Chapter Twelve

Network Security

Data Communications and Computer Networks: A Business User's Approach

Seventh Edition

After reading this chapter, you should be able to:

- Recognize the basic forms of system attacks
- Recognize the concepts underlying physical protection measures
- Cite the techniques used to control access to computers and networks
- Discuss the strengths and weaknesses of passwords
- List the techniques used to make data secure

After reading this chapter, you should be able to (continued):

- Explain the difference between a substitution-based cipher and a transposition-based cipher
- Outline the basic features of public key cryptography, Advanced Encryption Standard, digital signatures, and the public key infrastructure
- Cite the techniques used to secure communications
- Describe the differences between the frequency hopping spread spectrum technique and the direct sequence spread spectrum technique

After reading this chapter, you should be able to (continued):

- Recognize the importance of a firewall and be able to describe the two basic types of firewall protection
- Recognize the techniques used to secure wireless communications
- List the advantages to a business of having a security policy

Introduction

- While computer systems today have some of the best security systems ever, they are more vulnerable than ever before
- This vulnerability stems from the world-wide access to computer systems via the Internet
- Computer and network security comes in many forms, including encryption algorithms, access to facilities, digital signatures, and using fingerprints and face scans as passwords

Standard System Attacks

- Viruses
  - Computer virus – small program that alters the way a computer operates and often does various types of damage by deleting and corrupting data and program files, or by altering operating system components, so that computer operation is impaired or even halted
  - Many different types of viruses, such as parasitic, boot sector, stealth, polymorphic, and macro

Standard System Attacks (continued)

- Worms
  - Computer worm – program that copies itself from one system to another over a network, without the assistance of a human being
  - Worms usually propagate themselves by transferring from computer to computer via e-mail
- Typically, a virus or a worm is transported as a Trojan horse
  - In other words, hiding inside a harmless-looking piece of code such as an e-mail or an application macro

Standard System Attacks (continued)

- Two popular forms of attacks:
  - Exploiting known operating system vulnerabilities
  - Exploiting known vulnerabilities in application software
- For both of these, software company issues a patch
  - Patch may fix it, or introduce even more holes
    - Either way, bad guys find new holes and exploit

Standard System Attacks (continued)

- Very common way to attack vulnerability is via an e-mail attachment
  - You open the attachment and you launch the virus
- Second common way to attack is to simply scan your computer ports while you are connected to the Internet (either dial-up or non-dial-up)
  - If you have an open port, hacker will download malicious software to your machine

Standard System Attacks (continued)

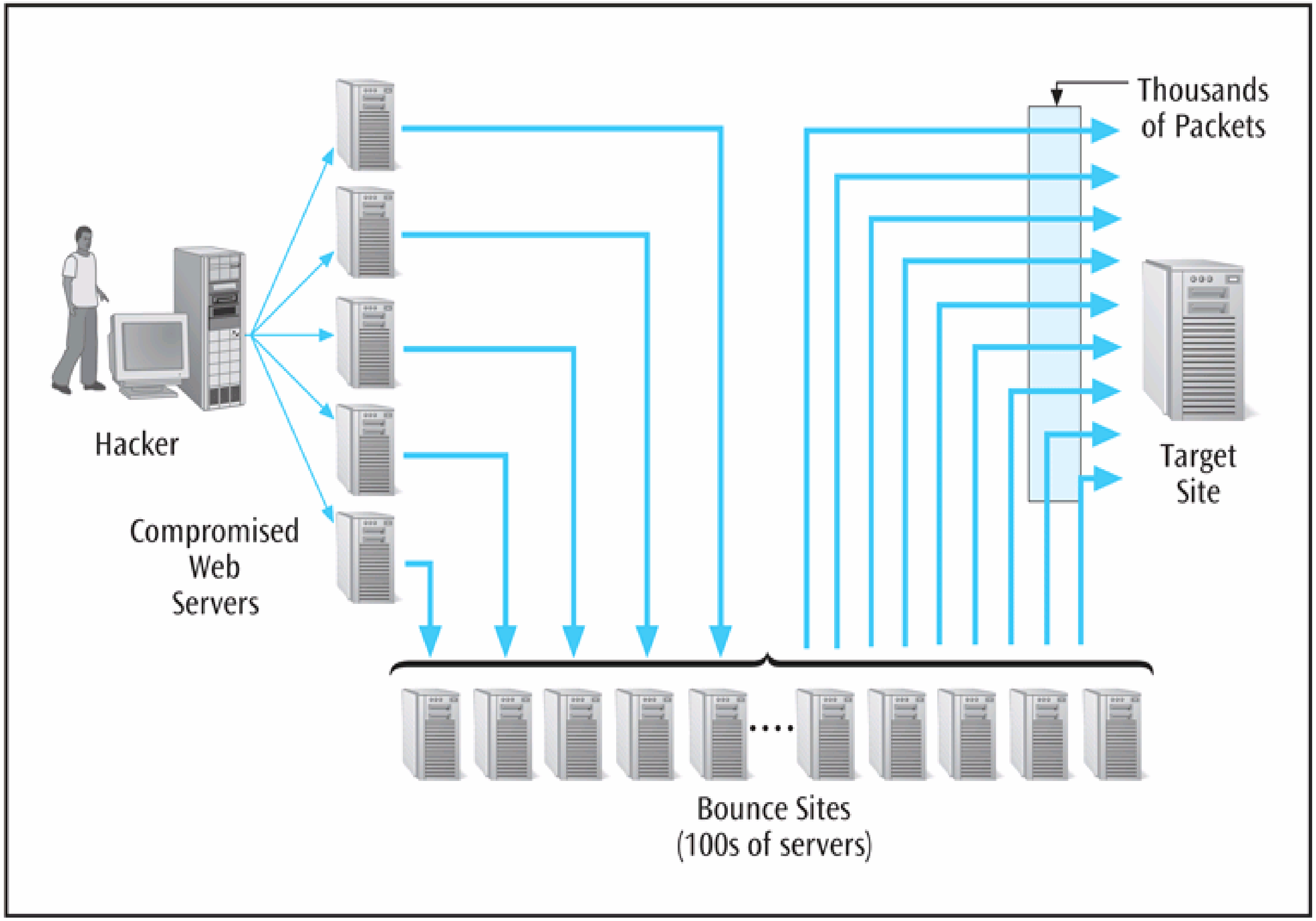
- Other standard attacks
  - Denial of service attacks, or distributed denial of service attacks
    - Bombard computer site with so many messages that site is incapable of answering valid request
  - E-mail bombing
    - User sends an excessive amount of unwanted e-mail to someone
  - Botnets
    - Malicious programs that take over operations on a comprised computer

Standard System Attacks (continued)

- Other standard attacks (continued)
  - Smurfing
    - Nasty technique in which a program attacks a network by exploiting IP broadcast addressing operations
  - Ping storm
    - Condition in which the Internet ping program is used to send a flood of packets to a server

Standard System Attacks (continued)

Figure 12-1
An example of smurfing intended to cripple a Web server



Standard System Attacks (continued)

- Other standard attacks (continued)
  - Spoofing
    - When a user creates a packet that appears to be something else or from someone else
  - Trojan Horse
    - Malicious piece of code hidden inside a seemingly harmless piece of code.
  - Stealing, guessing, and intercepting passwords is also a tried and true form of attack

Standard System Attacks (continued)

