Management of Information Security, 4th Edition

Chapter 10

Protection Mechanisms

Objectives

- Describe the various access control approaches, including authentication, authorization, and biometric access controls
- Identify the various types of firewalls and the common approaches to firewall implementation
- Enumerate and discuss the current issues in dial-up access and protection
- Identify and describe the types of intrusion detection systems and the strategies on which they are based
- Explain cryptography and the encryption process, and compare/contrast symmetric and asymmetric encryption

Access Controls

- Access controls - regulate the admission of users into trusted areas of the organization
- Access control involves four processes:
  - Identification
  - Authentication
  - Authorization
  - Accountability

Identification

- Identification - a mechanism that provides information about an unverified entity that wants to be granted access to a known entity
  - Unverified entity is called a **supplicant**
- The label applied to the supplicant is called an identifier (ID)
- The ID must be a unique value that can be mapped to one entity within the security domain

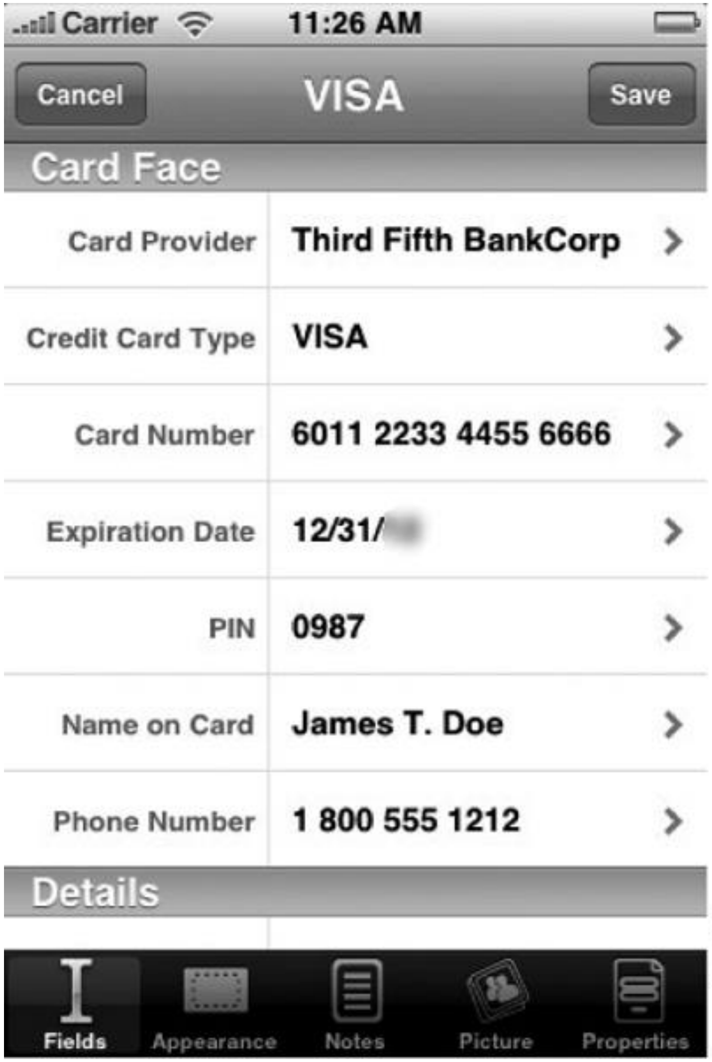
Authentication Part 1

- Authentication - the process of validating a supplicant's purported identity
- Four types of authentication mechanisms:
  - Something you *know*
  - Something you *have*
  - Something you *are*
  - Something you *produce*
- Strong authentication - at minimum, two different authentication mechanisms
  - Example: ATM requires a bank card and a PIN

Authentication Part 2

- Something you know - verifies identity by means of:
  - Password - secret word or combination of characters
  - Passphrase - a plain-language phrase from which a **virtual password** is derived
    - Example: May The Force Be With You Always, from which the virtual password MTFBWYA is derived
  - Some other unique authentication code (such as a PIN)
- A password memory support software application such as eWallet from Ilium Software
  - Is another method for creating strong passwords

Figure 10-2 eWallet from Ilium



Card Provider	Third Fifth BankCorp
Credit Card Type	VISA
Card Number	6011 2233 4455 6666
Expiration Date	12/31/[redacted]
PIN	0987
Name on Card	James T. Doe
Phone Number	1 800 555 1212

Source: Ilium Software.

Authentication Part 3

- Something You Have - makes use of something that the user or system has
  - **Dumb card** - cards with magnetic strips containing the digital PIN against which user input is compared
  - **Smart card** - contains a computer chip that can verify and validate information to addition to PINs
  - **Synchronous tokens** - synchronized with a server, each device generates the authentication number that is entered during the user login
  - **Asynchronous tokens** - the server challenges the user with a number and calculates a response

Authentication Part 4

- Something you are - takes advantage of something inherent in the user that is evaluated using biometrics, including:
  - Fingerprints (considered truly unique)
  - ID cards with face representations
  - Facial recognition
  - Hand geometry
  - Retina scan (considered truly unique)
  - Iris scan (considered truly unique)
  - Voice recognition
  - Palm vein authentication

Authentication Part 5

- Something you produce - makes use of something the user performs or produces
  - – Example: a signature or voice pattern

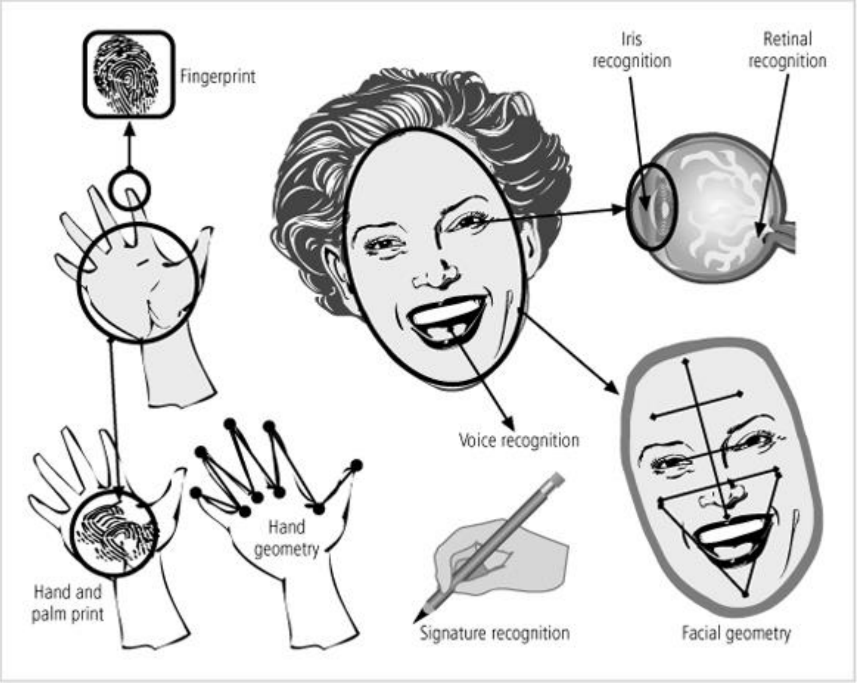


Figure 10-4 Recognition characteristics

Evaluating Biometrics

- Biometric means life measurement
- Biometric technologies are generally evaluated according to three basic criteria:
  - *False reject rate* - percentage of authorized users who are denied access
  - *False accept rate* - percentage of unauthorized users who are allowed access
  - *Crossover error rate* - the point at which the number of false rejections equals the number of false acceptances

