contents
- Monitor handshaking between packets to decide whether the traffic is legitimate
- Typically used when trust internal users by allowing general outbound connections
- SOCKS commonly used for this.

Circuit Level Firewalls Example



4. MAC Layer Firewalls

- MAC Layer Firewalls While not as well known or widely referenced as the firewall approaches above, MAC layer firewalls are designed to operate at the media access control sublayer of the *data link layer* (Layer 2) of the OSI network model.
- This enables these firewalls to consider the specific host computer's identity, as represented by its MAC or network interface card (NIC) address in its filtering decisions.
- Thus, MAC layer firewalls link the addresses of specific host computers to ACL entries that identify the specific types of packets that can be sent to each host, and block all other traffic**.**

5. Hybrid Firewalls

- Hybrid firewalls combine the elements of other types of firewalls— that is, the elements of packet filtering and proxy services, or of packet filtering and circuit gateways.
- A hybrid firewall system may actually consist of two separate firewall devices; each is a separate firewall system, but they are connected so that they work in tandem.

- For example, a hybrid firewall system might include a packet-filtering firewall that is set up to screen all acceptable requests, then pass the requests to a proxy server, which in turn requests services from a Web server deep inside the organization's networks.
- An added advantage to the hybrid firewall approach is that it enables an organization to make a security improvement without completely replacing its existing firewalls**.**

Types of Firewalls

- Finally, Types depending on whether the firewalls keeps track of the state of network connections or treats each packet in isolation, two additional categories of firewalls exist:
    1. Stateful firewall
    2. Stateless firewall

Stateful firewall

- Keeps track of the state of network connections (such as TCP streams) traveling across it.
- Stateful firewall is able to hold in memory significant attributes of each connection, from start to finish. These attributes, which are collectively known as the state of the connection, may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection.

Stateless firewall

- Treats each network frame (Packet) in isolation. Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.
- The classic example is the File Transfer Protocol, because by design it opens new connections to random ports.

Advantages of a Firewall

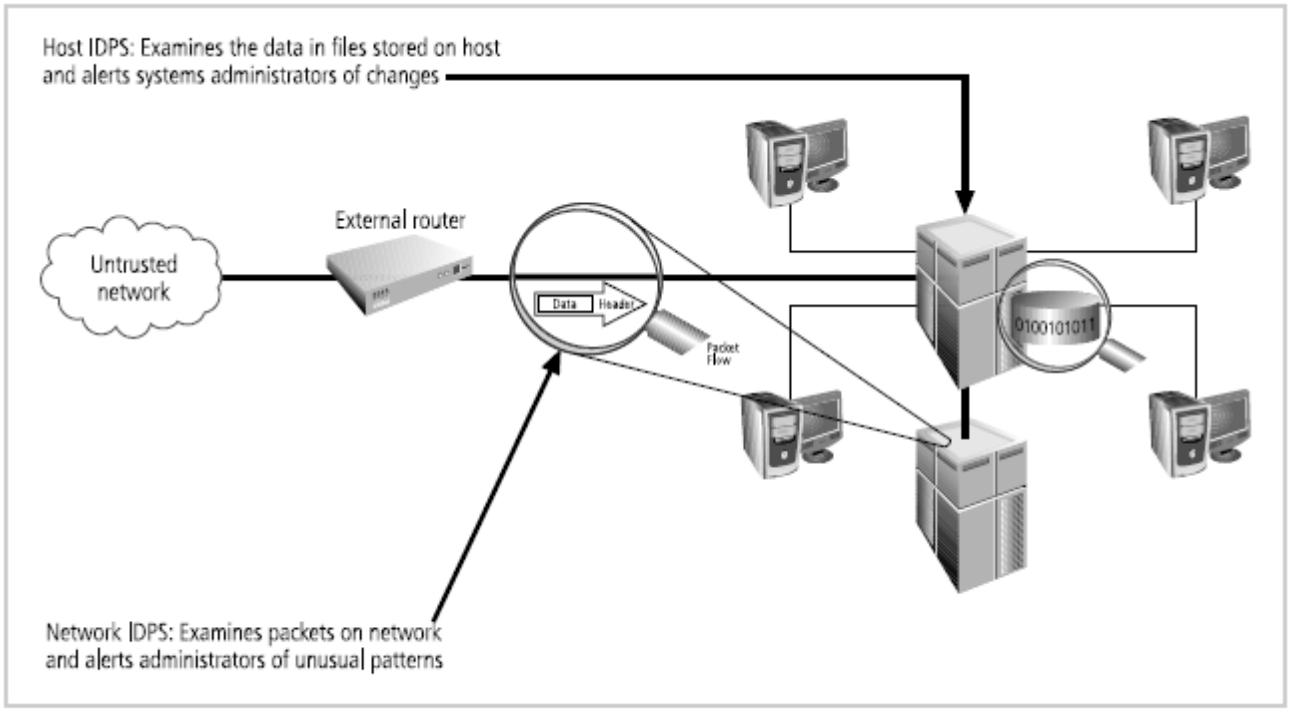
- Stop incoming calls to insecure services
- Such as rlogin and NFS
- Control access to other services
- Control the spread of viruses
- Cost Effective
- More secure than securing every System

Disadvantages of a Firewall

- Central point of attack
- Restrict legitimate use of the Internet
- Bottleneck for performance
- Does not protect the 'back door'
- Cannot always protect against
- Smuggling
- Cannot prevent insider attacks**.**

5.2 INTRUSION DETECTION SYSTEM (IDS)

- A current extension of IDS technology is the intrusion prevention system (IPS), which can detect an intrusion and also prevent that intrusion from successfully attacking the organization by means of an active response.
- Because the two systems often coexist, the combined term ***intrusion detection and prevention system (IDPS)*** is generally used to describe current anti-intrusion technologies
- An ***intrusion*** occurs when an attacker attempts to gain entry into or disrupt the normal operations of an information system, almost always with the intent to do harm.



Intrusion Detection and Prevention Systems

- Intrusion ***prevention*** consists of activities that deter an intrusion. Some important intrusion prevention activities are writing and implementing good enterprise information security policy, planning and executing effective information security programs, installing and testing technology-based information security countermeasures (such as firewalls and intrusion detection systems), and conducting and measuring the effectiveness of employee training and awareness activities.
- Intrusion ***detection*** consists of procedures and systems that identify system intrusions. Intrusion reaction encompasses the actions an organization takes when an intrusion is detected.

Why Use an IDPS?

- According to the NIST documentation on industry best practices, there are several compelling reasons to acquire and use an IDPS:

1. To prevent problem behaviours by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system
2. To detect attacks and other security violations that are not prevented by other security measures
3. To detect and deal with the preambles to attacks (commonly experienced as network probes and other "doorknob rattling" activities)
4. To document the existing threat to an organization
5. To act as quality control for security design and administration, especially in large and complex enterprises
6. To provide useful information about intrusions that do take place, allowing improved diagnosis, recovery, and correction of causative factors.

5.2.1 Types of IDPS

- IDPSs operate as
    1. Network based
    2. Host-based systems.
- A network-based IDPS is focused on protecting network information assets. Two specialized subtypes of network-based IDPS are the wireless IDPS and the network behavior analysis (NBA) IDPS
- A host-based IDPS protects the server or host's information assets; monitors both network connection activity and current information states on host servers.

1. **Host-based IDPS**

- Resides on a particular computer or server and monitors activity only on that system
- Benchmark and monitor the status of key system files and detect when intruder creates, modifies, or deletes files
- Most HIDPSs work on the principle of configuration or change management
- Advantage over NIDPS: can usually be installed so that it can access information encrypted when traveling over network
- Configures and classifies various categories of systems and data files
- HIDPSs provide only a few general levels of alert notification
- Unless the HIDPS is very precisely configured, benign actions can generate a large volume of false alarms
- HIDPSs can monitor multiple computers simultaneously

Advantages of HIDPSs

- Can detect local events on host systems and detect attacks that may elude a network-based IDPS
- Functions on host system, where encrypted traffic will have been decrypted and is available for processing
- Not affected by use of switched network protocols
- Can detect inconsistencies in how applications and systems programs were used by examining records stored in audit logs

Disadvantages of HIDPSs

- Pose more management issues
- Vulnerable both to direct attacks and attacks against host operating system
- Does not detect multi-host scanning, nor scanning of non-host network devices
- Susceptible to some denial-of-service attacks
- Can use large amounts of disk space
- Can inflict a performance overhead on its host systems

2. **Network-Based IDPS**

- Resides on computer or appliance connected to segment of an organization's network; looks for signs of attacks

- Installed at specific place in the network where it can watch traffic going into and out of particular network segment
- Monitor network traffic
- When a predefined condition occurs, notifies the appropriate administrator
- Looks for patterns of network traffic
- Match known and unknown attack strategies against their knowledge base to determine whether an attack has occurred
- Yield many more false-positive readings than host-based IDPSs

Advantages of NIDPSs

- Good network design and placement of NIDPS can enable organization to use a few devices to monitor large network
- NIDPSs are usually passive and can be deployed into existing networks with little disruption to normal network operations
- NIDPSs not usually susceptible to direct attack and may not be detectable by attackers

Disadvantages of NIDPSs

- Can become overwhelmed by network volume and fail to recognize attacks
- Require access to all traffic to be monitored
- Cannot analyze encrypted packets
- Cannot reliably ascertain if attack was successful or not
- Some forms of attack are not easily discerned by NIDPSs, specifically those involving fragmented packets

5.2.2 IDPS Detection Methods

- IDPSs use a variety of detection methods to monitor and evaluate network traffic.
- Three methods dominate:
    1. Signature-based approach,
    2. Statistical-anomaly approach, and
    3. Stateful packet inspection approach.