- Other standard attacks (continued)
  - Phishing
    - Hackers create emails which look as if they are coming from a legit source when in reality the hacker is trying to get the user to give up ID and password info
  - Pharming
    - Hacker redirects unknowing user to bogus look-alike website

Standard System Attacks (continued)

- Other standard attacks (continued)
  - Rootkit
    - A program that has been installed deep within a user’s operating system; defies detection and takes over the user’s computer
  - Keylogger
    - A software system that secretly captures and records keystrokes made at a user’s keyboard

Physical Protection

- Protection from environmental damage such as floods, earthquakes, and heat
- Physical security such as locking rooms, locking down computers, keyboards, and other devices
- Electrical protection from power surges
- Noise protection from placing computers away from devices that generate electromagnetic interference

Physical Protection (continued)

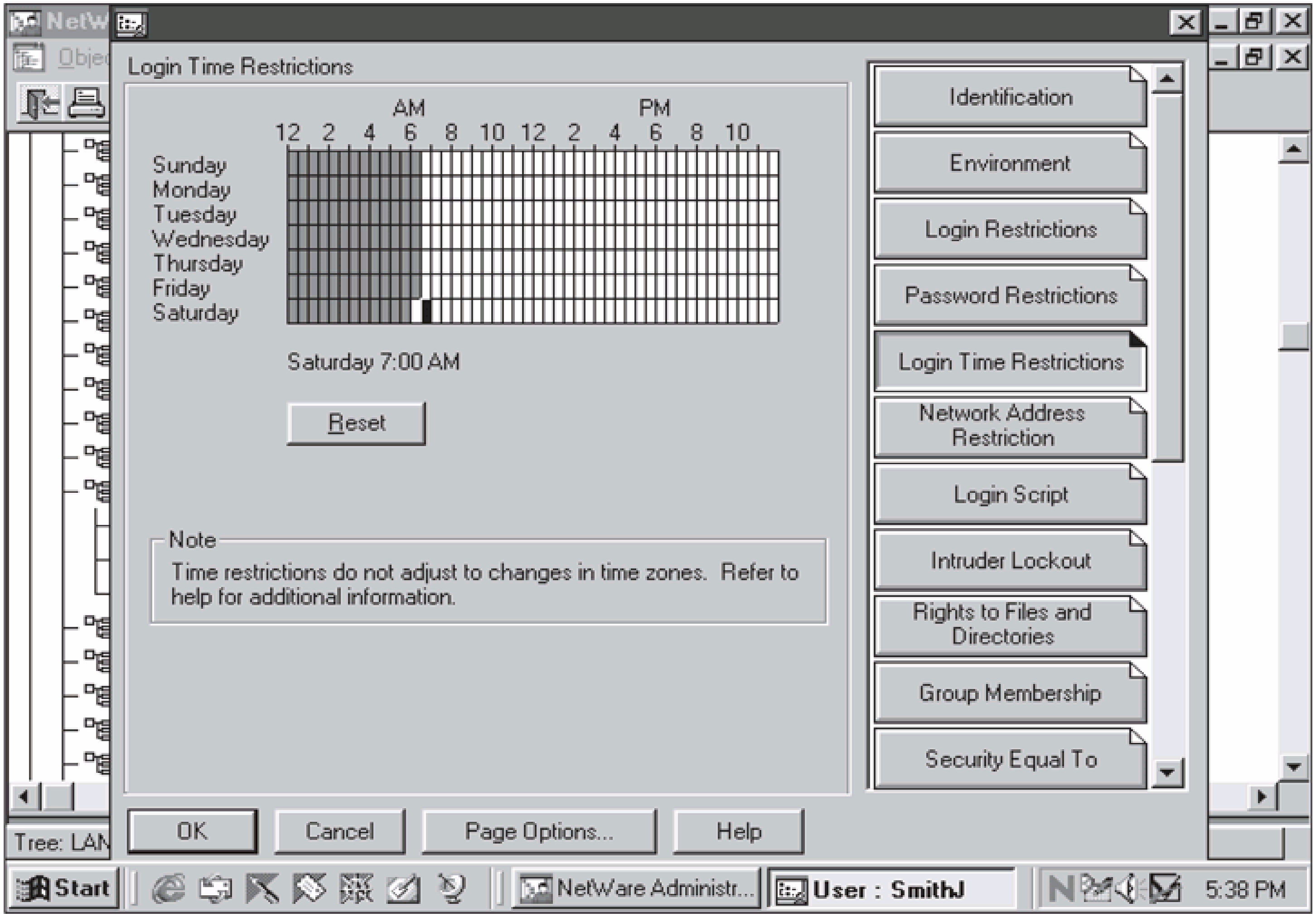
- Surveillance
  - Proper placement of security cameras can deter theft and vandalism
  - Cameras can also provide a record of activities
  - Intrusion detection is a field of study in which specialists try to prevent intrusion and try to determine if a computer system has been violated
  - Honeypot is an indirect form of surveillance
    - Network personnel create a trap, watching for unscrupulous activity

Controlling Access

- Deciding who has access to what
- Limiting time of day access
- Limiting day of week access
- Limiting access from a location, such as not allowing a user to use a remote login during certain periods of time

Controlling Access (continued)

Figure 12-2
Sample dialog box from a network operating system for setting time of day restrictions