Table 10-2 Orders of effectiveness and acceptance

Effectiveness of Biometric Authentication Systems Ranking from Most Secure to Least Secure	**Acceptance of Biometric Authentication Systems Ranking from Most Accepted to Least Accepted**
• Retina pattern recognition	• Keystroke pattern recognition
• Fingerprint recognition	• Signature recognition
• Handprint recognition	• Voice pattern recognition
• Voice pattern recognition	• Handprint recognition
• Keystroke pattern recognition	• Fingerprint recognition
• Signature recognition	• Retina pattern recognition

Authorization

- Authorization can be handled in one of three ways:
  - Authorization for each authenticated user
  - Authorization for members of a group
  - Authorization across multiple systems
    - A central authentication and authorization system verifies entity identity and grants a set of credentials to the verified entity

Accountability

- **Accountability** - ensures that all actions on a system can be attributed to an authenticated identity
  - Most often accomplished by implementing and auditing system logs and database journals
- **System logs** - records maintained by a particular system that has been configured to record specific information
  - Such as failed access attempts and systems modifications
  - Can be used for intrusion detection, determining the root cause of a system failure, and tracking resource usage

Log Generation

- Log generation involves the configuration of systems to create logs
- Issues in log generation include:
  - *Multiple log sources*
  - *Inconsistent log content, timestamps, and log format*
- In order to interpret data from the Log Generation tier, the following functions must be addressed:
  - *Log parsing*
  - *Event filtering*
  - *Event aggregation*

Log Analysis and Storage Part 1

- Log analysis and storage - the transference of log data to an analysis system
  - Known as **security event information management (SEIM) systems**
- Management functions within log storage include:
  - *Log rotation*
  - *Log archival*
  - *Log compression*
  - *Log reduction*
  - *Log conversion*

Log Analysis and Storage Part 2

- Management functions within log storage (cont’d):
  - *Log normalization*
  - *Log file integrity*
- Management functions within log analysis include:
  - Event correlation
  - Log viewing
  - Log reporting
- Log disposal or log clearing is the specification of when logs may be deleted or overwritten within a system

Log Analysis and Storage Part 3

- General suggestions for managing logs:
  - Make sure data stores can handle the amount of data generated by the configured logging activities
  - Rotate logs when unlimited data storage is not possible
  - Archive logs - copy to remote storage locations
  - Secure logs - should be encrypted in case log data store is compromised
  - Destroy logs - once log data has outlived its usefulness, it should be securely destroyed

Managing Access Controls

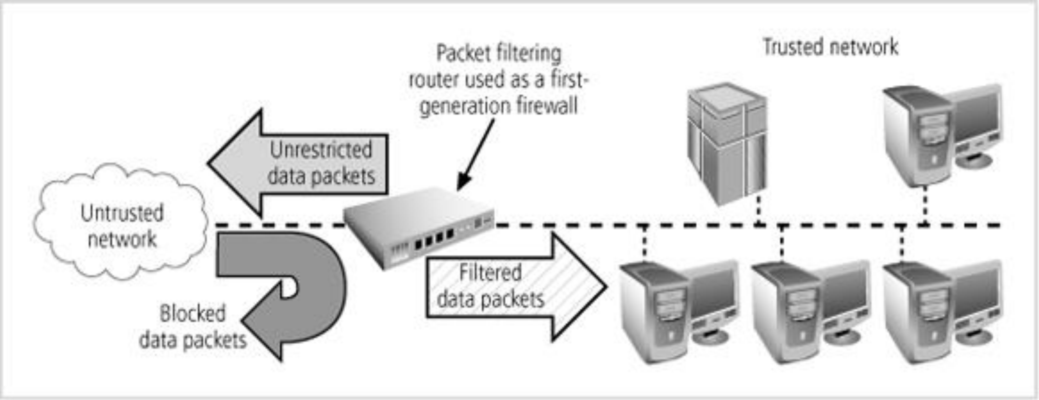
- Access control policy - specifies how access rights are granted to entities and groups
- Must include provisions for:
  - Periodically reviewing all access rights
  - Granting access rights to new employees
  - Changing access rights when job roles change
  - Revoking access rights as appropriate
- Without it, system administrators may implement access controls in a way that is inconsistent with the organization’s overall philosophy

Firewalls

- In InfoSec, a firewall is any device that prevents a specific type of information from moving between the outside world (**untrusted network**) and the inside world (**trusted network**)
- A firewall may be a
  - Separate computer system
  - Service running on an existing router or server
  - Separate network containing a number of supporting devices

The Development of Firewalls Part 1

- Packet filtering firewalls - simple networking devices that filter packets by examining every incoming and outgoing packet header
  - Can filter based on IP address, type of packet, port request, and/or other elements present in the packet


Packet filtering router used as a first-generation firewall
Trusted network
Unrestricted data packets
Untrusted network
Filtered data packets
Blocked data packets

Copyright © 2014 Cengage Learning®.