1. Signature-Based IDPS

- A signature-based IDPS (sometimes called a knowledge-based IDPS or a misuse-detection IDPS) examines network traffic in search of patterns that match known signatures—that is, preconfigured, predetermined attack patterns.
- Signature based IDPS technology is widely used because many attacks have clear and distinct signatures, for example:
    - footprinting and fingerprinting activities use ICMP, DNS querying, and e-mail routing analysis;
    - exploits use a specific attack sequence designed to take advantage of a vulnerability to gain access to a system;
    - DoS and DDoS attacks, during which the attacker tries to prevent the normal usage of a system, overload the system with requests so that the system's ability to process them efficiently is compromised or disrupted.
- A weakness of this method:
    - If attacks are slow and methodical, they may slip undetected through the IDPS, as their actions may not match a signature that includes factors based on duration of the events

2. Statistical Anomaly-Based IDPS

- Also called behavior-based IDPS
- First collects data from normal traffic and establishes a baseline
- Then periodically samples network activity, based on statistical methods, and compares the samples to the baseline
- When activity falls outside the baseline parameters (clipping level), The IDPS notifies the administrator
- Advantages:
    - Able to detect new types of attacks, because it looks for abnormal activity of any type
    - IDPS can detect new types of attacks
- Disadvantages
    - Requires much more overhead and processing capacity than signature-based
    - May generate many false positives.

5.3 HONEYPOTS, HONEYNETS, AND PADDED CELL SYSTEMS

- A class of powerful security tools that go beyond routine intrusion detection is known variously as honeypots, honeynets, or padded cell systems. To understand why these tools are not yet widely used, you must first understand how they differ from a traditional IDPS.
- Honeypots are decoy systems designed to lure potential attackers away from critical systems. In the industry, they are also known as decoys, lures, and fly-traps. When a collection of honeypots connects several honeypot systems on a subnet, it may be called a honeynet.
- A honeypot system (or in the case of a honeynet, an entire subnetwork) contains pseudo-services that emulate well-known services, but is configured in ways that make it look vulnerable to attacks.
- This combination is meant to lure potential attackers into committing an attack, thereby revealing themselves—the idea being that once organizations have detected these attackers, they can better defend their networks against future attacks targeting real assets. In sum, honeypots are designed to do the following.
  - Divert an attacker from critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to document the event and, perhaps, respond.

Padded cell

- A Padded Cell is a honey pot that has been protected so that it cannot be easily compromised. In other words, a padded cell is a hardened honey spot..
- The advantages and disadvantages of using honey pot or padded cell approach

Advantages:

- Attackers can be diverted to targets that they cannot damage.
- Administrators have time to decide how to respond to an attacker.
- Attackers action can be easily and extensively monitored
- Honey pots may be effective at catching insiders who are snooping around a network.

Disadvantages:

- The legal implication of using such devices are not well defined.

- Honey pots and Padded cells have not yet been shown to be generally useful security technologies.
- An expert attacker, once diverted into a decoy system, may become angry and launch a hostile attack against an organization‘s systems
- Admins and security managers will need a high level of expertise to use these systems**.**

5.4 SCANNING AND ANALYSIS TOOLS

- In order to secure a network, it is imperative that someone in the organization knows exactly where the network needs securing. This may sound simple and obvious; however, many companies skip this step.
- They install a simple perimeter firewall, and then, lulled into a sense of security by this single layer of defense, they relax. To truly assess the risk within a computing environment, you must deploy technical controls using a strategy of defense in depth, which is likely to include intrusion detection systems (IDSs), active vulnerability scanners, passive vulnerability scanners, automated log analyzers, and protocol analyzers (commonly referred to as sniffers).

Port Scanners

- Port scanning utilities, or port scanners, are tools used by both attackers and defenders to identify (or fingerprint) the computers that are active on a network, as well as the ports and services active on those computers, the functions and roles the machines are fulfilling, and other useful information.
- These tools can scan for specific types of computers, protocols, or resources, or their scans can be generic. It is helpful to understand the network environment so that you can use the tool most suited to the data collection task at hand.
- A port is a network channel or connection point in a data communications system. Within the TCP/IP networking protocol, TCP and User Datagram Protocol (UDP) port numbers differentiate the multiple communication channels that are used to connect to the network services being offered on the same network device.
- Each application within TCP/IP has a unique port number. Some have default ports but can also use other ports. Some of the well-known port numbers are presented in Table.

- In all, there are 65,536 port numbers in use for TCP and another 65,536 port numbers for UDP. Services using the TCP/IP protocol can run on any port; however, services with reserved ports generally run on ports 1–1023.
- Port 0 is not used. Ports greater than 1023 are typically referred to as ephemeral ports and may be randomly allocated to server and client processes.

TCP Port Numbers	TCP Service
20 and 21	File Transfer Protocol (FTP)
22	Secure Shell (SSH)
23	Telnet
25	Simple Mail Transfer Protocol (SMTP)
53	Domain Name Services (DNS)
67 and 68	Dynamic Host Configuration Protocol (DHCP)
80	Hypertext Transfer Protocol (HTTP)
110	Post Office Protocol (POP3)
161	Simple Network Management Protocol (SNMP)
194	IRC chat port (used for device sharing)
443	HTTP over SSL
8080	Used for proxy services

Select Commonly Used Port Numbers

Firewall Analysis Tools

- Understanding exactly where an organization's firewall is located and what the existin rule sets on the firewall do are very important steps for any security administrator.
- There are several tools that automate the remote discovery of firewall rules and assist the administrator (or attacker) in analyzing the rules to determine exactly what they allow and what they reject.
- The ***Nmap tool*** mentioned earlier has some advanced options that are useful for firewall analysis. The Nmap option called idle scanning (which is run with the -I switch) will allow the Nmap user to bounce your scan across a firewall by using one of the idle DMZ hosts as the initiator of the scan.
- Another tool that can be used to analyze firewalls is ***Firewalk***. Written by noted author and network security expert Mike Schiffman, Firewalk uses incrementing Time-To-Live (TTL) packets to determine the path into a network as well as the default firewall policy. Running

Firewalk against a target machine reveals where routers and firewalls are filtering traffic to the target host.

- A final firewall analysis tool worth mentioning is HPING, which is a modified ping client. It supports multiple protocols and has a command-line method of specifying nearly any of the ping parameters.

Operating System Detection Tools

- Detecting a target computer's operating system is very valuable to an attacker, because once the OS is known, all of the vulnerabilities to which it is susceptible can easily be determined.
- There are many tools that use networking protocols to determine a remote computer's OS. One specific tool worth mentioning is *XProbe*, which uses ICMP to determine the remote OS.
- When run, *XProbe* sends many different ICMP queries to the target host. As reply packets are received, XProbe matches these responses from the target's TCP/IP stack with its own internal database of known responses.
- Because most OSs have a unique way of responding to ICMP requests, Xprobe is very reliable in finding matches and thus detecting the operating systems of remote computers.

Vulnerability Scanners

- ***Active vulnerability*** scanners scan networks for highly detailed information. An active scanner is one that initiates traffic on the network in order to determine security holes. As a class, this type of scanner identifies exposed usernames and groups, shows open network shares, and exposes configuration problems and other vulnerabilities in servers.
- Example : LANguard , Nessus
- A ***passive vulnerability*** scanner is one that listens in on the network and determines vulnerable versions of both server and client software.
- At the time of this writing, there are two primary vendors offering this type of scanning solution: Tenable Network Security with its Passive Vulnerability Scanner (PVS) and Sourcefire with its RNA product.
- Passive scanners are advantageous in that they do not require vulnerability analysts to get approval prior to testing. These tools simply monitor the network connections to and from a server to obtain a list of vulnerable applications.

Packet Sniffers

- A packet sniffer (sometimes called a network protocol analyzer) is a network tool that collects copies of packets from the network and analyzes them. It can provide a network administrator with valuable information for diagnosing and resolving networking issues.
- To use a packet sniffer legally, the administrator must
  (1) be on a network that the organization owns,
  (2) be under direct authorization of the owners of the network, and
  (3) have knowledge and consent of the content creators.
- If all three conditions are met, the administrator can selectively collect and analyze packets to identify and diagnose problems on the network. Conditions one and two are self-explanatory.
- The third, consent, is usually handled by having all system users sign a release when they are issued a user ID and passwords. Incidentally, these three items are the same requirements for employee monitoring in general, and packet sniffing should be construed as a form of employee monitoring

Wireless Security Tools

- 802.11 wireless networks have sprung up as subnets on nearly all large networks. A wireless connection, while convenient, has many potential security holes.
- An organization that spends all of its time securing the wired network and leaves wireless networks to operate in any manner is opening itself up for a security breach. As a security professional, you must assess the risk of wireless networks.
- AirSnare is a free tool that can be run on a low-end wireless workstation. AirSnare monitors the airwaves for any new devices or access points. When it finds one, AirSnare sounds an alarm alerting the administrators that a new, potentially dangerous, wireless apparatus is attempting access on a closed wireless network.