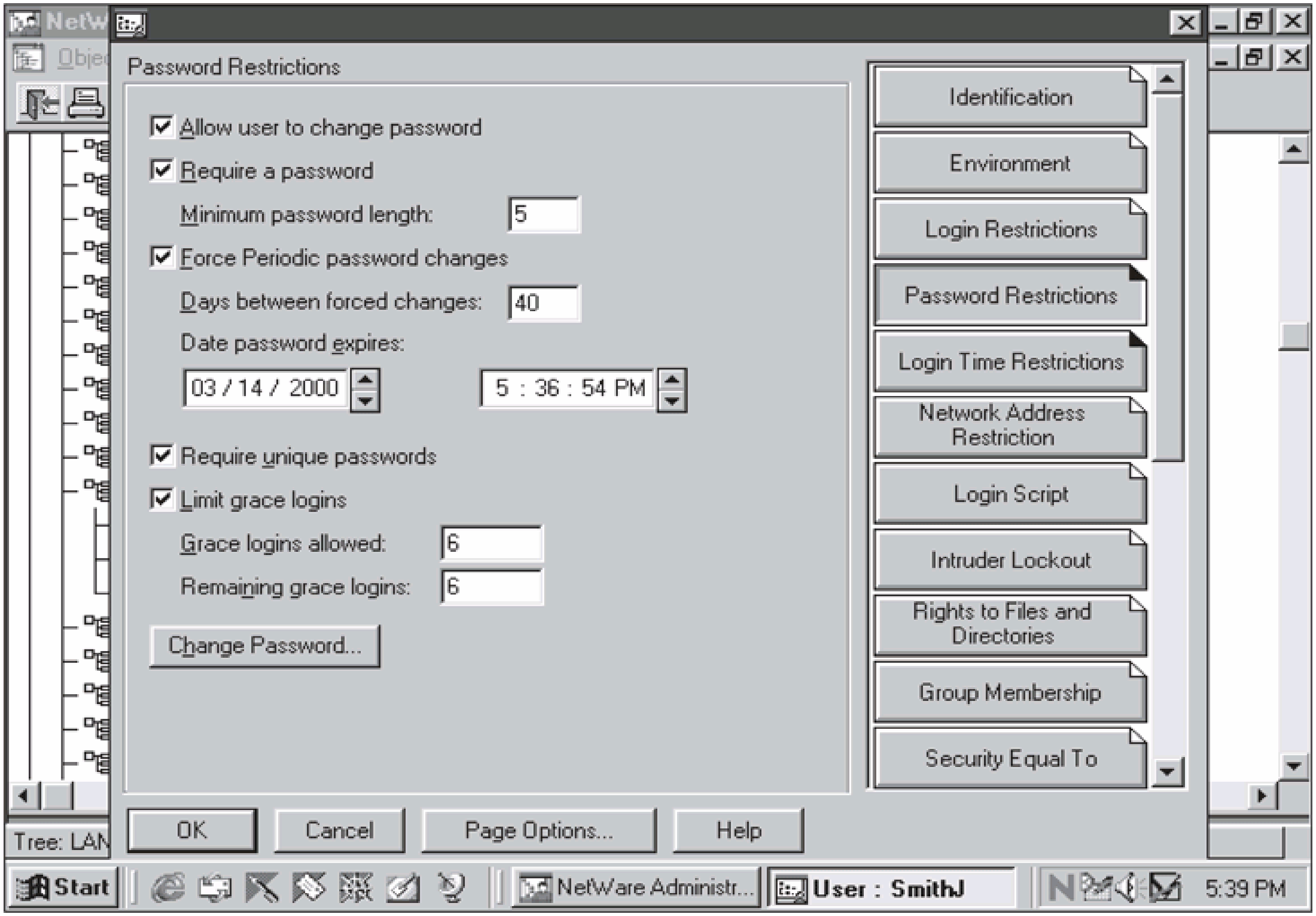


Passwords and ID Systems

- Passwords are the most common form of security and the most abused
- Simple rules help support safe passwords, including:
  - Change your password often
  - Pick a good, random password (minimum 8 characters, mixed symbols)
  - Don’t share passwords or write them down
  - Don’t select names and familiar objects as passwords

Passwords and ID Systems (continued)

Figure 12-3
Controlling a user password with a typical network operating system



Passwords and ID Systems (continued)

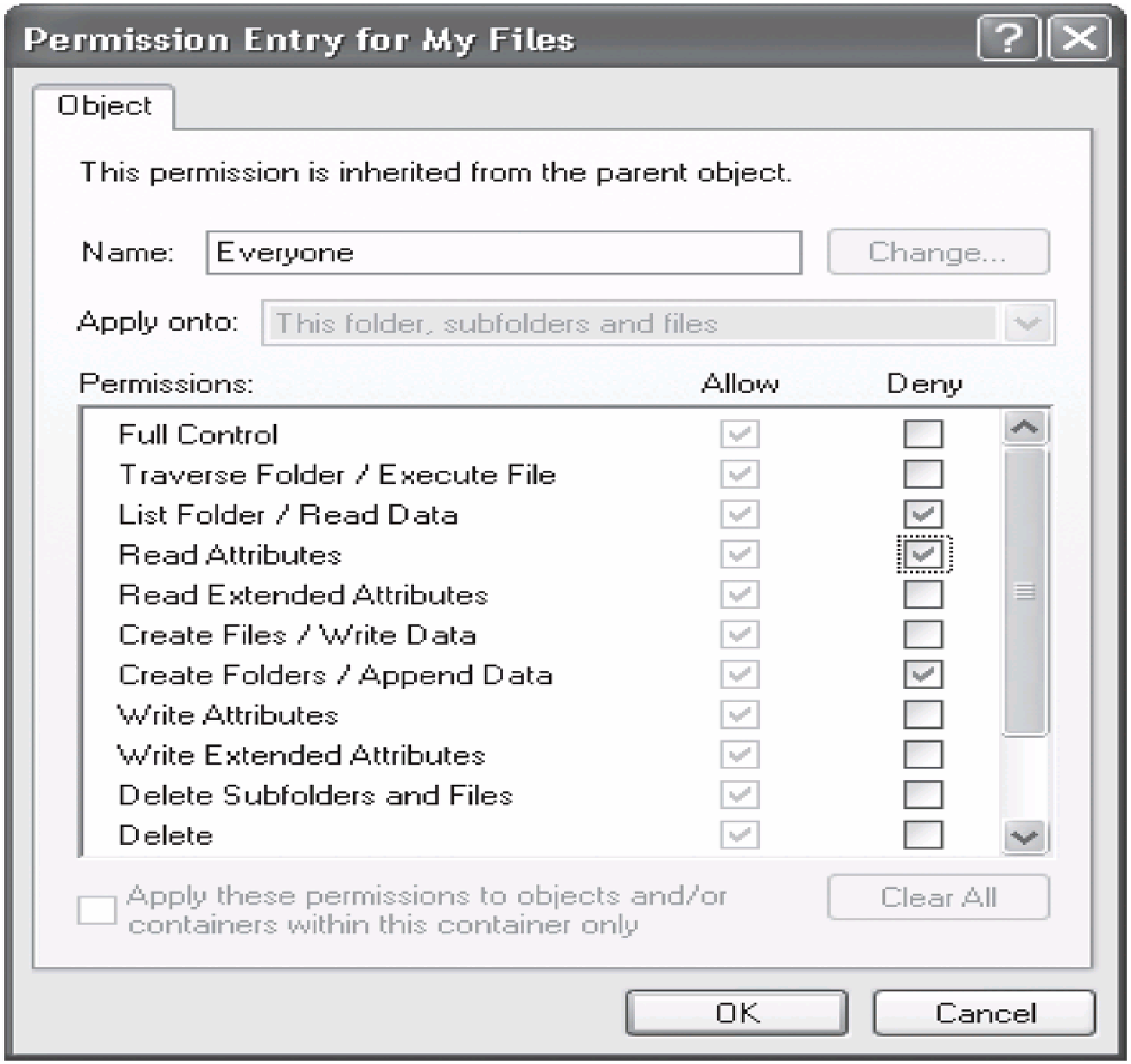
- Many new forms of “passwords” are emerging (biometrics):
  - Fingerprints
  - Face prints
  - Retina scans and iris scans
  - Voice prints
  - Ear prints (?)

Access Rights

- Two basic questions to access rights:
  - Who and how?
- Who do you give access rights to?
  - No one, group of users, entire set of users?
- How does a user or group of users have access?
  - Read, write, delete, print, copy, execute?
- Most network operating systems have a powerful system for assigning access rights

Access Rights (continued)