Figure 10-5 Packet filtering firewall

The Development of Firewalls Part 2

- **Application-level firewalls** - often consist of dedicated computers kept separate from the first filtering router (called an edge router)
  - Commonly used in conjunction with a second or internal filtering router (called a proxy server)
- **Demilitarized zone (DMZ)** - an intermediate area between a trusted network and an untrusted network
- **Cache server** - A proxy server or application-level firewall that stores recently accessed Web content in its internal cache

The Development of Firewalls Part 3

- **Stateful inspection firewalls** - keep track of each network connection established between internal and external systems using a state table
  - State tables track the state and context of each exchanged packet by recording which station sent which packet and when
- **Dynamic packet filtering firewalls** - allow only a particular packet with a specific source, destination, and port address to pass through the firewall

The Development of Firewalls Part 4

- **Unified Threat Management (UTM)** - Networking devices categorized by their ability to perform the work of a:
  - – Stateful inspection firewall
  - – Network intrusion detection and prevention system
  - – Content filter and spam filter
  - – Malware scanner and filter

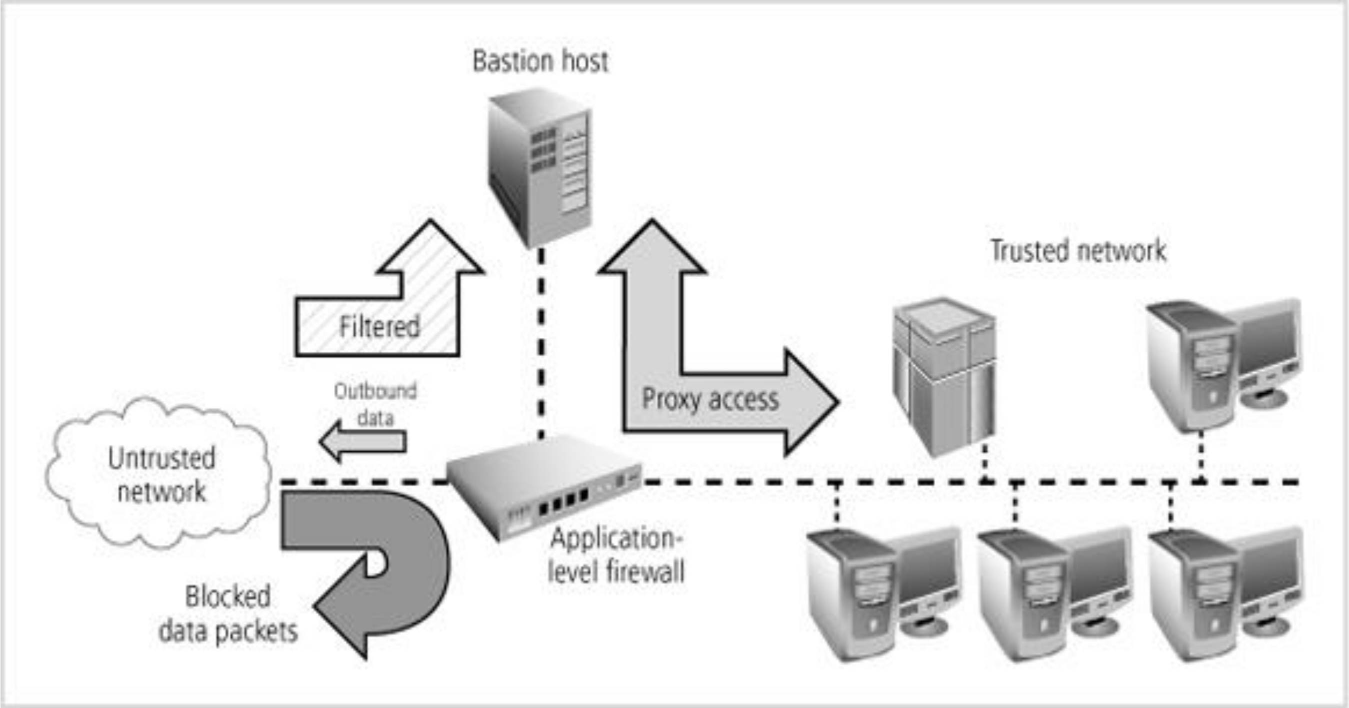
Firewall Architectures Part 1

- Four architectural implementations of firewalls are common:
  - Packet filtering routers
  - Screened-host firewalls
  - Dual-homed host firewalls
  - Screened-subnet firewalls
- **Packet Filtering Routers** - simple but effective means of lowering the risk of an external attack
  - Lacks auditing and strong authentication
  - Packet filtering can degrade network performance

Firewall Architectures Part 2

- **Screened-Host Firewall Systems** - combine the packet filtering router with a separate, dedicated firewall such as an application proxy server
  - **Bastion host**: the separate application proxy that examines an application-layer protocol, such as HTTP, and performs the proxy services, thus representing a single, rich target for external attacks and that should, therefore, be very thoroughly secured
    - Also commonly referred to as the **sacrificial host**

Figure 10-6 Screened-host firewall



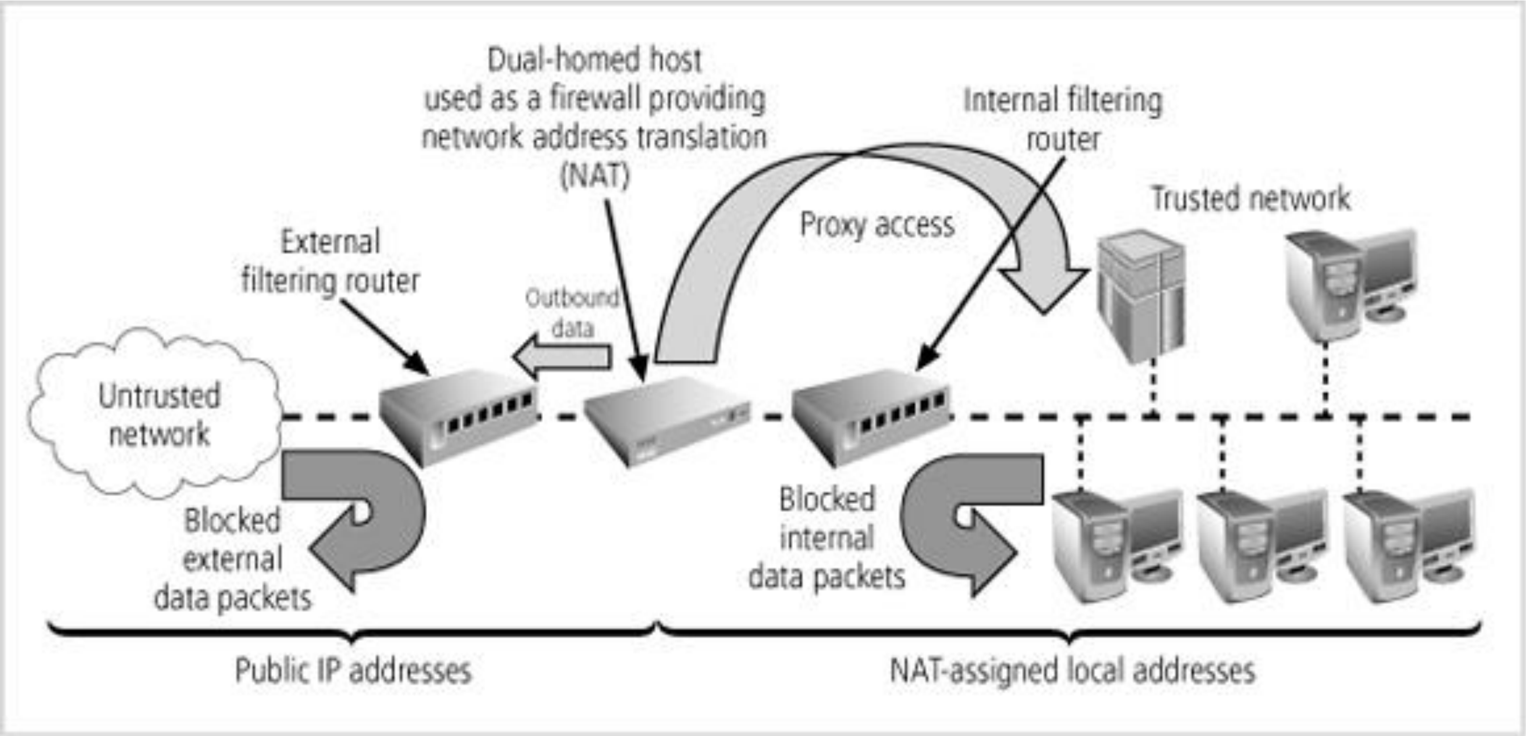
Copyright © 2014 Cengage Learning®.