5.5 CRYPTOGRAPHY

- Cryptography, which comes from the Greek words kryptos, meaning “hidden,” and graphein, meaning “to write,” is the process of making and using codes to secure the transmission of information.
- Cryptanalysis is the process of obtaining the original message (called the plaintext) from an encrypted message (called the ciphertext) without knowing the algorithms and keys used to perform the encryption.
- *Encryption* is the process of converting an original message into a form that is unreadable to unauthorized individuals—that is, to anyone without the tools to convert the encrypted message back to its original format.
- *Decryption* is the process of converting the ciphertext message back into plaintext so that it can be readily understood.

Terminology

- **Algorithm**: the mathematical formula used to convert an unencrypted message into an encrypted message.
- **Cipher:** the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components.
- **Ciphertext or cryptogram:** the unintelligible encrypted or encoded message resulting from an encryption.
- **Code:** the transformation of the larger components (words or phrases) of an unencrypted message into encrypted components.
- **Cryptosystem:** the set of transformations necessary to convert an unencrypted message into an encrypted message.
- **Decipher:** to decrypt or convert ciphertext to plaintext.
- **Encipher:** to encrypt or convert plaintext to ciphertext.
- **Key or cryptovariable:** the information used in conjunction with the algorithm to create ciphertext from plaintext.
- **Keyspace**: the entire range of values that can possibly be used to construct an individual key.
- Link encryption: a series of encryptions and decryptions between a numbers of systems, whereby each node decrypts the message sent to it and then re-encrypts it using different keys and sends it to the next neighbour, until it reaches the final destination.

- **Plaintext:** the original unencrypted message that is encrypted and results from successful decryption.
- **Steganography:** the process of hiding messages in a picture or graphic.
- **Work factor:** the amount of effort (usually in hours) required to perform cryptanalysis on an encoded message.

5.5.1 Cipher Methods

- There are two methods of encrypting plaintext: the bit stream method or the block cipher method.
- In the *bit stream method*, each bit in the plaintext is transformed into a cipher bit one bit at a time.
- In the *block cipher method*, the message is divided into blocks, for example, sets of 8-, 16-, 32-, or 64-bit blocks, and then each block of plaintext bits is transformed into an encrypted block of cipher bits using an algorithm and a key.
- Bit stream methods commonly use algorithm functions like the exclusive OR operation (XOR), whereas block methods can use substitution, transposition, XOR, or some combination of these operations are
    - Substitution Cipher
    - Transposition Cipher
    - Exclusive OR
    - Vernam Cipher
    - Book or Running Key Cipher
    - Hash Functions

Substitution Cipher

- To use a substitution cipher, you substitute one value for another
- For example a letter in the alphabet with the letter three values to the right. Or you can substitute one bit for another bit that is four places to its left. A three-character substitution to the right results in the following transformation of the standard English alphabet:

Initial alphabet yields	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Encryption alphabet	DEFGHIJKLMNOPQRSTUVWXYZABC

- Within this substitution scheme, the plaintext MOM would be encrypted into the ciphertext PRP.

- This type of substitution is based on a ***monoalphabetic substitution,*** because it only uses one alphabet.
- More advanced substitution ciphers use two or more alphabets, and are referred to as ***polyalphabetic substitutions.***
- To extend the previous example, consider the following block of text:

Plaintext	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Substitution cipher 1	DEFGHIJKLMNOPQRSTUVWXYZABC
Substitution cipher 2	GHIJKLMNOPQRSTUVWXYZABCDEF
Substitution cipher 3	JKLMNOPQRSTUVWXYZABCDEFGHI
Substitution cipher 4	MNOPQRSTUVWXYZABCDEFGHIJKL

- The first row here is the plaintext, and the next four rows are four sets of substitution ciphers, which taken together constitute a single polyalphabetic substitution cipher.
- To encode the word TEXT with this cipher, you substitute a letter from the second row for the first letter in TEXT, a letter from the third row for the second letter, and so on—a process that yields the ciphertext WKGF. Note how the plaintext letter T is transformed into a W or a F, depending on its order of appearance in the plaintext.

Transposition Cipher

- The transposition cipher (or permutation cipher) simply rearranges the values within a block to create the ciphertext. This can be done at the bit level or at the byte (character) level. For an example, consider the following transposition key pattern.

Key pattern: 1 →4, 2→ 8, 3→ 1, 4 →5, 5→ 7, 6 →2, 7 →6, 8 →3

- In this key, the bit or byte (character) in position 1 (with position 1 being at the far right) moves to position 4 (counting from the right), and the bit or byte in position 2 moves to position 8, and so on.
- The following rows show the numbering of bit locations for this key; the plaintext message 00100101011010111001010101010100, which is broken into 8-bit blocks for clarity; and the ciphertext that is produced when the transposition key depicted above is applied to the plaintext:

Bit locations:	87654321 87654321 87654321 87654321
Plaintext 8-bit blocks:	00100101|01101011|10010101|01010100
Ciphertext:	00001011|10111010|01001101|01100001

Exclusive OR

- The exclusive OR operation (XOR) is a function of Boolean algebra in which two bits are compared, and if the two bits are identical, the result is a binary 0.
- If the two bits are not the same, the result is a binary 1. XOR encryption is a very simple symmetric cipher that is used in many applications where security is not a defined requirement. Table shows an XOR truth table with the results of all the possible combinations of two bits.

First Bit	Second Bit	Result
0	0	0
0	1	1
1	0	1
1	1	0

XOR Truth Table

- To see how XOR works, consider an example in which the plaintext is the word "CAT." The ASCII binary representation of the plaintext is "01000011 01000001 01010100". In order to encrypt the plaintext, a key value should be selected. In this case, the bit pattern for the letter "V" (01010110) is used, and is repeated for each character to be encrypted, written.

Text Value	Binary Value
CAT as bits	0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 1 0 1 0 1 0 0
VVV as key	0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0 0 1 0 1 0 1 1 0
Cipher	0 0 0 1 0 1 0 1 0 0 0 1 0 1 1 1 0 0 0 0 0 0 1 0

Example XOR Encryption

Vernam cipher

- Vernam cipher, which was developed by AT&T, uses a set of characters only one time for each encryption process (hence the name one-time pad). The pad in the name comes from the days of manual encryption and decryption when the key values for each ciphering session were prepared by hand and bound into an easy-to-use form—that is, a pad of paper.

- To perform the Vernam cipher encryption operation, the pad values are added to numeric values that represent the plaintext that needs to be encrypted.
- Each character of the plaintext is turned into a number and a pad value for that position is added to it.
- The resulting sum for that character is then converted back to a ciphertext letter for transmission. If the sum of the two values exceeds 26, then 26 is subtracted from the total.
- To examine the Vernam cipher and its use of modulo, consider the following example, which uses "SACK GAUL SPARE NO ONE" as plaintext.
- In the first step of this encryption process, the letter "S" is converted into the number 19 (because it is the nineteenth letter of the alphabet), and the same conversion is applied to the rest of the letters of the plaintext message, as shown below

Plaintext:	S	A	C	K	G	A	U	L	S	P	A	R	E	N	O	O	N	E
Plaintext value:	19	01	03	11	07	01	21	12	19	16	01	18	05	14	15	15	14	05
One-time pad text:	F	P	Q	R	N	S	B	I	E	H	T	Z	L	A	C	D	G	J
One time pad value:	06	16	17	18	14	19	02	09	05	08	20	26	12	01	03	04	07	10
Sum of plaintext and pad:	25	17	20	29	21	20	23	21	24	24	21	44	17	15	18	19	21	15
After modulo Subtraction:				03								18						
Ciphertext:	Y	Q	T	C	U	T	W	U	X	X	U	R	Q	O	R	S	U	O

Book or Running Key Cipher

- One encryption method made popular by spy movies involves using the text in a book as the key to decrypt a message. The ciphertext consists of a list of codes representing the aapage number, line number, and word number of the plaintext word.
- The algorithm is the mechanical process of looking up the references from the ciphertext and converting each reference to a word by using the ciphertext's value and the key (the book).

Hash Functions

- In addition to ciphers, another important encryption technique that is often incorporated into cryptosystems is the hash function. Hash functions are mathematical algorithms that generate a message summary or digest (sometimes called a fingerprint) to confirm the identity of a specific message and to confirm that there have not been any changes to the content.
- While they do not create a ciphertext, hash functions confirm message identity and integrity, both of which are critical functions in e-commerce.