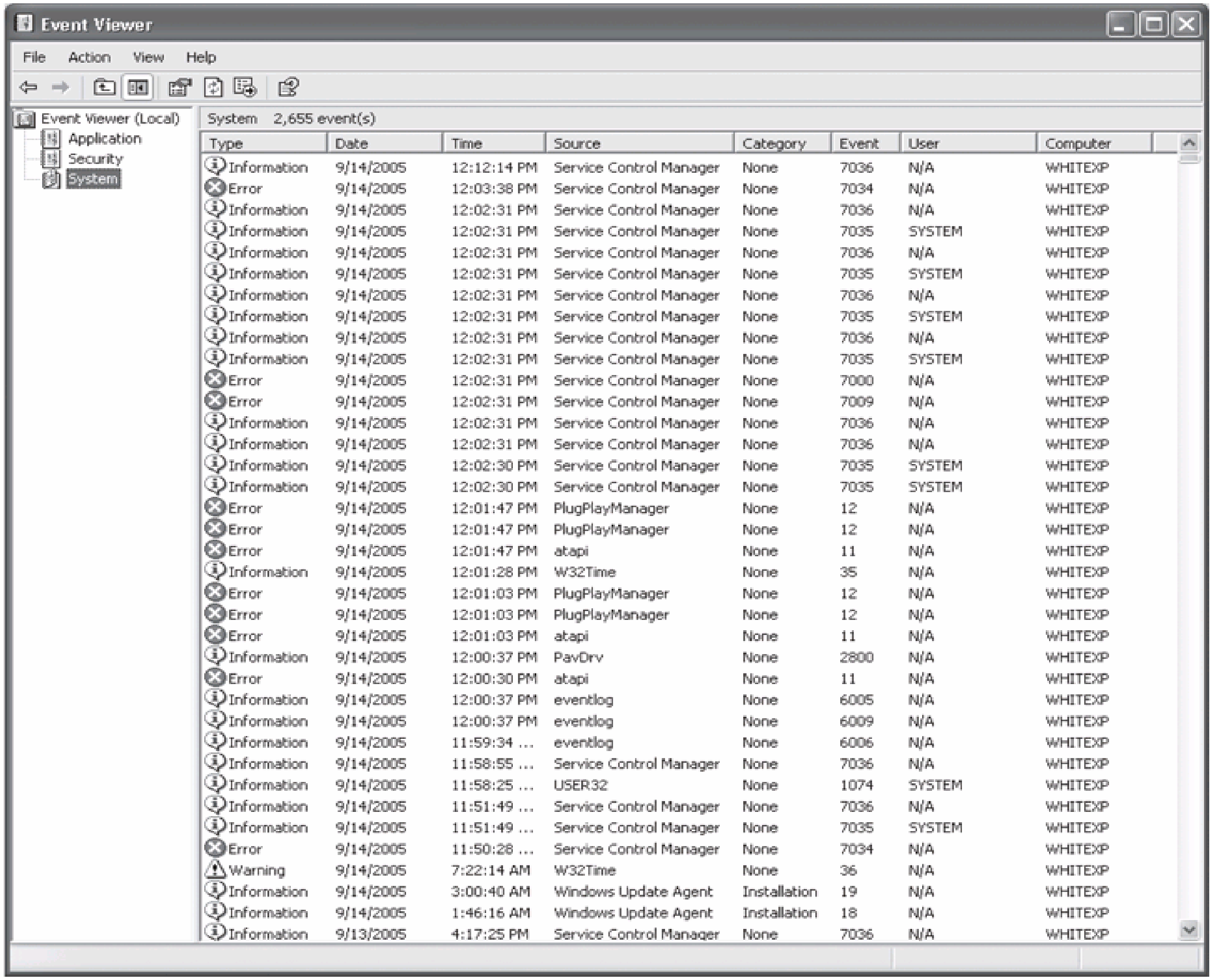
Figure 12-4
A network operating system assigning access rights to a resource



Auditing

- Creating a computer or paper audit can help detect wrongdoing
- Auditing can also be used as a deterrent
- Many network operating systems allow the administrator to audit most types of transactions
- Many types of criminals have been caught because of computer-based audits

Auditing (continued)



Type	Date	Time	Source	Category	Event	User	Computer
Information	9/14/2005	12:12:14 PM	Service Control Manager	None	7036	N/A	WHITEXP
Error	9/14/2005	12:03:38 PM	Service Control Manager	None	7034	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Error	9/14/2005	12:02:31 PM	Service Control Manager	None	7000	N/A	WHITEXP
Error	9/14/2005	12:02:31 PM	Service Control Manager	None	7009	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:31 PM	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	12:02:30 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Information	9/14/2005	12:02:30 PM	Service Control Manager	None	7035	SYSTEM	WHITEXP
Error	9/14/2005	12:01:47 PM	PlugPlayManager	None	12	N/A	WHITEXP
Error	9/14/2005	12:01:47 PM	PlugPlayManager	None	12	N/A	WHITEXP
Error	9/14/2005	12:01:47 PM	atapi	None	11	N/A	WHITEXP
Information	9/14/2005	12:01:28 PM	W32Time	None	35	N/A	WHITEXP
Error	9/14/2005	12:01:03 PM	PlugPlayManager	None	12	N/A	WHITEXP
Error	9/14/2005	12:01:03 PM	PlugPlayManager	None	12	N/A	WHITEXP
Error	9/14/2005	12:01:03 PM	atapi	None	11	N/A	WHITEXP
Information	9/14/2005	12:00:37 PM	PavDrv	None	2800	N/A	WHITEXP
Error	9/14/2005	12:00:30 PM	atapi	None	11	N/A	WHITEXP
Information	9/14/2005	12:00:37 PM	eventlog	None	6005	N/A	WHITEXP
Information	9/14/2005	12:00:37 PM	eventlog	None	6009	N/A	WHITEXP
Information	9/14/2005	11:59:34 ...	eventlog	None	6006	N/A	WHITEXP
Information	9/14/2005	11:58:55 ...	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	11:58:25 ...	USER32	None	1074	SYSTEM	WHITEXP
Information	9/14/2005	11:51:49 ...	Service Control Manager	None	7036	N/A	WHITEXP
Information	9/14/2005	11:51:49 ...	Service Control Manager	None	7035	SYSTEM	WHITEXP
Error	9/14/2005	11:50:28 ...	Service Control Manager	None	7034	N/A	WHITEXP
Warning	9/14/2005	7:22:14 AM	W32Time	None	36	N/A	WHITEXP
Information	9/14/2005	3:00:40 AM	Windows Update Agent	Installation	19	N/A	WHITEXP
Information	9/14/2005	1:46:16 AM	Windows Update Agent	Installation	18	N/A	WHITEXP
Information	9/13/2005	4:17:25 PM	Service Control Manager	None	7036	N/A	WHITEXP

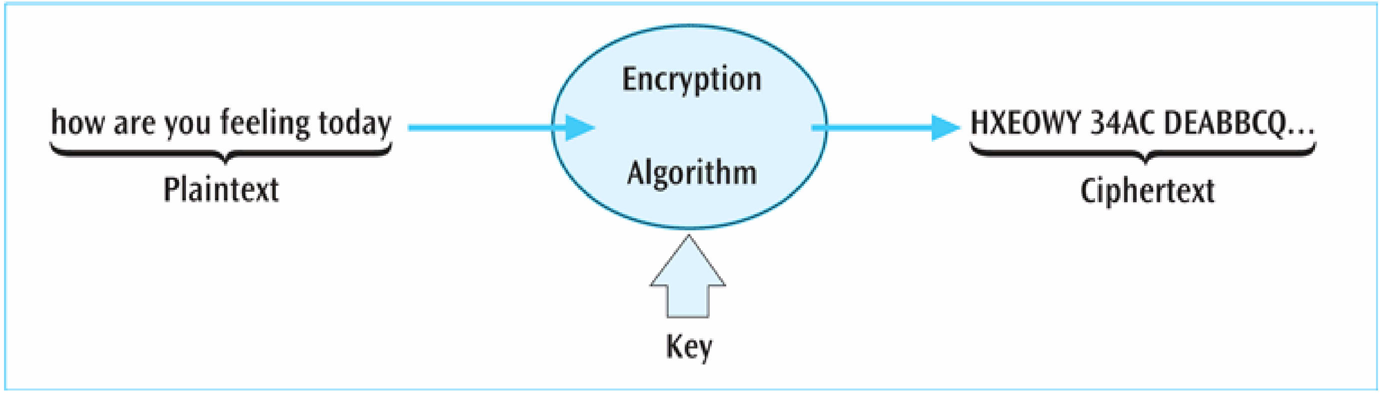
Figure 12-5
Windows Event Viewer example