© Cengage Learning 2014

Firewall Architectures Part 3

- **Dual-Homed Host Firewalls** - the bastion host contains two network interfaces: one is connected to the external network and one to the internal network
  - All traffic must go through the firewall
- **Network-address translation (NAT)** - a method of converting multiple real, routable external IP addresses to ranges of internal IP addresses
  - Often implemented in this architecture
- **Port-address translation (PAT)** similar to NAT, only it uses a one to many approach using port numbers

Figure 10-7 Dual-homed host firewall


Dual-homed host used as a firewall providing network address translation (NAT)
Internal filtering router
Trusted network
Proxy access
External filtering router
Outbound data
Untrusted network
Blocked external data packets
Blocked internal data packets
Public IP addresses
NAT-assigned local addresses

Copyright © 2014 Cengage Learning®.

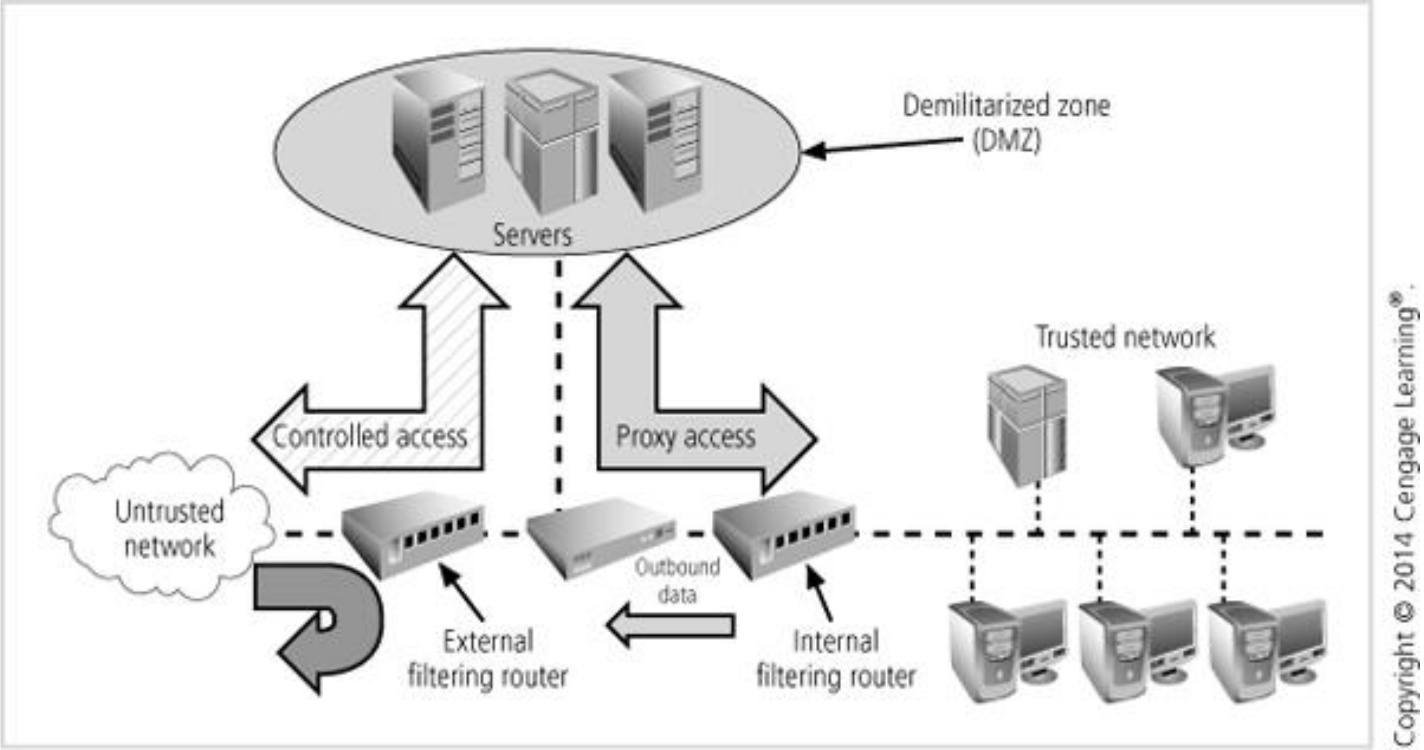
Firewall Architectures Part 4

- Dual-homed hosts take advantage of NAT or PAT by preventing external attacks from reaching internal machines with addresses in specified ranges
- Two disadvantages:
  - If the dual-homed host is compromised, it can take out the connections to the external network
  - As traffic volume increases, the dual-homed host can become overloaded
- Big advantage:
  - Provides strong protection with minimal expense

Firewall Architectures Part 5

- **Screened-Subnet Firewalls (with DMZ)** - consists of one or more internal bastion hosts located behind a packet filtering router, with each host protecting the trusted network
  - Provides an intermediate area (DMZ) between the trusted network and the untrusted network
  - This DMZ can be a dedicated port on the firewall device or it can be connected to a screened subnet or DMZ
  - Until recently, servers providing services via the untrusted network were placed in the DMZ

Figure 10-8 Screened subnet (DMZ)



Copyright © 2014 Cengage Learning®.