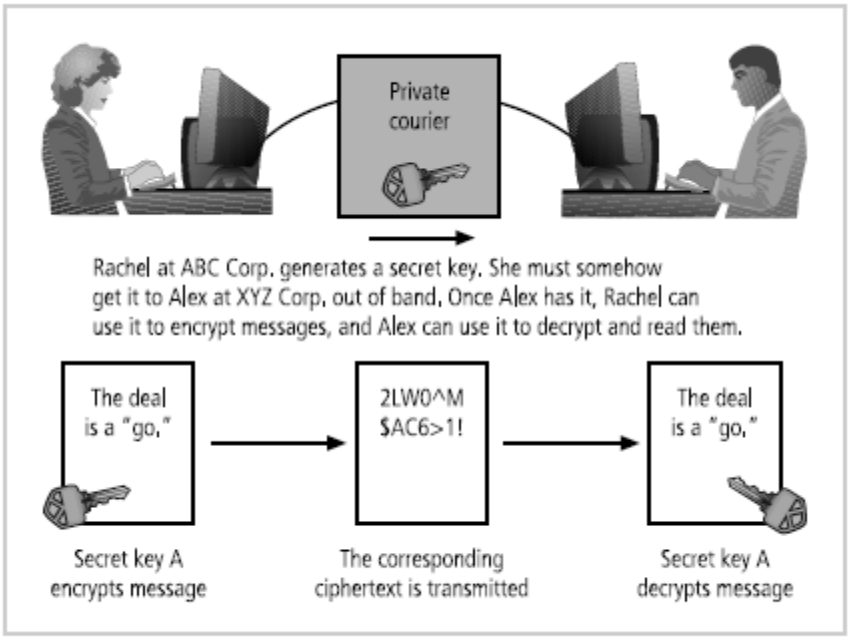
- Hash algorithms are public functions that create a hash value, also known as a message digest, by converting variable-length messages into a single fixed-length value. The message digest is a fingerprint of the author's message that is compared with the recipient's locally calculated hash of the same message. If both hashes are identical after transmission, the message has arrived without modification. Hash functions are considered one-way operations in that the same message always provides the same hash value, but the hash value itself cannot be used to determine the contents of the message.

5.5.2 Cryptographic Algorithms

- Cryptographic algorithms are often grouped into two broad categories—symmetric and asymmetric—but in practice, today's popular cryptosystems use a hybrid combination of symmetric and asymmetric algorithms.
- Symmetric and asymmetric algorithms are distinguished by the types of keys they use for encryption and decryption operations.

Symmetric Encryption

- Encryption methodologies that require the same secret key to encipher and decipher the message are using what is called *private key encryption or symmetric encryption*.



Example of Symmetric Encryption

- Symmetric encryption methods use mathematical operations that can be programmed into extremely fast computing algorithms so that the encryption and decryption processes are executed quickly by even small computers.
- Two types of popular symmetric encryption cryptosystems, they are
    1. Data Encryption Standard (DES)
    2. Triple DES (3DES)

Data Encryption Standard (DES)

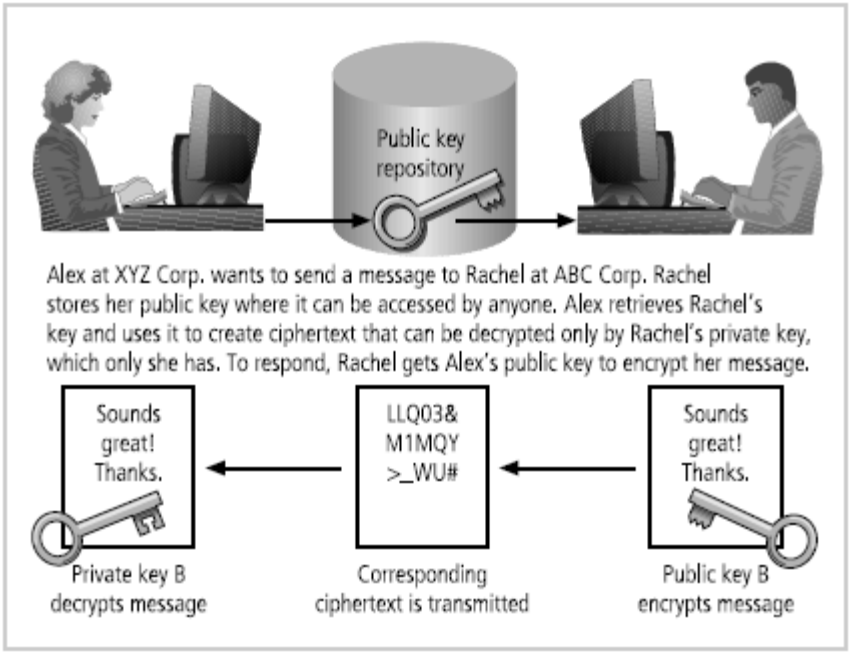
- Data Encryption Standard (DES), which was developed by IBM and is based on the company's Lucifer algorithm, which uses a key length of 128 bits. As implemented, DES uses a 64-bit block size and a 56-bit key.
- DES was adopted by NIST in 1976 as a federal standard for encryption of non-classified information, after which it became widely employed in commercial applications.
- DES enjoyed increasing popularity for almost twenty years, until 1997, when users realized that a 56-bit key size did not provide acceptable levels of security. In 1998, a group called the Electronic Frontier Foundation (www.eff.org), using a specially designed computer, broke a DES key in less than three days (just over 56 hours, to be precise).
- Since then, it has been theorized that a dedicated attack supported by the proper hardware (not necessarily a specialized computer) can break a DES key in less than four hours.

Triple DES

- Triple DES (3DES) was created to provide a level of security far beyond that of DES.
- 3DES was an advanced application of DES, and while it did deliver on its promise of encryption strength beyond DES, it too soon proved too weak to survive indefinitely—especially as computing power continued to double every 18 months. Within just a few years, 3DES needed to be replaced.
- The successor to 3DES is the Advanced Encryption Standard (AES). AES is a federal information processing standard (FIPS) that specifies a cryptographic algorithm used within the U.S. government to protect information in federal agencies that are not a part of the national defense infrastructure.

Asymmetric Encryption

- While symmetric encryption systems use a single key to both encrypt and decrypt a message, asymmetric encryption uses two different but related keys, and either key can be used to encrypt or decrypt the message.
- If, however, key A is used to encrypt the message, only key B can decrypt it, and if key B is used to encrypt a message, only key A can decrypt it.
- Asymmetric encryption can be used to provide elegant solutions to problems of secrecy and verification. This technique has its highest value when one key is used as a private key, which means that it is kept secret (much like the key in symmetric encryption), known only to the owner of the key pair, and the other key serves as a public key, which means that it is stored in a public location where anyone can use it.
- This is why the more common name for asymmetric encryption is public-key encryption.



Example of Asymmetric Encryption

- One of the most popular public key cryptosystems is RSA, whose name is derived from Rivest-Shamir-Adleman, the algorithm's developers.
- The RSA algorithm was the first public key encryption algorithm developed (in 1977) and published for commercial use. It is very popular and has been embedded in both Microsoft and Netscape Web browsers to enable them to provide security for e-commerce applications.
- The patented RSA algorithm has in fact become the de facto standard for public-use encryption applications. To learn how this algorithm works, see the Technical Details box entitled "RSA Algorithm.

The sender publishes the public key, which consists of modulus n and exponent e. The remaining variables d, p, and q are kept secret.

A message can then be encrypted by:	$C = M^e$ (recipient) mod n(recipient)
Digitally signed by:	$C' = M'^d$ (sender) mod n(sender)
Verified by:	$M' = C'^e$ (sender) mod n(sender)
Decrypted by:	$M = C^d$ (recipient) mod n(recipient)

Examples

The following sections contain practice examples to help you better understand the machinations of the RSA algorithms.

RSA Algorithm Example:[7] Work through the following steps to better understand how the RSA algorithm functions:

1. Choose two large, random prime numbers: P, Q (usually P, Q > 10^100) → This means 10 to the power 100.
2. Compute:
   $N = P \times Q$
   $Z = (P - 1Q - 1)$
3. Choose a relatively prime number with Z and call it D.
   D < N; relatively prime means that D and Z have no common factors except 1.
4. Find number E, such that → $E \times D = 1$ mod Z.
5. The public key is (N, E); the private key is (N, D).
6. Create cipher (encrypted text):
   C = | TEXT |E (MOD N)
   C → Encrypted text → this is the text that is transmitted
   | TEXT | → Plaintext to be encrypted (its numerical correspondent)
7. Decrypt the message:
   D = Plaintext = CD (MOD N), C = Ciphertext from part 6.

Note that it is almost impossible to obtain the private key, knowing the public key, and it's almost impossible to factor N into P and Q.

