E-commerce

business. technology. society.

Fourth Edition

Kenneth C. Laudon

Carol Guercio Traver

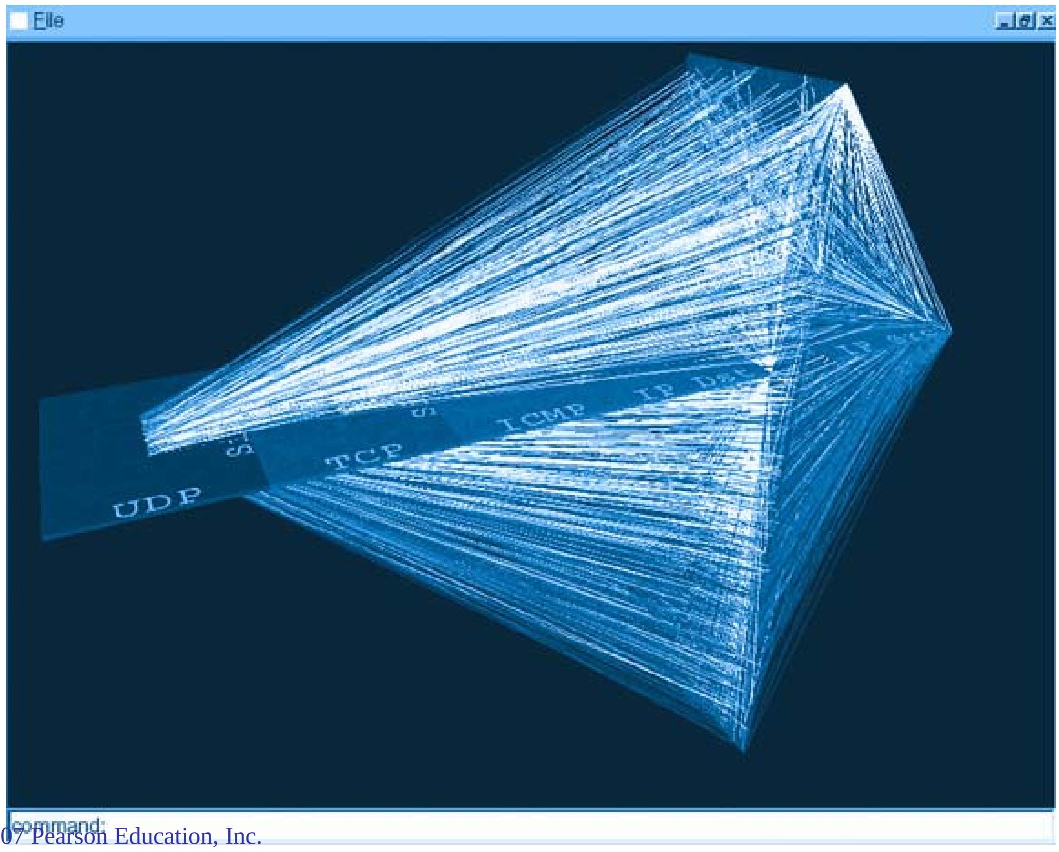
Chapter 5

Online Security System

Cyberwar in Estonia
Class Discussion

- What is a DDoS attack? Why did it prove to be so effective against Estonia?
- What are botnets? Why are they used in DDoS attacks?
- What percentage of computers belong to botnets? What percentage of spam is sent by botnets?
- Can anything be done to stop DDoS attacks?