Firewall Architectures Part 6

- When evaluating a firewall, ask the following:
  - What type of firewall technology offers the right balance between protection and cost?
  - What features are included in the base price? What features are available at extra cost?
  - How is easy is set up and configuration? How accessible are the staff technicians who can configure the firewall?
  - Can the candidate firewall adapt to the growing network in the target organization?

Managing Firewalls Part 1

- Configuring firewall rule sets can be complex
  - Logic errors in the preparation can cause unintended behavior
  - Each rule must be placed into the list in the proper sequence
  - Proper rule sequence ensures the most resource-intensive actions are performed after the most restrictive ones
    - Reduces the number of packets that undergo intense scrutiny

Managing Firewalls Part 2

- Firewalls limitations:
  - They are not creative and cannot make sense of human actions outside of their programming
  - They deal strictly with defined patterns of measured observation
  - They are computers and prone to programming errors, flaws in rule sets, and inherent vulnerabilities
  - They are designed to function within limits of hardware capacity and can only respond to patterns of events that happen expectantly
  - They are designed, implemented, and configured by people and are subject to human error

Managing Firewalls Part 3

- Administrative challenges to firewall operation:
  - *Training*
  - *Uniqueness*
  - *Responsibility*
  - *Administration*
- Recommended practices for firewall use:
  - All traffic from the trusted network is allowed out
  - The firewall device is never accessible directly from the public network
  - SMTP data is allowed to pass through the firewall and routed to a SMTP gateway to filter and route messaging traffic securely

Managing Firewalls Part 4

- Recommended practices for firewall use (cont’d):
  - All ICMP data is denied
  - Telnet/terminal emulation access to all internal servers from the public networks is blocked
  - When Web services are offered outside the firewall, HTTP traffic is prevented from reaching your internal networks via the implementation of some form of proxy access or DMZ architecture

Intrusion Detection and Prevention Systems

- **Intrusion detection and prevention systems (IDPSs)** - specialized hardware and/or software that works like burglar alarms by detecting a violation, activating an alarm, and, under certain circumstances, reacting to the intrusion
  - Can be configured to notify administrators via e-mail and numerical or text paging
  - Require complex configurations to provide the appropriate level of detection and response

Intrusion Detection and Prevention Systems (continued)

- Systems that include intrusion prevention attempt to prevent the attack from succeeding by one of the following:
  - Stopping the attack by terminating the network connection or the attacker’s user session
  - Changing the security environment by reconfiguring network devices to block access to the targeted system
  - Changing the attack’s content to make it benign

Host-Based IDPS

- **Host-based IDPS (HIDPS)** - works by configuring and classifying various categories of systems and data files
  - Can monitor multiple computers simultaneously
  - They store a client file on each monitored host
    - That host must report back to the master console
  - The master console monitors the information from the managed clients
    - Notifies the administrator when predetermined attack conditions occur

Network-Based IDPS

- **Network-based IDPS (NIDPS)** - an IDPS that monitors network traffic, looking for patterns of network traffic
  - Such as large collections of related traffic that can indicate a DoS attack or a series of related packets that could indicate a port scan in progress
- Organizations may install data collection sensors that are both host-based and network-based
  - This type is called a hybrid-IDPS

Signature-Based IDPS

- **Signature-based IDPS** - examines data traffic for something that matches the signatures, which comprise preconfigured, predetermined attack patterns
  - Also known as a **knowledge-based IDPS**
- Signatures must be continually updated as new attack strategies emerge
- Another weakness:
  - The time frame over which attacks occur

Anomaly-Based IDPS

- **Anomaly-based IDPS** - first collects data from normal traffic and establishes a baseline
  - Then periodically samples network activity, using statistical methods, compares the samples to the baseline, and notifies the administrator when the activity falls outside the clipping level
  - Also known as a **behavior-based IDPS** and formerly called a **statistical anomaly-based IDPS**
  - System is able to detect new types of attacks but require much more overhead and processing capacity than signature-based versions

Managing Intrusion Detection and Prevention Systems

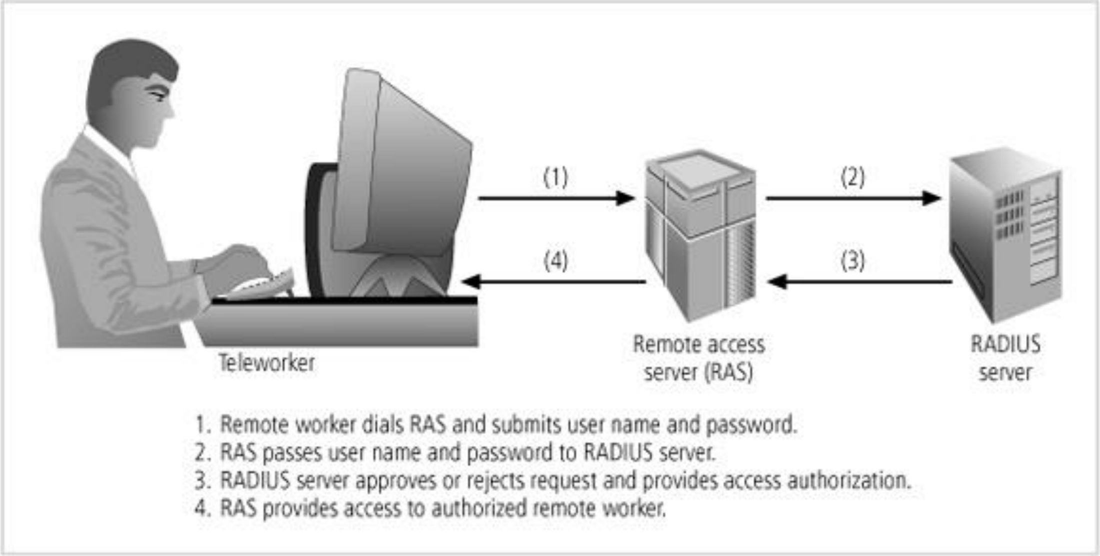
- IDPSs must be configured using technical knowledge and adequate business and security knowledge
  - To differentiate between routine circumstances and low, moderate, or severe threats to the security of information assets
- Most IDPS monitor system by means of agents
  - Sometimes called a **sensor**, an **agent** is a piece of software that resides on a system and reports back to a management server

Remote Access Protection

- Unsecured dial-up access represents a substantial exposure to attack
- Attackers can use a device called a war-dialer
  - **War-dialer**: an automatic phone-dialing program that dials every number in a configured range
    - Checks whether a person, answering machine, or modem picks up
    - Attacker attempts to hack into the network through a modem connection
- Some newer technologies have improved means of authentication for dial-up connections

RADIUS and TACACS

- **Remote Authentication Dial-In User Service (RADIUS)** - authentication of each user takes place on a central RADIUS server



1. Remote worker dials RAS and submits user name and password.
2. RAS passes user name and password to RADIUS server.
3. RADIUS server approves or rejects request and provides access authorization.
4. RAS provides access to authorized remote worker.