Encryption Key Size

- When using ciphers, size of cryptovariable or key is very important
- Strength of many encryption applications and cryptosystems measured by key size
- For cryptosystems, security of encrypted data is not dependent on keeping encrypting algorithm secret
- Cryptosystem security depends on keeping some or all of elements of cryptovariable(s) or key(s) secret

Key Length (bits)	Maximum Number of Operations (guesses)	Maximum Time to Crack	Estimated Average Time to Crack
8	256	0.0000000085 seconds	0.0000000043 seconds
16	65,636	0.0000022 seconds	0.00000109 seconds
24	16,777,216	0.00056 seconds	0.00028 seconds
32	4,294,967,296	0.143 seconds	0.072 seconds
56	72,057,594,037,927,900	27.800 days	13.9 days
64	18,446,744,073,709,600,000	19.498 years	9.7 years
128	3.40282E+38	359,676,102,360,201, 000,000 years	179,838,051,180,100, 000,000 years
256	1.15792E+77	122,391,435,436,027, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years	61,195,717,718,013,400, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000 years
512	1.3408E+154	14,171,960,013,891,600, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years	7,085,980,006,945,820, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000, 000,000,000,000,000 years

Encryption Key Power

5.5.3 Cryptographic Tools

Public Key Infrastructure (PKI):

- Integrated system of software, encryption methodologies, protocols, legal agreements, and third-party services enabling users to communicate securely
- PKI systems based on public-key cryptosystems; include digital certificates and certificate authorities (CAs)
- PKI protects information assets in several ways:
  - Authentication
  - Integrity
  - Privacy
  - Authorization
  - Nonrepudiation

- When an asymmetric cryptographic process uses the sender's private key to encrypt a message, the sender's public key must be used to decrypt the message when the decryption happens successfully, it provides verification that the message was sent by the sender and cannot be refuted.
- This is known as non-repudiation, which is the foundation of digital signatures.
- Digital signatures are encrypted messages that are independently verified by a central facility (registry) as authentic.

Digital Signatures

- Digital signatures were created in response to the rising need to verify information transferred via electronic systems.
- Asymmetric encryption processes are used to create digital signatures. When an asymmetric cryptographic process uses the sender's private key to encrypt a message, the sender's public key must be used to decrypt the message.
- When the decryption is successful, the process verifies that the message was sent by the sender and thus cannot be refuted. This process is known as nonrepudiation and is the principle of cryptography that underpins the authentication mechanism collectively known as a digital signature.
- Digital signatures are, therefore, encrypted messages that can be mathematically proven authentic.

Digital Certificates

- As you learned earlier in this chapter, a digital certificate is an electronic document or container file that contains a key value and identifying information about the entity that controls the key. The certificate is often issued and certified by a third party, usually a certificate authority.
- A digital signature attached to the certificate's container file certifies the file's origin and integrity. This verification process often occurs when you download or update software via the Internet.
- Different client-server applications use different types of digital certificates to accomplish their assigned functions, as follows:
- The CA application suite issues and uses certificates (keys) that identify and establish a trust relationship with a CA to determine what additional certificates (keys) can be authenticated.

- Mail applications use Secure/Multipurpose Internet Mail Extension (S/MIME) certificates for signing and encrypting e-mail as well as for signing forms.
- Development applications use object-signing certificates to identify signers of object oriented code and scripts.
- Web servers and Web application servers use Secure Sockets Layer (SSL) certificates to authenticate servers via the SSL protocol (which is described shortly) in order to establish an encrypted SSL session.
- Web clients use client SSL certificates to authenticate users, sign forms, and participate in single sign-on solutions via SSL.

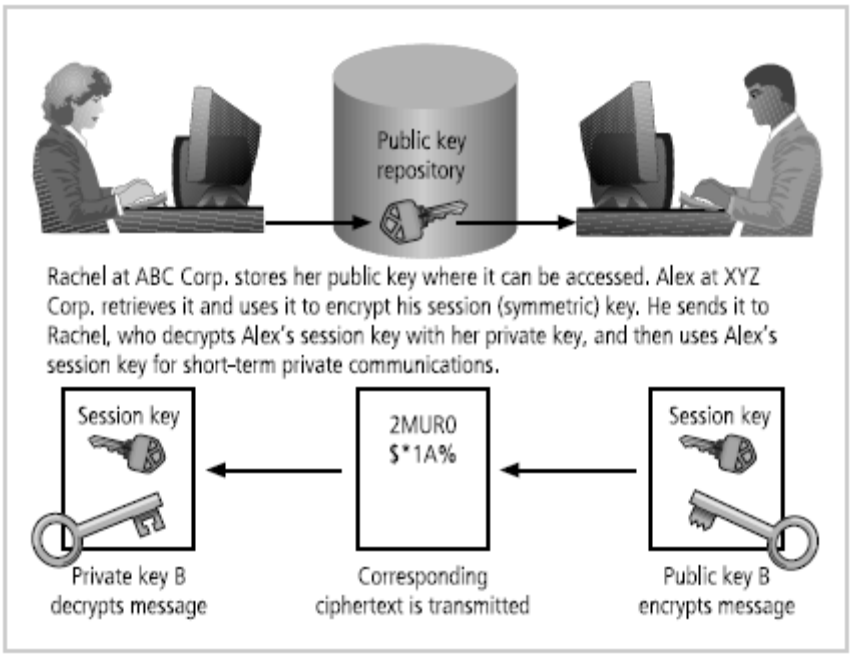
X.509 v3 Certificate Structure
Version
Certificate Serial Number
Algorithm ID • Algorithm ID • Parameters
Issuer Name
Validity • Not Before • Not After
Subject Name
Subject Public Key Info • Public Key Algorithm • Parameters • Subject Public Key
Issuer Unique Identifier (Optional)
Subject Unique Identifier (Optional)
Extensions (Optional) • Type • Criticality • Value
Certificate Signature Algorithm
Certificate Signature

X.509 v3 Certificate Structure[11]

Hybrid Cryptography Systems

- Except with digital certificates, pure asymmetric key encryption not widely used
- Asymmetric encryption more often used with symmetric key encryption, creating hybrid system

- Diffie-Hellman Key Exchange method: most common hybrid system; provided foundation for subsequent developments in public-key encryption.



Example of Hybrid Encryption

Steganography

- The word steganography—the art of secret writing—is derived from the Greek words steganos, meaning "covered" and graphein, meaning "to write."
- Process of hiding information; in use for a long time
- Most popular modern version hides information within files appearing to contain digital pictures or other images
- Some applications hide messages in .bmp, .wav, .mp3, and .au files, as well as in unused space on CDs and DVDs.

5.5.4 Attacks on cryptosystems

- Attempts to gain unauthorized access to secure communications have typically used brute force attacks (ciphertext attacks)
- Attacker may alternatively conduct known-plaintext attack or selected-plaintext attach schemes

Man-in-the-Middle Attack

- Designed to intercept transmission of public key or insert known key structure in place of requested public key

- From victim's perspective, encrypted communication appears to be occurring normally, but in fact attacker receives each encrypted message, decodes, encrypts, and sends to originally intended recipient
- Establishment of public keys with digital signatures can prevent traditional man-in-the-middle attack

Correlation Attacks

- Collection of brute-force methods that attempt to deduce statistical relationships between structure of unknown key and ciphertext
- Differential and linear cryptanalysis have been used to mount successful attacks
- Only defense is selection of strong cryptosystems, thorough key management, and strict adherence to best practices of cryptography in frequency of changing keys

Timing Attacks

- Attacker eavesdrops during victim's session; uses statistical analysis of user's typing patterns and inter-keystroke timings to discern sensitive session information
- Can be used to gain information about encryption key and possibly cryptosystem in use
- Once encryption successfully broken, attacker may launch a replay attack (an attempt to resubmit recording of deciphered authentication to gain entry into secure source)

Defending Against Attacks

- No matter how sophisticated encryption and cryptosystems have become, if key is discovered, message can be determined
- Key management is not so much management of technology but rather management of people.

5.6 ACCESS CONTROL DEVICES

- A successful access control system includes a number of components, depending on the system's needs for authentication and authorization.
- Strong authentication requires at least two of the forms of authentication listed below to authenticate the supplicant's identity. A second factor that is required to verify the supplicant's identify is frequently a physical device.
- The technology to manage authentication based on what a supplicant knows is widely integrated into the networking and security software systems in use across the IT industry.

Authentication

- Authentication is the validation of a user's identity.
- There are four general forms of authentication to consider:
- What a user knows.
- What a user has.
- What a user is.
- What a user produces.

What a User Knows

- A password is a private word or combination of characters that only the user should know.
- One of the biggest debates in the information security industry concerns the complexity of passwords. A password should be difficult to guess but must be something the user can easily remember.
- A passphrase is a series of characters, typically longer than a password, from which a virtual password is derived.

What a User Has

- The second area of authentication addresses something the user carries in his or her possession—that is, something they have.
- These include dumb cards, such as ID cards or ATM cards with magnetic stripes that contain the digital (and often encrypted) user personal identification number (PIN), against which the number a user inputs is compared.

- An improved version of the dumb card is the smart card, which contains a computer chip that can verify and validate a number of pieces of information instead of just a PIN.

What a User Has

- Another device often used is the token, a card or key fob with a computer chip and a liquid crystal display that shows a computer-generated number used to support remote login authentication. Tokens are synchronous or asynchronous.
- Once synchronous tokens are synchronized with a server, both devices (server and token) use the same time or a time-based database to generate a number that is displayed and entered during the user login phase.
- Asynchronous tokens use a challenge-response system, in which the server challenges the user during login with a numerical sequence.