Basic Encryption and Decryption Techniques

- Cryptography – study of creating and using encryption and decryption techniques
- Plaintext – data before any encryption has been performed
- Ciphertext – data after encryption has been performed
- The key is the unique piece of information that is used to create ciphertext and decrypt the ciphertext back into plaintext

Basic Encryption and Decryption Techniques (continued)

Figure 12-6
Basic encryption and decryption procedure



Monoalphabetic Substitution-Based Ciphers

- Monoalphabetic substitution-based ciphers replace a character or characters with a different character or characters, based upon some key
  - Replacing: `abcdefghijklmnopqrstuvwxyz`
    with: `POIUYTREWQLKJHGFDSAMNBVCXZ`
  - The message: `how about lunch at noon`
    encodes into: `EGVPO GNMKN HIEPM HGGH`

Polyalphabetic Substitution-Based Ciphers

- Similar to monoalphabetic ciphers except multiple alphabetic strings are used to encode the plaintext
- Example – matrix of strings, 26 rows by 26 characters or columns can be used
- A key such as COMPUTERSCIENCE is placed repeatedly over the plaintext
  - `COMPUTERSCIENCECOMPUTERSCIENCECOMPUTER`
  - `thisclassondatacommunicationsisthebest`

Polyalphabetic Substitution-Based Ciphers (continued)

- To encode the message, take the first letter of the plaintext, t, and the corresponding key character immediately above it, C
  - Go to row C column t in the 26x26 matrix and retrieve the ciphertext character V
- Continue with the other characters in plaintext

Polyalphabetic Substitution-Based Ciphers (continued)

Table 12-1

An example of a Vigenére 26 × 26 ciphertext character matrix

Key Character	Plaintext Letters																									
	A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**	**N**	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
...	...																									
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Transposition-Based Ciphers

- In a transposition-based cipher, the order of the plaintext is not preserved
- As a simple example, select a key such as COMPUTER
  - Number the letters of the word COMPUTER in the order they appear in the alphabet

```
1 4 3 5 8 7 2 6
C O M P U T E R
```

Transposition-Based Ciphers (continued)

- Now take the plaintext message and write it under the key

1	4	3	5	8	7	2	6
C	O	M	P	U	T	E	R
t	h	i	s	i	s	t	h
e	b	e	s	t	c	l	a
s	s	i	h	a	v	e	e
v	e	r	t	a	k	e	n

Transposition-Based Ciphers (continued)

- Then read the ciphertext down the columns, starting with the column numbered 1, followed by column number 2

  TESVTLEEIEIRHBSESSHTHAENSCVKITAA

Public Key Cryptography

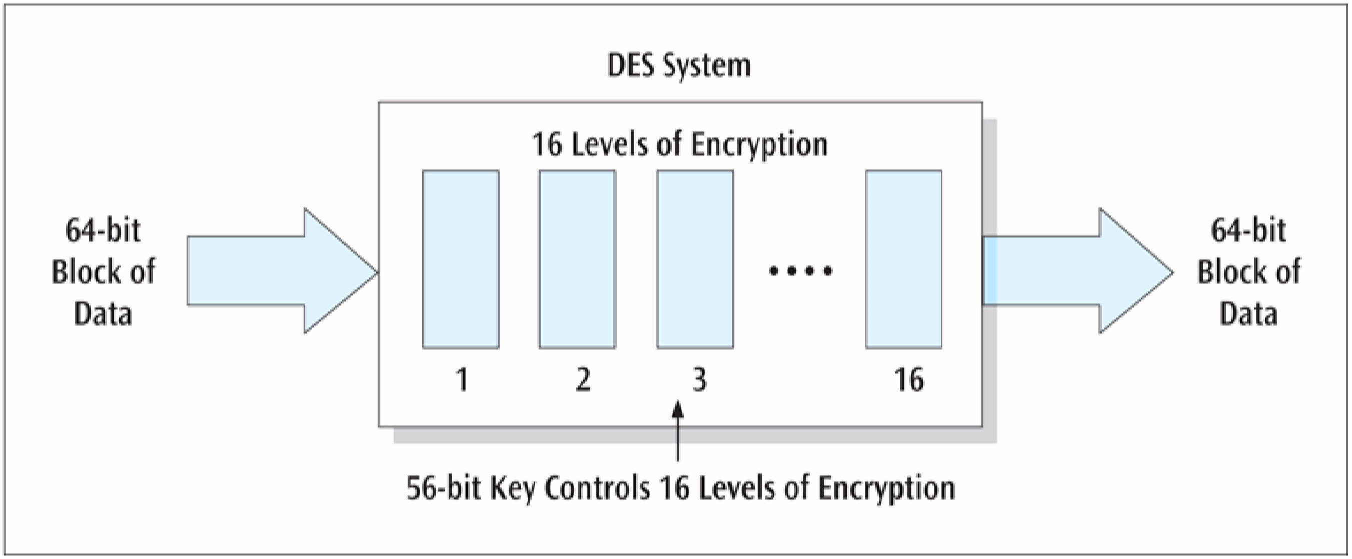
- Very powerful encryption technique in which two keys are used
  - First key (the public key) encrypts the message
  - Second key (the private key) decrypts the message
- Not possible to deduce one key from the other
- Not possible to break code given public key
- If you want someone to send you secure data, give them your public key, you keep the private key
- Secure Sockets Layer on the Internet is a common example of public key cryptography

Data Encryption Standard and Advanced Encryption Standard

- Created in 1977 and in operation into the 1990s, the Data Encryption Standard took a 64-bit block of data and subjected it to 16 levels of encryption
- The choice of encryption performed at each of the 16 levels depends on the 56-bit key applied
- Even though 56 bits provides over 72 quadrillion combinations, a system using this standard has been cracked (in 1998 by Electronic Frontier Foundation in 3 days)

Data Encryption Standard and Advanced Encryption Standard (continued)

Figure 12-7
The basic operations of the Data Encryption Standard



Data Encryption Standard and Advanced Encryption Standard (continued)

- Triple-DES
  - More powerful data encryption standard
  - Data is encrypted using DES three times:
    - First time by the first key
    - Second time by a second key
    - Third time by the first key again
      - Can also have 3 unique keys
  - While virtually unbreakable, triple-DES is CPU intensive
  - With more smart cards, cell phones, and PDAs, a faster (and smaller) piece of code is highly desirable

Data Encryption Standard and Advanced Encryption Standard (continued)

- Advanced Encryption Standard (AES)
  - Selected by the U.S. government to replace DES
  - National Institute of Standards and Technology selected the algorithm Rijndael (pronounced rain-doll) in October 2000 as the basis
  - Has more elegant mathematical formulas, requires only one pass, and was designed to be fast, unbreakable, and able to support even the smallest computing device

Data Encryption Standard and Advanced Encryption Standard (continued)