Copyright © 2014 Cengage Learning®.

Figure 10-10 RADIUS configuration

RADIUS and TACACS (continued)

- **Terminal Access Controller Access Control System (TACACS)** - a remote access authorization system based on a client/server configuration that makes use of a centralized data service in order to validate the user’s credentials at the TACACS server
  - Commonly used in UNIX systems
- Three versions of TACACS exist:
  - TACACS, Extended TACACS, and TACACS+

Managing Dial-Up Connections

- Organizations with dial-up remote access must:
  - *Determine how many dial-up connections it has*
  - *Control access to authorized modem numbers*
  - *Use call-back whenever possible*
  - *Use token authentication if at all possible*

Wireless Networking Protection Part 1

- **Footprint** - in wireless networking, the geographic area within which there is sufficient signal strength to make a network connection
  - The size of the footprint depends on the amount of power the transmitter/receiver **wireless access points (WAPs)** emit
- **War driving** - moving through a geographic area or building, actively scanning for open or unsecured WAPs
- A number of encryption protocols can be used to secure wireless networks

Wireless Networking Protection Part 2

- **Wired Equivalent Privacy (WEP)** - designed to provide a basic level of security protection
  - Part of the IEEE 802.11 wireless standard
  - There are flaws that led to the replacement of WEP as the industry standard with WPA
- **Wi-Fi Protected Access (WPA)** - set of protocols used to secure wireless networks
  - Includes WPA and WPA2 and can use an IEEE 802.1X authentication server
  - Can issue keys to users to share a key (preshared)

Wireless Networking Protection Part 3

- **WiMAX** - next generation of wireless networking
  - Also known as Wireless MAN
  - Essentially an improvement on the technology developed for cellular telephones and modems
- **Bluetooth** - standard for short-range wireless communications between devices such as wireless telephones and headsets
  - Offers approximately a 30-foot range
  - Securing Bluetooth enabled devices: (1) turn off Bluetooth when not needed (2) do accept incoming communications unless you know the requestor

Scanning and Analysis Tools Part 1

- **Port scanners** - a group of utility applications that can identify computers that are active on a network
  - As well as the active ports and services on those computers
  - Port: a network channel or connection point in a data communication system
- **Vulnerability scanners** - variants of port scanners
  - Capable of scanning networks for information
  - Identify exposed user names and groups, show open network shares, expose configuration problems and other vulnerabilities

Scanning and Analysis Tools Part 2

- **Packet sniffer** - a network tools that collects and analyzes copies of packets from the network
  - Can provide a network administrator with information to help diagnose and resolve networking issues
  - In the wrong hands, can be used to eavesdrop
- **Content Filters** - a software program or a hardware/software appliance that allows administrators to restrict content that comes on a network
  - Common applications are the restriction of access to Web sites and spam e-mail

Scanning and Analysis Tools Part 3

- **Trap and Trace** - applications that entice individuals who are illegally perusing the internal areas of a network
  - By providing simulated rich content areas but distract the attacker while the software notifies the administrator of the intrusion
  - Some are capable of tracking the attacker back through the network
  - Better known as honey pots

Managing Scanning and Analysis Tools

- Drawbacks to using scanners and tools:
  - Tools are not human and cannot simulate the more creative behavior of a human attacker
  - Most tools function by pattern recognition, only previously known issues can be detected
  - Most of the tools are prone to errors, flaws, and vulnerabilities of their own
  - All of these tools are designed, configured, and operated by humans and are subject to human error
  - You get what you pay for

Managing Scanning and Analysis Tools (continued)

- Drawbacks to using scanners and tools (cont’d):
  - Specifically for content filters, some governments, agencies, institutions, and universities have established policies or laws to protect user’s right to access content
  - Tool usage and configuration must comply with an explicitly articulated policy
    - The policy must provide for valid exceptions

Cryptography

- The science of encryption is known as **cryptology**
  - Encompasses two disciplines: cryptography and cryptanalysis
- **Cryptography** - the set of processes involved in encoding and decoding messages so that others cannot understand them
- **Cryptanalysis** - the process of deciphering the original message (**plaintext**) from an encrypted message (**ciphertext**) without knowing the algorithms and keys used to perform the encryption

Encryption Operations Part 1

- Encryption is accomplished by using algorithms to manipulate the plaintext into ciphertext for transmission
- Common Ciphers
  - **Substitution cipher** - substitute one value for another
    - **Polyalphabetic substitutions** use two or more alphabets
  - **Transposition cipher** - rearranges the values within a block to create the ciphertext
    - Also called **permutation cipher**

Encryption Operations Part 2

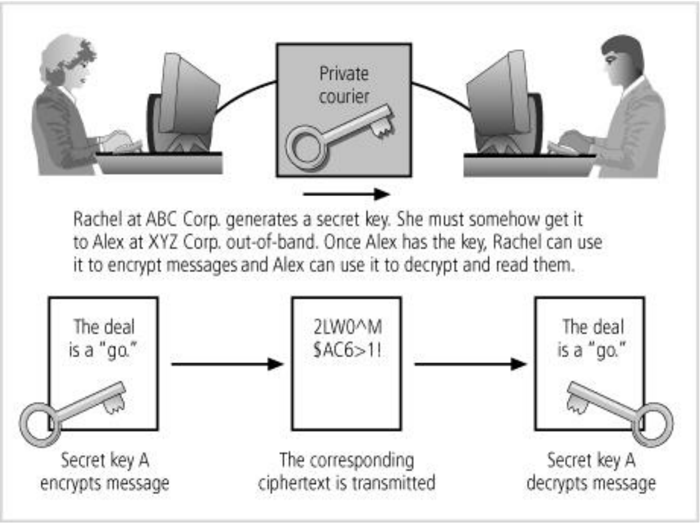
- Common Ciphers (cont'd)
  - **XOR cipher** - the bit stream is subjected to a Boolean XOR function against some other data stream
    - Typically a key stream
- **Vernam Cipher** - uses a set of characters for encryption operations only one time and then discards it
  - Developed at AT&T and also known as the "one-time pad"

Encryption Operations Part 3

- **Book or Running Key Cipher** - encryption method in which the words (or, in some cases, characters) found in a book act as the algorithm to decrypt a message
  - The key relies on two components: (1) knowing which book to refer to and (2) having a list of codes representing the page number, line number, and word number of the plaintext word
  - Dictionaries and thesauruses are the most popular sources