Biometric Access Controls

- Biometric access control is based on the use of some measurable human characteristic or trait to authenticate the identity of a proposed systems user (a supplicant). It relies upon recognition—the same thing you rely upon to identify friends, family, and other people you know. The use of biometric-based authentication is expected to have a significant impact in the future as technical and ethical issues with the technology are resolved.
- The process of using body measurements is known as biometrics and includes:
  - Fingerprint comparison of the user's actual fingerprint to a stored fingerprint.
  - Palm print comparison of the user's actual palm print to a stored palm print.
  - Hand geometry comparison of the user's actual hand to a stored measurement.
  - Facial recognition using a photographic ID card, in which a human security guard compares the user's face to a photo.
  - Facial recognition using a digital camera, in which a user's face is compared to a stored image.
  - Retinal print comparison of the user's actual retina to a stored image.
  - Iris pattern comparison of the user's actual iris to a stored image.
- Among all possible biometrics, only three human characteristics are usually considered truly unique:
  - Fingerprints
  - Retina of the eye (blood vessel pattern)

  - Iris of the eye (random pattern of features in the iris: freckles, pits, striations, vasculature, coronas, and crypts)
- Most of the technologies that scan human characteristics convert these images to some form of minutiae, which are unique points of reference that are digitized and stored in an encrypted format when the user's system access credentials are created.

What a User Produces

- The fourth and final area of authentication includes signature recognition and voice recognition.
- Retail stores use signature recognition, or at least signature capture, for authentication during a purchase.
- Currently, the technology for signature capturing is much more widely accepted than that for signature comparison, because signatures change due to a number of factors, including age, fatigue, and the speed with which the signature is written.
- In voice recognition, an initial voiceprint of the user reciting a phrase is captured and stored.
- Later, when the user attempts to access the system, the authentication process will require the user to speak this same phrase so that the technology can compare the current voiceprint against the stored value.

Effectiveness of Biometrics

- Biometric technologies are evaluated on three basic criteria:
- **The false reject rate**: The rate at which users who are authentic users are denied or prevented access to authorized areas as a result of a failure in the biometric device (Type I error).
- **The false accept rate:** The rate at which users who are not legitimate users are allowed access to systems or areas as a result of a failure in the biometric device (Type II error).
- **The crossover error rate (CER):** The level at which the number of false rejections equals the number of false acceptances (equal error rate). This is the most common and important overall measure of the accuracy of a biometric system.

Acceptability of Biometrics

- A balance must be struck between how acceptable a security system is to its users and how effective it is in maintaining security.
- Many the biometric systems that are highly reliable and effective are considered somewhat intrusive to users.

- As a result, many information security professionals, in an effort to avoid confrontation and possible user boycott of the biometric controls, don't implement them.

5.7 PHYSICAL SECURITY

- Physical security encompasses the design, implementation, and maintenance of countermeasures that protect the physical resources of an organization, including the people, hardware, and supporting system elements and resources that control information in all its states (transmission, storage, and processing).
- Most technology-based controls can be circumvented if an attacker gains physical access to the devices being controlled.
- Some computer systems are constructed in such a way that it easy to steal the hard drive and the information it contains.
- As a result, physical security should receive as much attention as logical security in the security development life cycle.

Seven Major Sources of Physical Loss

1. Extreme temperature: heat, cold
2. Gases: war gases, commercial vapors, humid or dry air, suspended particles
3. Liquids: water, chemicals
4. Living organisms: viruses, bacteria, people, animals, insects
5. Projectiles: tangible objects in motion, powered objects
6. Movement: collapse, shearing, shaking, vibration, liquefaction, flows waves, separation, slide
7. Energy anomalies: electrical surge or failure, magnetism, static electricity, aging circuitry; radiation: sound, light, radio, microwave, electromagnetic, atomic.

- General management: responsible for the security of the facility in which the organization is housed and the policies and standards for secure operation.
- IT management and professionals: responsible for environmental and access security in technology equipment locations and for the policies and standards of secure equipment operation.
- Information security management and professionals: perform risk assessments and implementation reviews for the physical security controls implemented by the other two groups.

1. Access Controls

- There are a number of physical access controls that are uniquely suited to the physical entry and exit of people to and from the organization's facilities, including biometrics, smart cards and wireless enabled keycards.

Facilities Management

- Before examining access controls, understand the concept of a secure facility and its design.
- From the point of view of facilities management, a secure facility is a physical location that has been engineered with controls designed to minimize the risk of attacks from physical threats.
- A secure facility can use the natural terrain; traffic flow, urban development, and can complement these features with protection mechanisms, such as fences, gates, walls, guards, and alarms.

Controls for Protecting the Secure Facility

- There are a number of physical security controls and issues that the organization's communities of interest should consider together when implementing physical security:
  - Walls, Fencing, and Gates.
  - Guards to apply human reasoning.
  - Dogs to provide their keen sense of smell and hearing and to be placed in harms way in lieu of humans.
  - ID Cards and Badges
  - Locks and Keys
  - Mantraps
  - Electronic Monitoring
  - Alarms and Alarm Systems
  - Computer Rooms
  - Walls and Doors

ID Cards and Badges

- One area of access control that ties physical security with information access control is the use of identification cards (ID) and name badges. An ID card is typically worn concealed, whereas a name badge is visible. These devices are forms of biometrics (facial recognition) to identify and authenticate an authorized individual with access to the facility.

Locks and Keys

- There are two types of locks: mechanical and electro-mechanical.
- The mechanical lock relies on a key of carefully shaped pieces of metal that turn tumblers to release secured loops of steel, aluminum, or brass (in brass padlocks).
- The electro-mechanical lock can accept a variety of inputs including keys that are magnetic strips on ID Cards, radio signals from name badges, PINs typed into a keypad.Locks are divided into four categories: manual, programmable, electronic, and biometric.
- As part of general management's responsibility for the physical environment, the management of keys and locks is a fundamental concern. Sometimes locks fail and facilities need alternative procedures for access.
- Locks fail in one of two ways: when the lock of a door fails and the door becomes unlocked, that is a fail-safe lock; when the lock of a door fails and the door remains locked, this is a fail-secure lock.

Mantraps

- A mantrap is a small enclosure that has an entry point and a different exit point. The individual entering the facility, area, or room, enters the mantrap, requests access through some form of electronic or biometric lock and key, and if verified, is allowed to exit the mantrap into the facility.
- This is called a mantrap, because if the individual is denied entry, the mantrap does not allow exit until a security official overrides the automatic locks of the enclosure.

Electronic Monitoring

- Used to record events within a specific area or areas where other types of physical controls are not practical. Monitoring frequently uses cameras viewing individuals, while on the other end of these cameras are video cassette recorders and related machinery that captures the video feed.
- These systems have drawbacks as for the most part they are reactive and do not prevent access or prohibited activity. Recorded monitoring requires an individual to review the information collected.

Alarms and Alarm Systems

- Alarm systems notify appropriate individuals when a predetermined event or activity occurs.

- This could be a fire, a break-in or intrusion, an environmental disturbance, such as flooding, or an interruption in services, such as a loss of power.
- Burglar alarm systems detect intrusions into unauthorized areas and notify either a local or remote security agency to react. These systems rely on a number of sensors that detect the intrusion: motion detectors, thermal detectors, glass breakage detectors, weight sensors, and contact sensors.

Computer Rooms and Wiring Closets

- Computer rooms and wiring and communications closets are facilities that require special attention to ensure the confidentiality, integrity, and availability of information.
- Logical access controls are easily defeated, if an attacker gains physical access to the computing equipment. Custodial staff are often the least scrutinized of employees and non-employees who have access to offices. Yet custodians are given the greatest degree of unsupervised access.

Interior Walls and Doors

- The security of information assets can sometimes be compromised because of the construction of the walls and doors of the facility. The walls in a facility are typically: standard interior or firewall.
- All high-security areas, such as computer rooms and wiring closets, must have firewall grade walls surrounding them.

2. Fire Safety

- The most serious threat to physical security and the safety of the people who work in the organization is the possibility of fire. Fires account for more property damage, personal injury, and death than any other threat to physical security.
- As a result, it is imperative that physical security plans examine and implement strong measures to detect and respond to fires and fire hazards.

Fire Detection and Response

- Fire suppression systems are devices installed and maintained to detect and respond to a fire, potential fire, or combustion situation.

- These devices typically work to deny an environment of one of the three requirements for a fire to burn: temperature, fuel, and oxygen. Water and water mist systems reduce the temperature of the flame to extinguish it and to saturate some categories of fuels to prevent ignition.
- Carbon dioxide systems rob fire of its oxygen. Soda acid systems deny fire its fuel, preventing spreading. Gas-based systems disrupt the fires chemical reaction but leave enough oxygen for people to survive for a short time. Before a fire can be suppressed, it must be detected.
- Fire detection systems fall into two general categories: manual and automatic.
- Manual fire detection systems include human responses, such as calling the fire department, as well as manually activated alarms, such as sprinklers and gaseous systems. During the chaos of a fire evacuation, an attacker can easily slip into offices and obtain sensitive information.
- As part of a complete fire safety program, it is advisable to designate individuals as floor monitors. There are three basic types of fire detection systems: thermal detection, smoke detection, and flame detection.