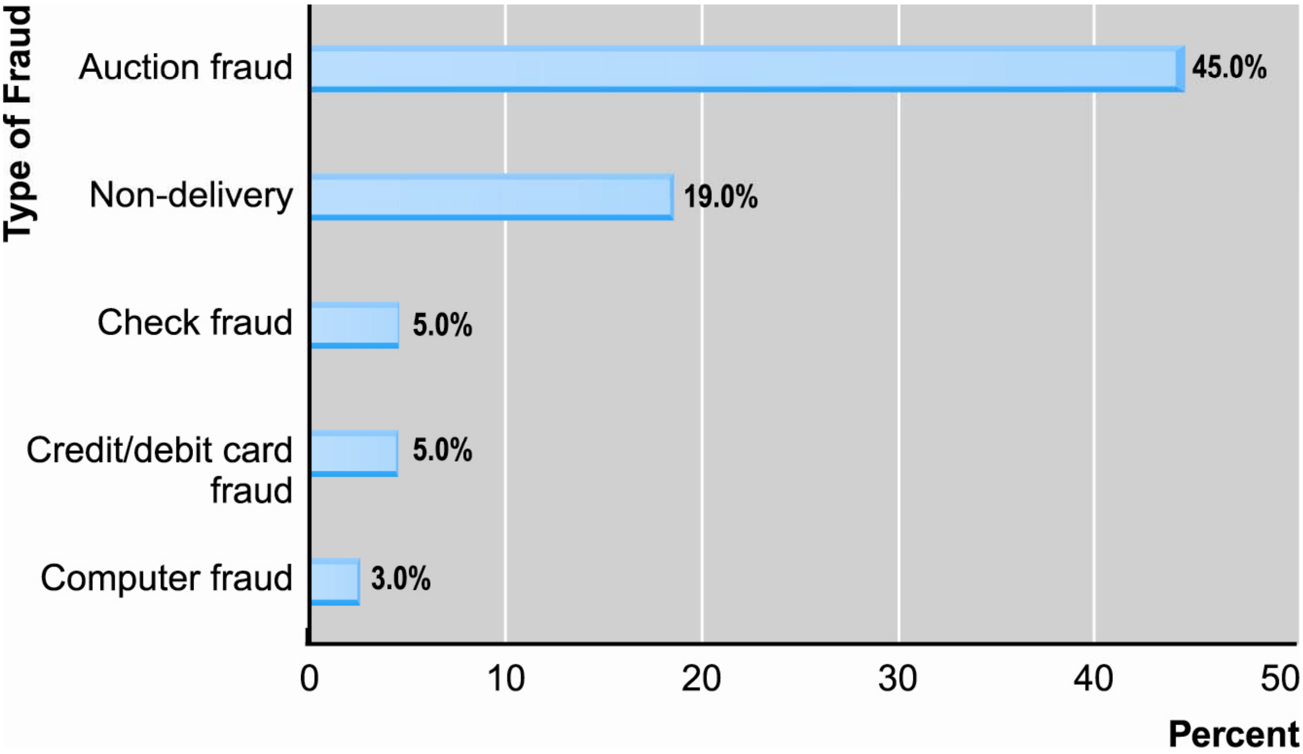
Computer-generated Simulation of a DDoS Attack



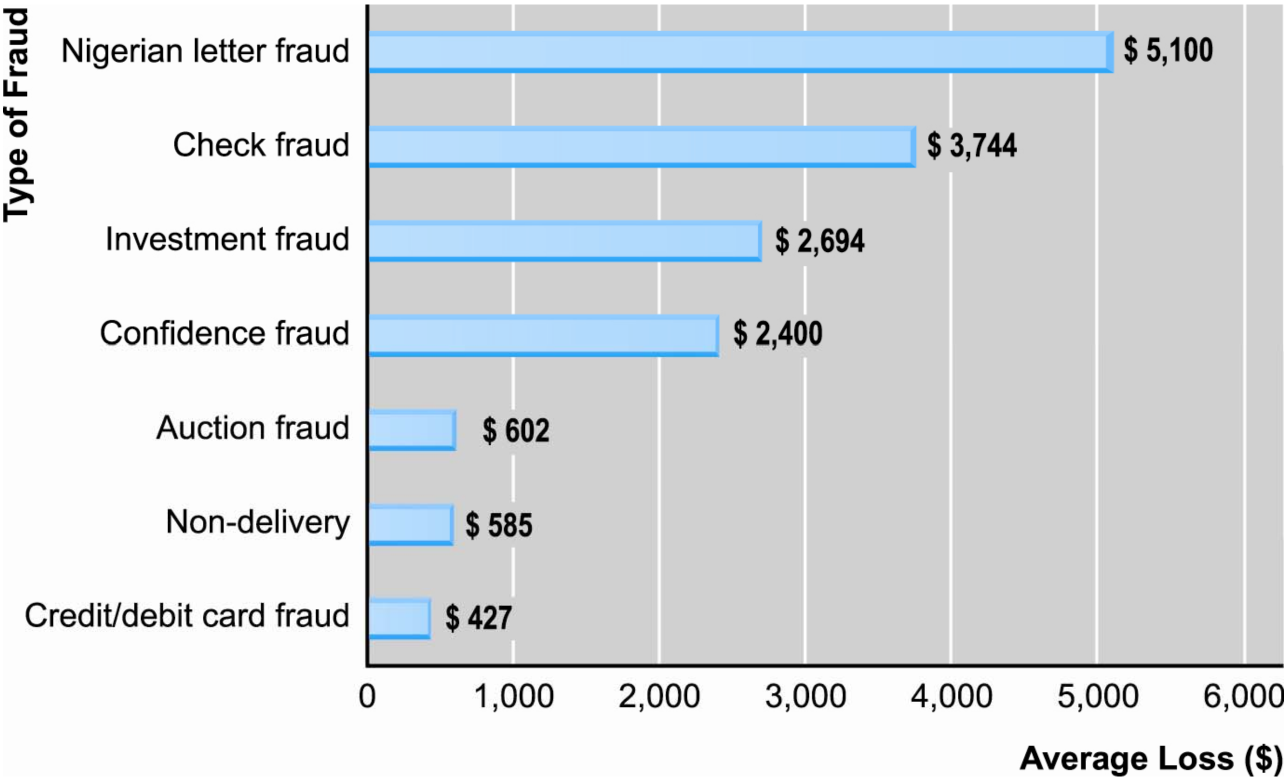
The E-commerce Security Environment: The Scope of the Problem