Encryption Operations Part 4

- **Symmetric Encryption** - encryption method in which the same algorithm and secret key is used to both encipher and decipher the message
  - Also known as private key encryption



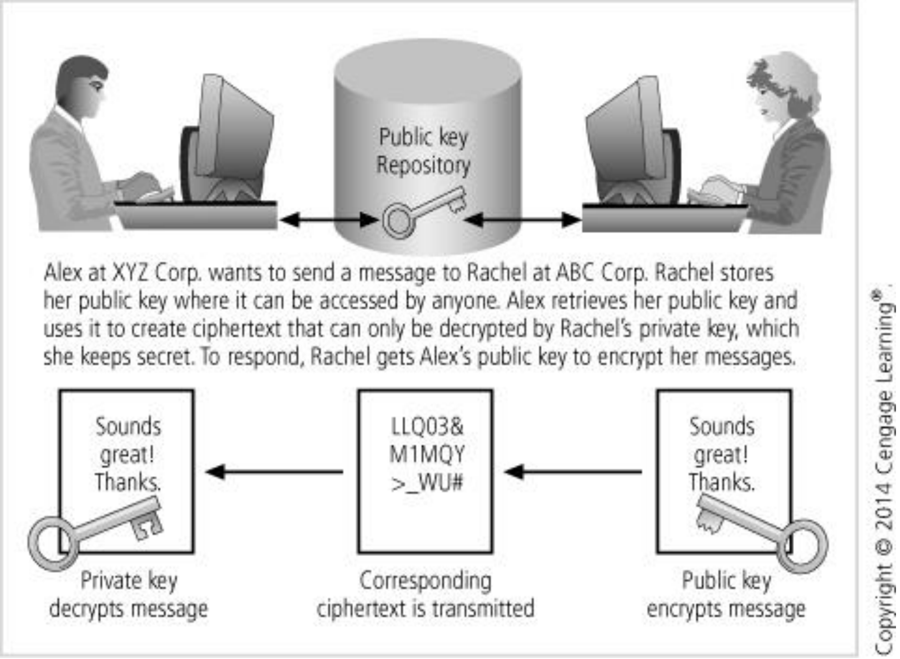
Rachel at ABC Corp. generates a secret key. She must somehow get it to Alex at XYZ Corp. out-of-band. Once Alex has the key, Rachel can use it to encrypt messages and Alex can use it to decrypt and read them.

Copyright © 2014 Cengage Learning®.

Figure 10-11 Symmetric encryption

Encryption Operations Part 5

- **Asymmetric Encryption** - encryption method that uses two different keys, either of which can be used to encrypt or decrypt a message, but not both


Public key Repository
Sounds great! Thanks.
LLQ03& M1MQY >_WU#
Sounds great! Thanks.
Private key decrypts message
Corresponding ciphertext is transmitted
Public key encrypts message

Alex at XYZ Corp. wants to send a message to Rachel at ABC Corp. Rachel stores her public key where it can be accessed by anyone. Alex retrieves her public key and uses it to create ciphertext that can only be decrypted by Rachel's private key, which she keeps secret. To respond, Rachel gets Alex's public key to encrypt her messages.

Copyright © 2014 Cengage Learning®.

Figure 10-12 Asymmetric encryption

Encryption Operations Part 6

- **Digital Signatures** - a process of using a reversed asymmetric encryption process in which a private key is used to encrypt a (usually short) message and the corresponding public key is used to decrypt it to provide nonrepudiation
  - thus creating encrypted messages whose authenticity can be independently verified by a central facility (registry)
  - **Digital certificate** - block of data, similar to a digital signature, is attached to a file to certify that the file is from the organization it claims to be from and has not been modified from the original format

Encryption Operations Part 7

- **RSA** - the first public key encryption algorithm developed for commercial use
  - A proprietary model called Rivest
  - One of the most popular public key cryptosystems
  - Has been integrated into both Microsoft Internet Explorer and Netscape Navigator

Encryption Operations Part 8

- **Public Key Infrastructure** - set of hardware, software, and cryptosystems necessary to implement public key encryption
- Common implementations of PKI include:
  - – Systems that issue digital certificates to users/servers
  - – System with computer key values to be included in digital certificates
  - – Tools for managing user enrollment, key generation, and certificate issuance
  - – Verification and return of certificates
  - – Key revocation services