- Advanced Encryption Standard (AES) (continued)
  - Key size of AES: 128, 192, or 256 bits
  - Estimated time to crack (assuming a machine could crack a DES key in 1 second) : 149 trillion years
  - Very fast execution with very good use of resources

Digital Signatures

- Document to be signed is sent through a complex mathematical computation that generates a hash
- Hash is encoded with owner's private key then stored
- To prove future ownership, stored hash is decoded using the owner's public key and that hash is compared with a current hash of the document
- If the two hashes agree, document belongs to the owner
- U.S. accepts digitally signed documents as legal proof (for some types of documents)

Pretty Good Privacy (PGP)

- Encryption software created by Philip Zimmermann
- Can be used to secure email and other data files
- Employs public key cryptography and digital signatures
- Available to anyone in the U.S. for free

Kerberos

- An authentication protocol designed to work on client/server networks
- Employs private key cryptography (one key both encrypts and decrypts)
- Another free software for use in the U.S.
- Many operating systems provide Kerberos for authentication of users and services

Public Key Infrastructure

- Combination of encryption techniques, software, and services that involves all the necessary pieces to support digital certificates, certificate authorities, and public key generation, storage, and management
- A certificate, or digital certificate, is an electronic document, similar to a passport, that establishes your credentials when you are performing transactions

Public Key Infrastructure (continued)

- A digital certificate contains your name, serial number, expiration dates, copy of your public key, and digital signature of certificate-issuing authority.
- Certificates are usually kept in a registry so other users may check them for authenticity.

Public Key Infrastructure (continued)

- Certificates are issued by a certificate authority (CA)
  - A CA is either specialized software on a company network or a trusted third party
- Let’s say you want to order something over the Internet
  - The Web site wants to make sure you are legit, so the Web server requests your browser to sign the order with your private key (obtained from your certificate)

Public Key Infrastructure (continued)

- Let’s say you want to order something over the Internet (continued)
  - The Web server then requests your certificate from the third party CA, validates that certificate by verifying third party’s signature, then uses that certificate to validate the signature on your order
  - The user can do the same procedure to make sure the Web server is not a bogus operation
- A certificate revocation list is used to “deactivate” a user’s certificate

Public Key Infrastructure (continued)

- Applications that could benefit from PKI:
  – Web transactions
  – Virtual private networks
  – Electronic mail
  – Client-server applications
  – Banking transactions

Steganography

- The art and science of hiding information inside other, seemingly ordinary messages or documents
- Unlike sending an encrypted message, you do not know when steganography is hiding a secret message within a document
- Examples include creating a watermark over an image or taking “random” pixels from an image and replacing them with the hidden data

Securing Communications

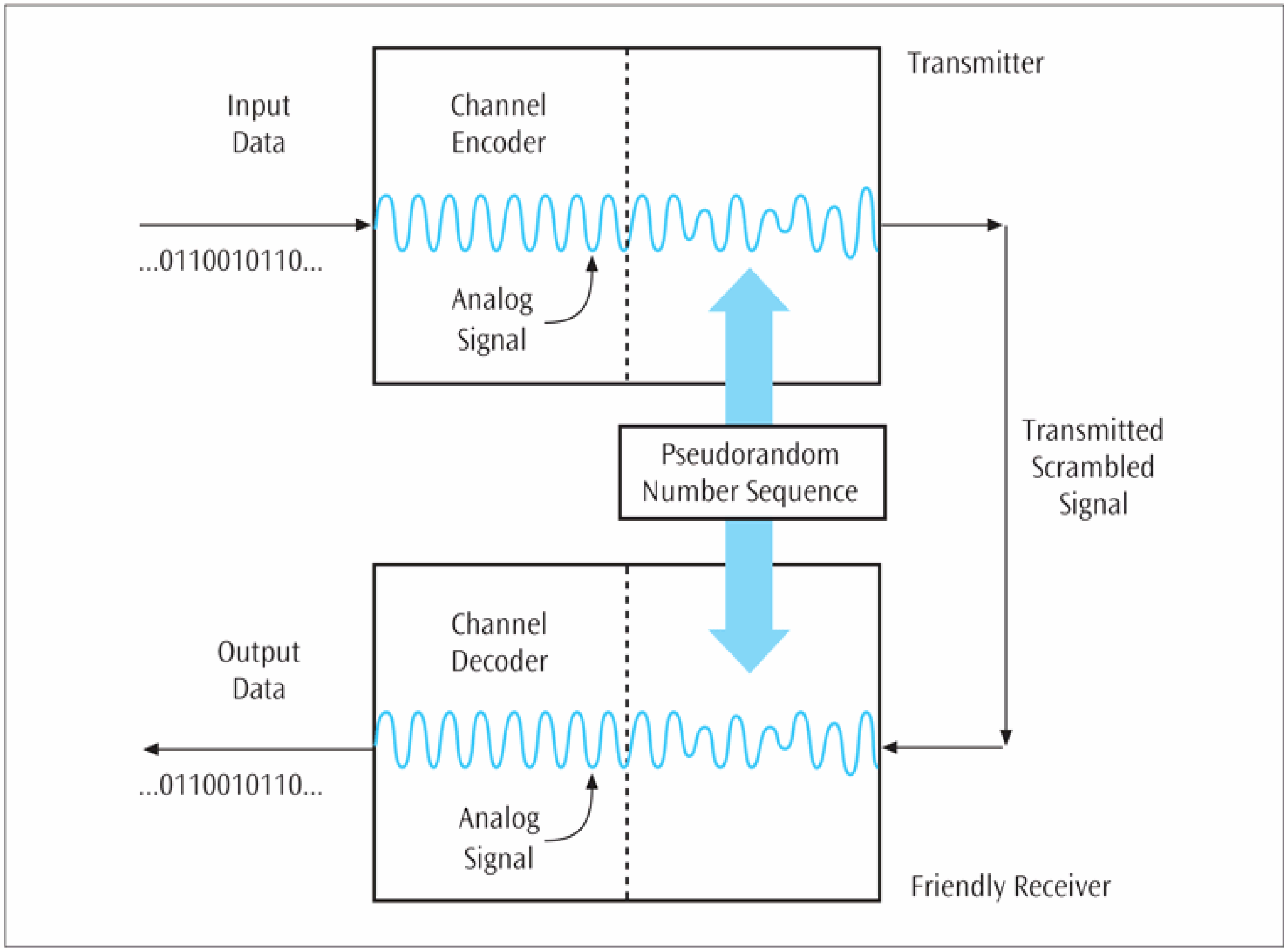
- So far we have examined standard system attacks, physical protection, controlling access, and securing data
  - Now let's examine securing communications
- One way to secure the transfer of data is to scramble the signal as it is being transmitted
  - This is called spread spectrum technology

Spread Spectrum Technology

- A secure encoding technique that uses multiple frequencies or codes to transmit data.
- Two basic spread spectrum technologies:
  - Frequency hopping spread spectrum
  - Direct sequence spread spectrum

Spread Spectrum Technology (continued)

Figure 12-8
Basic operation of a frequency hopping spread spectrum receiver and transmitter system