The thermal detection systems contain a sophisticated heat sensor that operates in one of two ways, fixed temperature, and rate-of-rise. Smoke-detection systems are perhaps the most common means of detecting a potentially dangerous fire, and are required by building codes:

Smoke detectors operate in one of three ways:

1. Photoelectric sensors project and detect an infrared beam, if interrupted activates alarm or suppression systems.
2. Ionization sensors contains a small amount of a harmless radioactive material within a detection chamber. When certain by-products of combustion enter, a change in the level of electrical conductivity activates the detector.
3. Air-aspirating detectors take in air, filtering it, and moving it through a chamber containing a laser beam. If the laser beam is diverted or refracted by smoke particles, the system is activated.

- The flame detector is a sensor that detects the infrared or ultraviolet light produced by an open flame. These systems require direct line-of-sight with the flame and compare the flame signature to a database to determine whether or not to activate the alarm and suppression systems.
- While highly sensitive, flame detection systems are expensive and must be installed where they can scan all areas of the protected area.

Fire Suppression

- Fire suppression systems can consist of portable, manual, or automatic apparatus. Portable extinguishers are rated by the type of fire:
    - **Class A:** fires of ordinary combustible fuels. Use water and multi-purpose, dry chemical fire extinguishers.
    - **Class B:** fires fuelled by combustible liquids or gases, such as solvents, gasoline, paint, lacquer, and oil. Use carbon dioxide, multi-purpose dry chemical and Halon fire extinguishers.
    - **Class C:** fires with energized electrical equipment or appliances. Use carbon dioxide, multi-purpose, dry chemical and Halon fire extinguishers.
    - **Class D:** fires fueled by combustible metals, such as magnesium, lithium, and sodium. Use special extinguishing agents and techniques.
- Manual and automatic fire response can include installed systems designed to apply suppressive agents. These are usually either sprinkler or gaseous systems.
- All sprinkler systems are designed to apply liquid, usually water, to all areas in which a fire has been detected. In sprinkler systems, the organization can implement wet pipe, dry pipe, or pre-action systems.
- Water mist sprinklers are the newest form of sprinkler systems and rely on micro-fine mists instead of traditional shower-type systems. Chemical gas systems can be used in the suppression of fires. Until recently there were only two major types of gaseous systems: carbon dioxide and Halon. Carbon dioxide robs a fire of its oxygen supply.
- Halon is a clean agent, which means that it does not leave any residue when dry, nor does it interfere with the operation of electrical or electronic equipment. Unfortunately the EPA has classified Halon as an ozone-depleting substance, and therefore new installations are prohibited.

3. Failure of Supporting Utilities and Structural Collapse

- Supporting utilities, such as heating, ventilation and air conditioning, power, water, and other utilities, have a significant impact on the continued safe operation of a facility.
- Extreme temperatures and humidity levels, electrical fluctuations and the interruption of water, sewage, and garbage services can create conditions that inject vulnerabilities in systems designed to protect information.

Heating, Ventilation, and Air Conditioning

- Although traditionally a facilities management responsibility, the operation of the heating, ventilation, and air conditioning (HVAC) system can have dramatic impact on information and information systems operations and protection.
- Specifically there are four areas within the HVAC system that can cause damage to information-carrying systems: temperature, filtration, humidity, and static electricity.

Temperature

- Computer systems are electronic and as such are subject to damage from extreme temperature.
- Rapid changes in temperature, from hot to cold, or from cold to hot can produce condensation, which can create short circuits or otherwise damage systems and components.
- The optimal temperature for a computing environment (and people) is between 70 and 74 degrees Fahrenheit

Humidity

- Humidity is the amount of moisture in the air. High humidity levels create condensation problems, and low humidity levels can increase the amount of static electricity in the environment. With condensation comes the short-circuiting of electrical equipment and the potential for mold and rot in paper-based information storage.

Static

- Static electricity is caused by a process called triboelectrification, which occurs when two materials are rubbed or touched and electrons are exchanged, resulting in one object becoming more positively changed and the other more negatively charged.
- When a third object with an opposite charge or ground is encountered, electrons flow again, and a spark is produced. One of the leading causes of damage to sensitive circuitry is electro-static discharge (ESD). Integrated circuits in a computer use between two and five volts of electricity. Voltage levels as low as 200 can cause microchip damage.
- Static electricity is not even noticeable to humans until levels approach 1,500 volts, and you can't see the little blue spark until it approaches 4,000 volts.
- A person can generate up to 12,000 volts of static current by walking across a carpet. Two types of failures can result from ESD damage to chips. Immediate failures, also known as catastrophic failures, occur right away, are usually totally destructive. Latent failures or delayed failures can

occur weeks or even months after the damage is done. It is imperative to maintain the optimal level of humidity, which is between 40 and 60 percent, in the computing environment. Humidity levels below this range create static, and levels above create condensation.

Ventilation Shafts

- One last discussion point within the topic of HVAC is the security of the ventilation system air ductwork. While in residential buildings the ductwork is quite small, in large commercial buildings it can be large enough for an individual to climb though.
- If the vents are large, security can install wire mesh grids at various points to compartmentalize the runs. In any case, the ventilation system is one more area within the HVAC that must be evaluated.

Power Management and Conditioning

- Not only is electrical quantity (voltage level and amperage rating) of concern, but so is the quality of the power (cleanliness and proper installation).
- Interference with the normal pattern of the electrical current is referred to as noise in the current. Any noise that interferes with the normal 60 Hertz cycle can result in inaccurate time clocks or, even worse, unreliable internal clocks inside the CPU.

Grounding

- Grounding ensures that the returning flow of current is properly discharged to the ground.
- If this is not properly installed, anyone touching a computer or other electrical device could be used as a ground source, causing damage to equipment and injury or death to the person.
- Power should also be provided in sufficient amperage to support needed operations.
- Overloading a circuit not only causes problems with the circuit tripping but can also overload the power load on an electrical cable, creating the risk of fire.

Uninterruptible Power Supplies (UPS)

- In case of power outage, a UPS is a backup power source for major computer systems.
- There are four basic configurations of UPS:
- A standby or offline UPS is an off-line battery backup that detects the interruption of power to the power equipment.

- A ferroresonant standby UPS is still an offline UPS, with the electrical service still providing the primary source of power, with the UPS serving as a battery backup. The ferroresonant transformer reduces power problems.
- The line-interactive UPS is always connected to the output, so has a much faster response time and incorporates power conditioning and line filtering.
- The true online UPS works in the opposite fashion to a standby UPS since the primary power source is the battery, with the power feed from the utility constantly recharging the batteries. This model allows constant feed to the system, while completely eliminating power problems.

Emergency Shutoff

- One important aspect of power management in any environment is the need to be able to stop power immediately should the current represent a risk to human or machine safety.
- Most computer rooms and wiring closets are equipped with an emergency power shutoff, which is usually a large red button, prominently placed to facilitate access, with an accident-proof cover to prevent unintentional use.
    - Electrical power influences:
    - Fault: momentary interruption in power
    - Blackout: prolonged interruption in power
    - Sag: momentary drop in power voltage levels
    - Brownout: prolonged drop in power voltage levels
    - Spike: momentary increase in power voltage levels
    - Surge: prolonged increase in power voltage levels

Water Problems

- Lack of water poses problem to systems, including the functionality of fire suppression systems, and the ability of water chillers to provide air-conditioning. On the other hand, a surplus of water, or water pressure, poses a real threat. It is therefore important to integrate water detection systems into the alarm systems that regulate overall facilities operations.

Structural Collapse

- Unavoidable environmental factors or forces of nature can cause failures of structures that house the organization. Structures are designed and constructed with specific load limits, and

overloading these design limits, intentionally or unintentionally, inevitably results in structural failure and potentially loss of life or injury.

- Periodic inspections by qualified civil engineers assists in identifying potentially dangerous structural conditions well before they fail.

Testing Facility Systems

- Just as with any phase of the security process, the physical security of the facility must be constantly documented, evaluated, and tested. Documentation of the facilities configuration, operation, and function is integrated into disaster recovery plans and standing operating procedures.
- Testing provides information necessary to improve the physical security in the facility and identifies areas weak points.

5.8 SECURITY AND PERSONAL ISSUES

- When implementing information security, an organization must address various issues.
- First, it must decide how to position and name the security function.
- Second, the information security community of interest must plan for the proper staffing (or adjustments to the staffing plan) for the information security function.
- Third, the IT community of interest must assess the impact of information security on every IT function and adjust job descriptions and documented practices accordingly.
- Finally, the general management community of interest must work with information security professionals to integrate solid information security concepts into the personnel management practices of the organization.

5.8.1 Positioning and Staffing the Security Function

- There are several valid choices for positioning the information security department within an organization. The model commonly used by large organizations places the information security department within the information technology department and usually designates as its head the CISO (or CSO, Chief Security Officer), who reports directly to the company's top computing executive, or CIO.
- Actually, there are many ways to position the information security program within an organization.