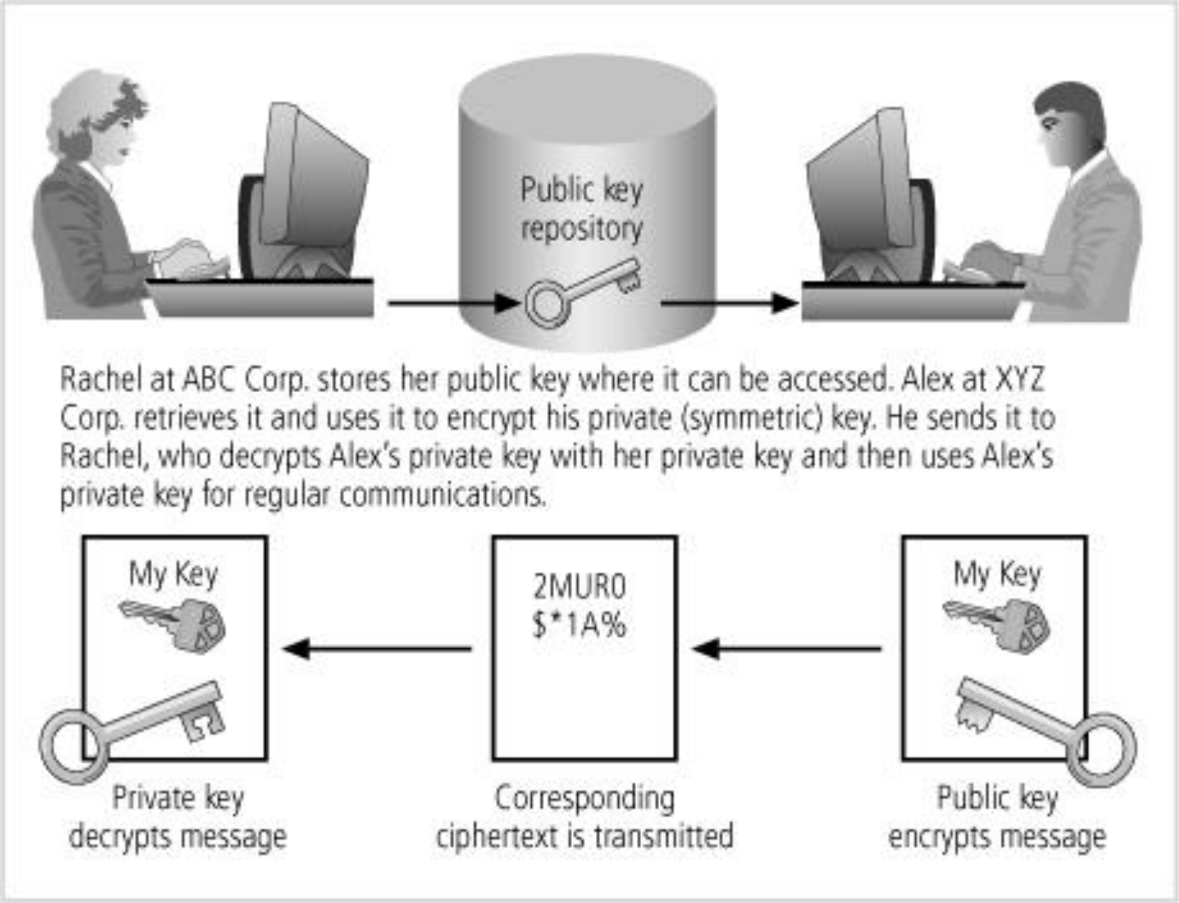
Encryption Operations Part 9

- An organization can increase its cryptographic capabilities by using PKI to provide the following:
  - *Authentication*
  - *Integrity*
  - *Confidentiality*
  - *Authorization*
  - *Nonrepudiation*

Encryption Operations Part 10

- **Hybrid Systems** - Purely asymmetric key encryption is not widely used
    - It is typically employed in conjunction with symmetric key encryption, creating a hybrid encryption system
    - Based on the Diffie-Hellman key exchange method, which provides a way to exchange private keys without exposure to any third parties
    - Asymmetric encryption is used to exchange symmetric keys

Figure 10-14 Hybrid encryption



Rachel at ABC Corp. stores her public key where it can be accessed. Alex at XYZ Corp. retrieves it and uses it to encrypt his private (symmetric) key. He sends it to Rachel, who decrypts Alex's private key with her private key and then uses Alex's private key for regular communications.

My Key
2MUR0
$*1A%
My Key
Private key decrypts message
Corresponding ciphertext is transmitted
Public key encrypts message

Copyright © 2014 Cengage Learning®.

Using Cryptographic Controls

- Cryptographic controls can be used to support several aspects of business:
  - Confidentiality and integrity of e-mail and attachments
  - Authentication, confidentiality, integrity, and nonrepudiation of e-commerce transactions
  - Authentication and confidentiality of remote access through VPN connections
  - A higher standard of authentication when used to supplement access control systems

E-Mail Security

- A number of cryptosystems have been adapted to help secure e-mail:
  - Secure Multipurpose Internet Mail Extensions (S/MIME)
  - Privacy Enhanced Mail (PEM)
  - Pretty Good Privacy (PGP)

Securing the Web Part 1

- **Secure Electronic Transactions (SET)** - developed by MasterCard and VISA to provide protection from electronic payment fraud
- **Secure Sockets Layer (SSL)** - developed by Netscape to provide security for online e-commerce transactions
- **Secure Hypertext Transfer Protocol (SHTTP)** - an encrypted solution to the unsecured version of HTTP
- **Secure Shell (SSH)** - provides security for remote access connections over public networks

Securing the Web Part 2

- **IP Security (IPSec)** - the primary cryptographic authentication and encryption product of the IETF’s IP Protocol Security Working Group
- IPSec combines several different cryptosystems:
  - Diffie-Hellman key exchange for deriving key material between peers on a public network
  - Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties
  - Bulk encryption algorithms
  - Digital certificates signed by a CA

Securing the Web Part 3

- IPSec has two components: 1) IP Security protocol; and 2) the Internet Key Exchange (IKE)
- IPSec works in two modes:
  - **Transport mode** - only IP data is encrypted
  - **Tunnel mode** - the entire IP packet is encrypted
- IPSec and other cryptographic extensions to TCP/IP are often used to support a **virtual private network (VPN)**
  - A VPN is a private, secure network operated over a public and insecure network

Securing Authentication

- **Kerberos** - uses symmetric key encryption to validate an individual user's access to resources
  - Keeps a database containing private keys of clients and servers that are in the authentication domain it supervises
- Kerberos consists of three interacting services:
  - *Authentication Server (AS)*
  - *Key Distribution Center (KDC)*
  - *Kerberos Ticket Granting Service (TGS)*

Securing Authentication (continued)

- Kerberos operates according to the following principles:
  - The KDC knows the secret keys of all clients and servers on the network
  - The KDC initially exchanges information with the client and server by using secret keys
  - Kerberos authenticates a client to a requested service on a server through TGS and by issuing temporary session keys
  - Communications take place between the client and server using the temporary session keys

Managing Cryptographic Controls

- Important managerial issues are:
  - Don’t lose your keys - if keys are compromised, so is all communication
  - Know who you are communicating with
  - It may be illegal to use a specific encryption technique when communicating to some nations
  - Every cryptosystem has weaknesses
  - Give access only to those users, systems, and servers with a business need - a principle known as “least privilege”

Managing Cryptographic Controls (continued)

- Important managerial issues are (cont’d):
  - There is no security in obscurity
- As with all other InfoSec program components
  - Make sure your organization’s use of cryptography is based on well-constructed policy and supported with sound management procedures

Summary Part 1

- Identification is a mechanism that provides basic information about an unknown entity
- Authentication is the validation of a user’s identity
- Authorization is the process of determining which actions an authenticated entity can perform in a particular physical or logical area
- To obtain strong authentication, a system must use two or more authentication methods
- Biometric technologies are evaluated on three criteria: false reject rate, false accept rate, and crossover error rate

Summary Part 2

- A firewall in an InfoSec program is any device that prevents a specific type of information from moving between the outside world and the inside world
- Types of firewalls include packet filtering firewalls, application-level firewalls, stateful inspection firewalls, and dynamic packet filtering firewalls
- A host-based IDPS resides on a particular computer or server and monitors activity on that system
- A signature-based IDPS examines data traffic for activity that matches signatures, which are preconfigured, predetermined attack patterns

Summary Part 3

- Symmetric encryption uses the same key to both encrypt and decrypt a message
- Asymmetric encryption uses two different keys
- A public key infrastructure (PKI) encompasses the entire set of hardware, software, and cryptosystems necessary to implement public key encryption
- A digital certificate is a block of data attached to a file certifying that the file is from the organization it claims to be from and has not been modified