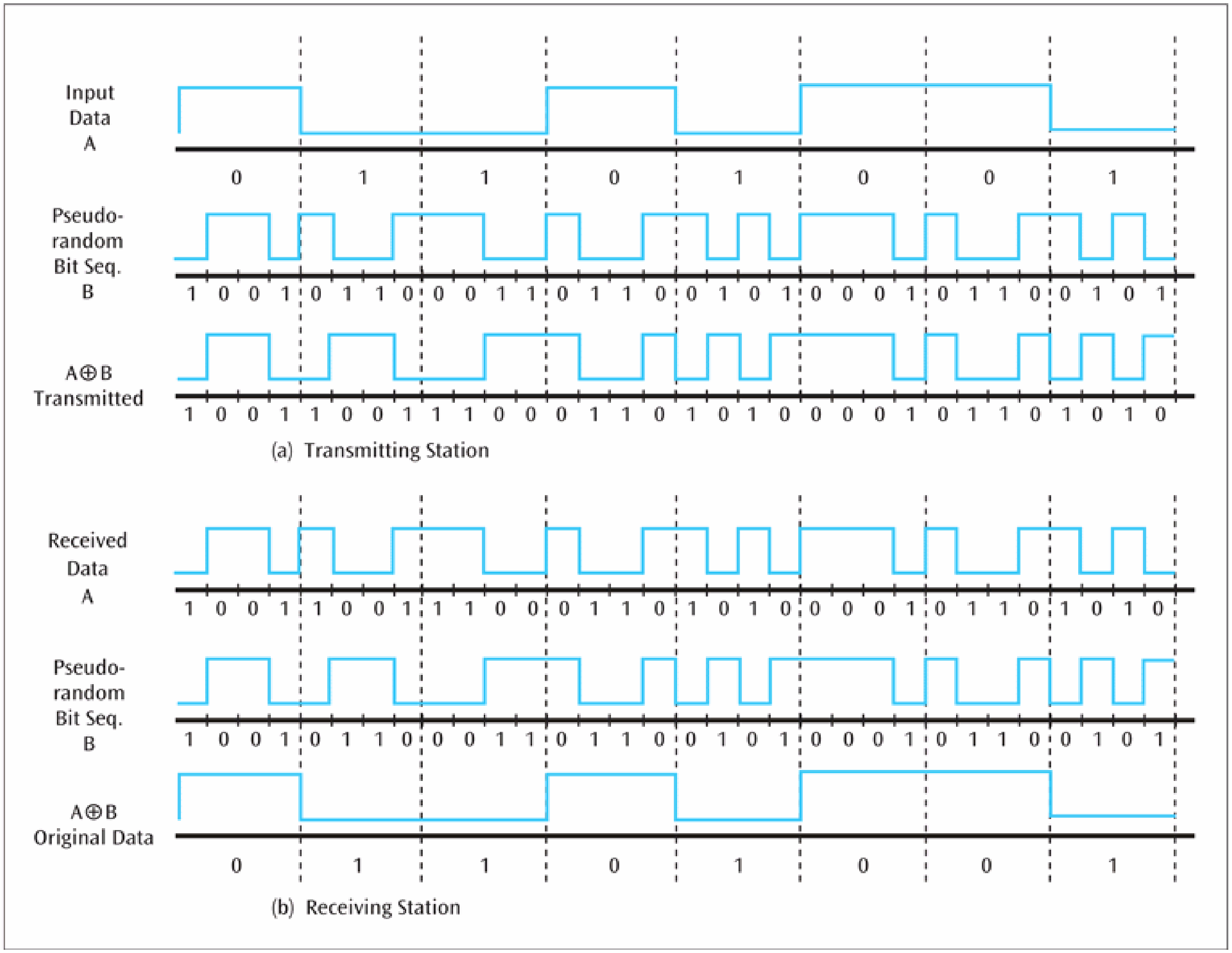


Spread Spectrum Technology (continued)

- Direct sequence spread spectrum
  - This technology replaces each binary 0 and binary 1 with a unique pattern, or sequence, of 1s and 0s
  - For example, one transmitter may transmit the sequence 10010100 for each binary 1, and 11001010 for each binary 0
    - Another transmitter may transmit the sequence 11110000 for each binary 1, and 10101010 for each binary 0

Spread Spectrum Technology (continued)

Figure 12-9
Example of binary data as it is converted into a direct sequence spread spectrum and back



Guarding Against Viruses

- Signature-based scanners look for particular virus patterns or signatures and alert the user
- Terminate-and-stay-resident programs run in the background constantly watching for viruses and their actions
- Multi-level generic scanning is a combination of antivirus techniques including intelligent checksum analysis and expert system analysis

Firewalls

- A system or combination of systems that supports an access control policy between two networks
- Can limit the types of transactions that enter a system, as well as the types of transactions that leave a system
- Can be programmed to stop certain types or ranges of IP addresses, as well as certain types of TCP port numbers (applications)

Three Basic Types of Firewalls

1. Packet filter firewall – essentially a router that has been programmed to filter out or allow to pass certain IP addresses or TCP port numbers
2. Proxy server – more advanced firewall that acts as a doorman into a corporate network
   - Any external transaction that requests something from the corporate network must enter through the proxy server
   - Proxy servers are more advanced but make external accesses slower

Three Basic Types of Firewalls (continued)

3. Application layer – inspects all packets coming into or leaving a connection using the application layer of the TCP/IP protocol suite
   – Goes beyond IP addresses and TCP port numbers and inspects packet to see to which application it belongs

Firewalls (continued)