- According to Wood, the information security function can be placed within any of the following organizational functions:
  - IT function, as a peer of other subfunctions such as networks, applications development, and the help desk
  - Physical security function, as a peer of physical security or protective services
  - Administrative services function, as a peer of human resources or purchasing
  - Insurance and risk management function
  - Legal department

5.8.2 Staffing the Information Security Function

- Selecting personnel is based on many criteria, including supply and demand
- Many professionals enter security market by gaining skills, experience, and credentials
- At present, information security industry is in period of high demand

Qualifications and Requirements

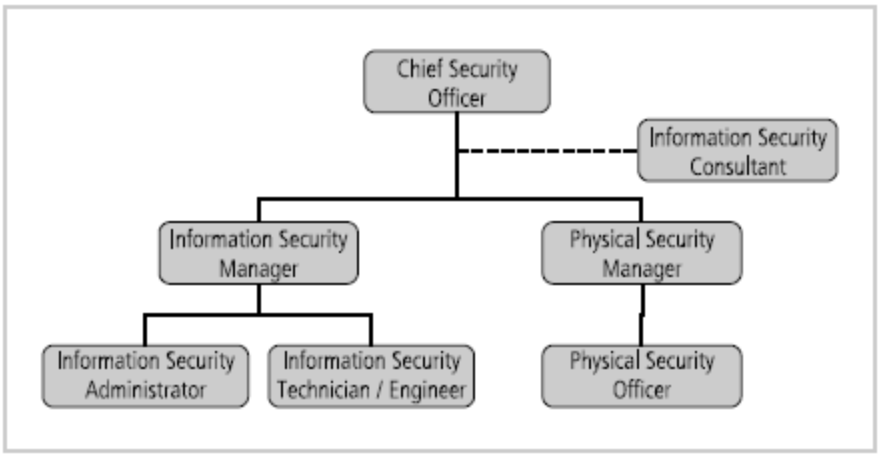
- The following factors must be addressed:
  - Management should learn more about position requirements and qualifications
  - Upper management should learn about budgetary needs of information security function
  - IT and management must learn more about level of influence and prestige the information security function should be given to be effective
- Organizations typically look for technically qualified information security generalist
- Organizations look for information security professionals who understand:
  - How an organization operates at all levels
  - Information security usually a management problem, not a technical problem
  - Strong communications and writing skills
  - The role of policy in guiding security efforts
- Organizations look for (continued):
  - Most mainstream IT technologies
  - The terminology of IT and information security
  - Threats facing an organization and how they can become attacks
  - How to protect organization's assets from information security attacks
  - How business solutions can be applied to solve specific information security problems.

Entry into the Information Security Profession

- Many information security professionals enter the field through one of two career paths:
- Law enforcement and military
- Technical, working on security applications and processes
- Today, students select and tailor degree programs to prepare for work in information security
- Organizations can foster greater professionalism by matching candidates to clearly defined expectations and position descriptions.

Information Security Positions

- Use of standard job descriptions can increase degree of professionalism and improve the consistency of roles and responsibilities between organizations
- Charles Cresson Wood's book Information Security Roles and Responsibilities Made
- Easy offers set of model job descriptions
- Chief Information Security Officer (CISO or CSO)
  - Top information security position; frequently reports to Chief Information Officer.
  - Manages the overall information security program
  - Drafts or approves information security policies
  - Works with the CIO on strategic plans
- Chief Information Security Officer (CISO or CSO) (continued)
  - Develops information security budgets
  - Sets priorities for information security projects and technology
  - Makes recruiting, hiring, and firing decisions or recommendations
  - Acts as spokesperson for information security team
  - Typical qualifications: accreditation; graduate degree; experience
- Security Manager
  - Accountable for day-to-day operation of information security program
  - Accomplish objectives as identified by CISO
  - Typical qualifications: not uncommon to have accreditation; ability to draft middle and lower level policies, standards and guidelines; budgeting, project management, and hiring and firing; manage technicians.



Positions in Information Securtiy

5.8.3 Employment Policies and Practices

- Management community of interest should integrate solid information security concepts into organization's employment policies and practices
- Organization should make information security a documented part of every employee's job description
- From information security perspective, hiring of employees is a responsibility laden with potential security pitfalls
- CISO and information security manager should provide human resources with information security input to personnel hiring guidelines.

Hiring Issues

Job Descriptions

- Integrating information security perspectives into hiring process begins with reviewing and updating all job descriptions
- Organization should avoid revealing access privileges to prospective employees when advertising open positions

Background Checks

- Investigation into a candidate's past
- Should be conducted before organization extends offer to candidate
- Background checks differ in level of detail and depth with which candidate is examined
- May include identity check, education and credential check, previous employment verification, references check, drug history, credit history, and more

Employment Contracts

- Once a candidate has accepted the job offer, employment contract becomes important security instrument
- Many security policies require an employee to agree in writing
- New employees may find policies classified as "employment contingent upon agreement," whereby employee is not offered the position unless binding organizational policies are agreed to

New Hire Orientation

- New employees should receive extensive information security briefing on policies, procedures, and requirements for information security
- Levels of authorized access are outlined; training provided on secure use of information systems
- By the time employees start, they should be thoroughly briefed and ready to perform duties securely

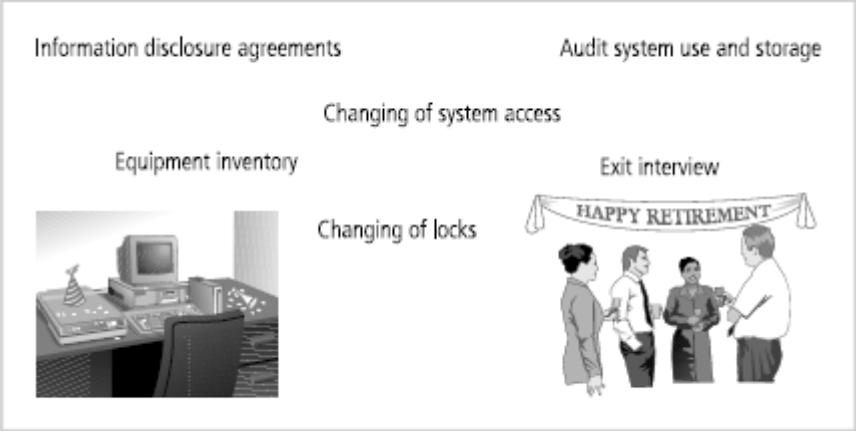
On-the-Job Security Training

- Organization should conduct periodic security awareness training
- Keeping security at the forefront of employees' minds and minimizing employee mistakes is an important part of information security awareness mission
- External and internal seminars also increase level of security awareness for all employees, particularly security employees

Evaluating Performance

- Organizations should incorporate information security components into employee performance evaluations
- Employees pay close attention to job performance evaluations; if evaluations include information security tasks, employees are more motivated to perform these tasks at a satisfactory level.

Termination



Termination Activities

- When employee leaves organization, there are a number of security-related issues
- Key is protection of all information to which employee had access
- Once cleared, the former employee should be escorted from premises
- Many organizations use an exit interview to remind former employee of contractual obligations and to obtain feedback
- Hostile departures include termination for cause, permanent downsizing, temporary lay-off, or some instances of quitting
    - Before employee is aware, all logical and keycard access is terminated
    - Employee collects all belongings and surrenders all keys, keycards, and other company property
    - Employee is then escorted out of the building
- Friendly departures include resignation, retirement, promotion, or relocation
    - Employee may be notified well in advance of departure date
    - More difficult for security to maintain positive control over employee's access and information usage

  - Employee access usually continues with new expiration date
  - Employees come and go at will, collect their own belongings, and leave on their own
- Offices and information used by the employee must be inventoried; files stored or destroyed; and property returned to organizational stores
- Possible that employees foresee departure well in advance and begin collecting organizational information for their future employment
- Only by scrutinizing systems logs after employee has departed can organization determine if there has been a breach of policy or a loss of information
- If information has been copied or stolen, action should be declared an incident and the appropriate policy followed.

5.8.4 Security Considerations for Nonemployees in an Organization

- Individuals not subject to screening, contractual obligations, and eventual secured termination often have access to sensitive organizational information
- Relationships with these individuals should be carefully managed to prevent possible information leak or theft

Temporary Employees

- Hired by organization to serve in temporary position or to supplement existing workforce
- Often not subject to contractual obligations or general policies; if temporary employees breach a policy or cause a problem, possible actions are limited
- Access to information for temporary employees should be limited to that necessary to perform duties
- Temporary employee's supervisor must restrict the information to which access is possible

Contract Employees

- Typically hired to perform specific services for organization
- Host company often makes contract with parent organization rather than with individual for a particular task
- In secure facility, all contract employees escorted from room to room, as well as into and out of facility
- There is need for restrictions or requirements to be negotiated into contract agreements when they are activated

Consultants

- Should be handled like contract employees, with special requirements for information or facility access integrated into contract
- Security and technology consultants must be prescreened, escorted, and subjected to nondisclosure agreements to protect organization
- Just because security consultant is paid doesn't make the protection of organization's information the consultant's number one priority

Business Partners

- Businesses find themselves in strategic alliances with other organizations, desiring to exchange information or integrate systems
- There must be meticulous, deliberate process of determining what information is to be exchanged, in what format, and to whom
- Nondisclosure agreements and the level of security of both systems must be examined before any physical integration takes place