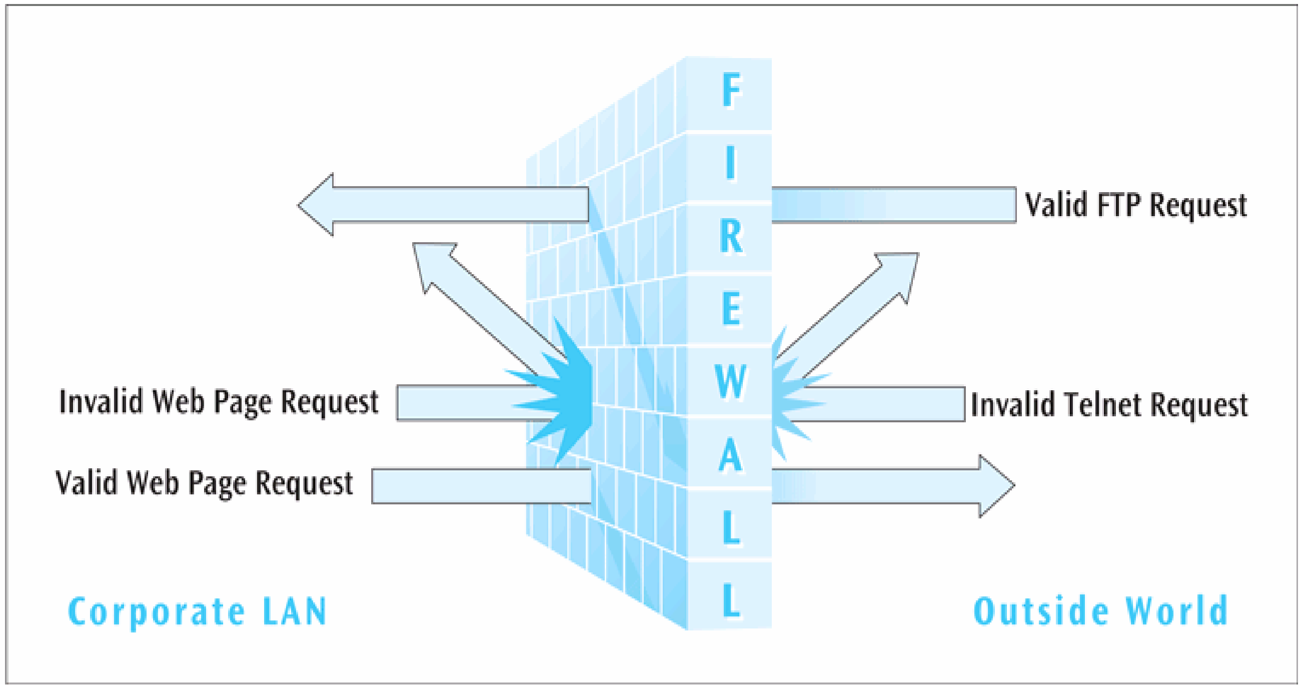
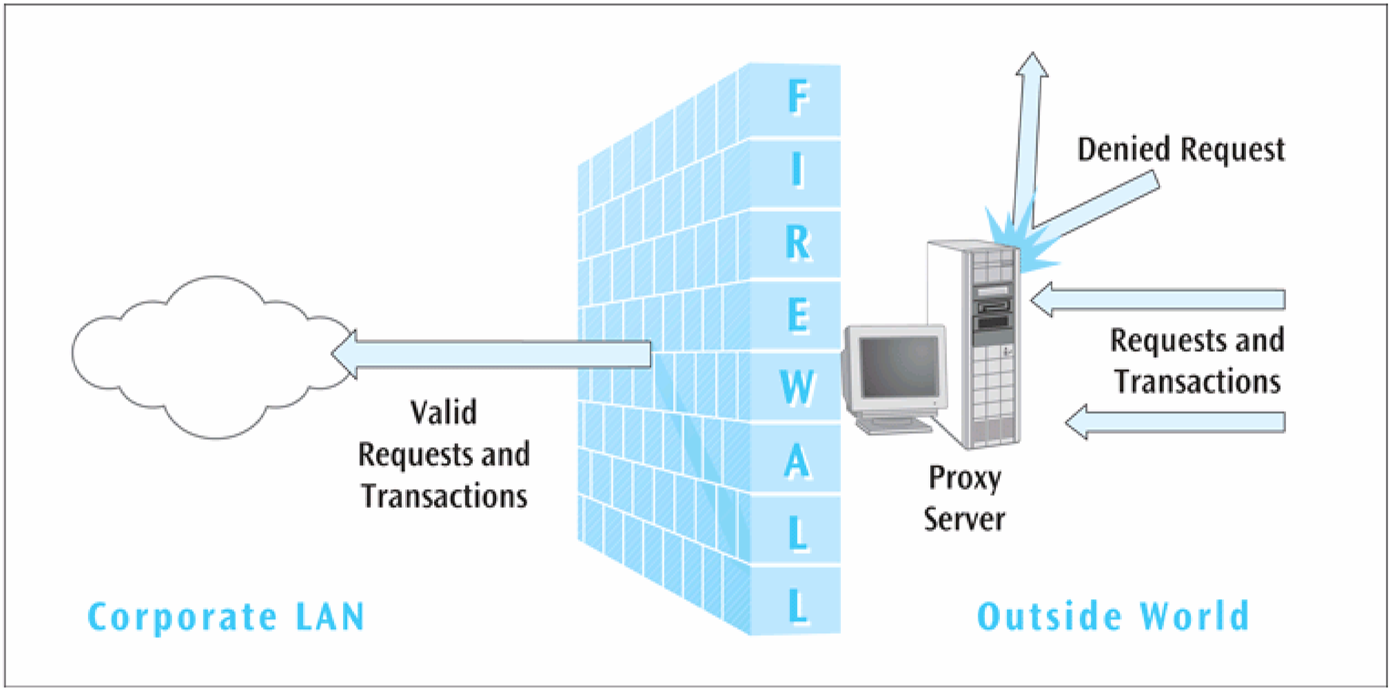


Figure 12-10
A firewall as it stops certain internal and external transactions

Firewalls (continued)

Figure 12-11
The proxy server sitting outside the protection of the corporate network



Wireless Security

- How do you make a wireless LAN secure?
  - WEP (Wired Equivalency Protocol) was the first security protocol used with wireless LANs
    - It had weak 40-bit static keys and was too easy to break
  - WPA (Wi-Fi Protected Access) replaced WEP
    - Major improvement including dynamic key encryption and mutual authentication for wireless clients

Wireless Security (continued)

- Both of these should eventually give way to a new protocol created by the IEEE
  - IEEE 802.11i, or WPA2
- WPA2 allows keys, encryption algorithms, and negotiation to be dynamically assigned
- Also, AES encryption based on the Rijndael algorithm with 128-, 192-, or 256-bit keys is incorporated

Security Policy Design Issues

- What is the company's desired level of security?
- How much money is the company willing to invest in security?
- If the company is serious about restricting access through an Internet link, what about restricting access through all other entry ways?
- The company must have a well-designed security policy

Network Security In Action: Making Wireless LANs Secure

- Recall Hannah the network administrator from Chapters Seven, Eight, and Nine – Now her company wants to add a wireless LAN to their system and make it secure
- She needs to protect herself from war drivers
- Should she use WEP?
- What about Cisco’s LEAP (Lightweight Extensible Authentication Protocol)?

Network Security In Action: Making Wireless LANs Secure (continued)

- What about WPA?
  - If she decides to use WPA, where does she have to install the WPA software?
    - In the user's laptop?
    - At the wireless access point?
    - At the network server?
    - All the above?
- What about WPA2?
  - Too new? Compatible software and hardware systems?

Summary

- Network security continues to be an increasingly important topic, particularly with increase in network interconnectivity
- Three common system attacks are:
  - Attacking known OS and application software vulnerabilities
  - Denial of service attacks
  - Using valid user accounts for unauthorized purposes
- Network personnel and users must take physical protection measures
- Controlling access to computer system and its network is an essential aspect of network security

Summary (continued)

- Passwords and other ID systems are very common access-controlling security techniques
  - Passwords can be stolen and used by unscrupulous parties
- Most computer systems apply access rights to resources of the system and users
- Software that conducts continuous audit of network transactions creates electronic trail that companies can use when trying to catch malicious users
- Providing security for system data is just as important as securing the system itself

Summary (continued)

- Public key cryptography uses two keys
  - One key to encode messages
  - Second key to decode messages
- Data Encryption Standard was created in 1977 and uses a 56-bit key to encrypt data transmitted between two business locations
- Digital signatures use public key cryptography and can be used to verify that a given document belongs to given person
- Pretty Good Privacy is free encryption software that allows regular users as well as commercial users to encrypt and decrypt everyday transmissions

Summary (continued)

- Kerberos is secret key encryption technique that can be used by commercial application programs to verify that a user is who he or she claims to be
- Public key infrastructure uses public key cryptography, digital signatures, and digital certificates to enable secure passage of data over unsecured networks
- Steganography is study of hiding secret data within an unrelated document, for example, hiding bits of a message within pixels of an image
- Along with securing network data, it is imperative to secure network communications

Summary (continued)

- In order to secure communications, network administrators and users must be aware of standard computer attacks and viruses that can damage computer systems
- Another means of securing communications is a firewall, a system or combination of systems that supports an access control policy between two networks
- Securing wireless networks is a new and exciting field of study
- A proper network security design helps corporate network staff by clearly delineating which network transactions are acceptable