- Overall size of cybercrime unclear; amount of losses significant but stable; individuals face new risks of fraud that may involve substantial uninsured losses
  - Symantec: Cybercrime on the rise from 2006
  - IC3: Processed 200,000+ Internet crime complaints
  - 2007 CSI survey: 46% detected security breach; 91% suffered financial loss as a result
  - Underground economy marketplace that offers sales of stolen information growing

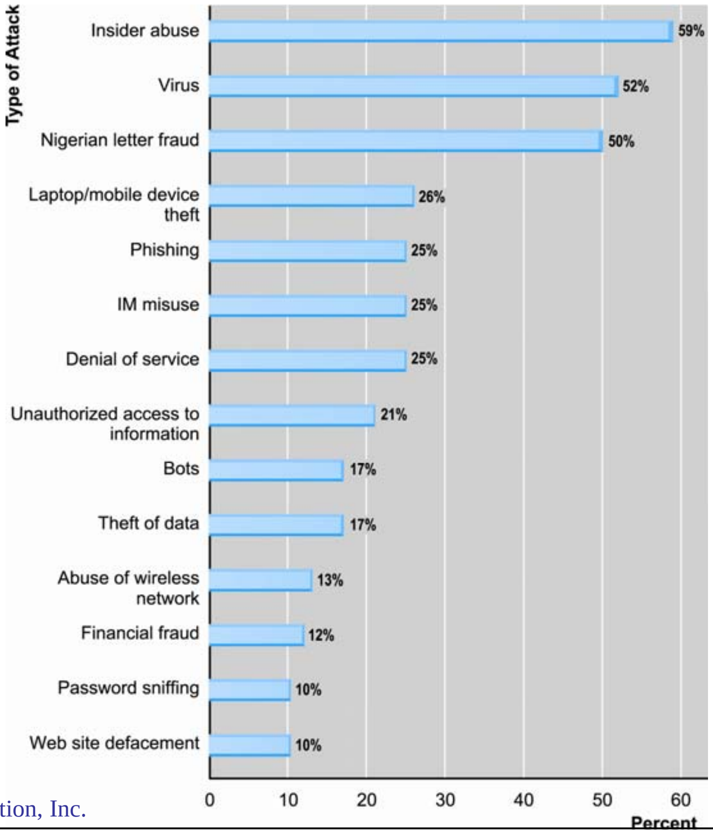
Categories of Internet Crime Complaints Reported to the IC3



Average Reported Losses for Various Types of Internet Complaints

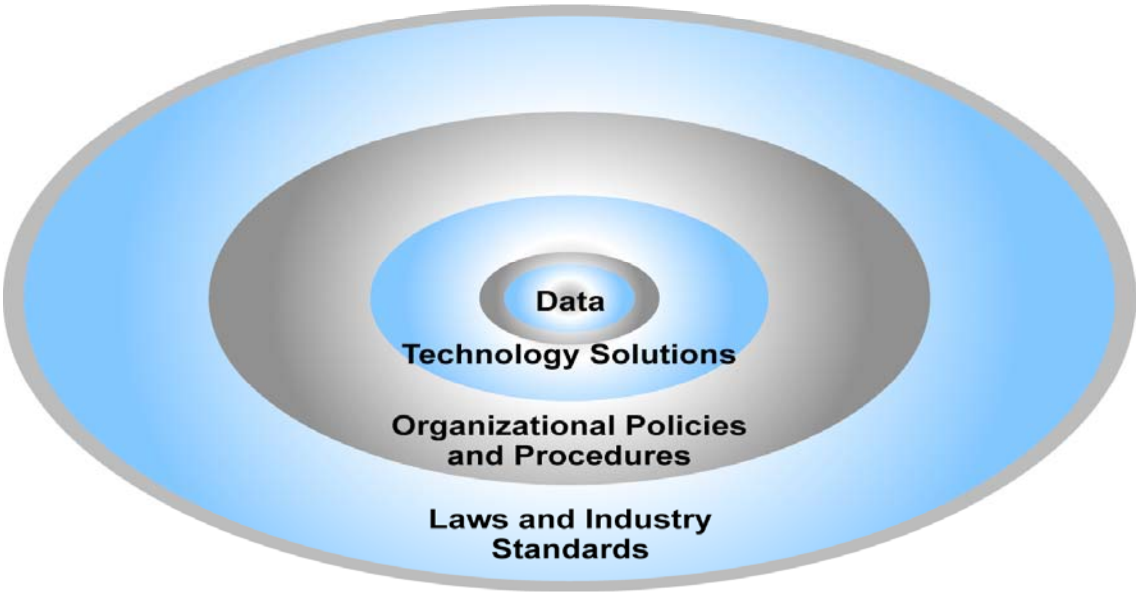


Type of Attacks against Computer Systems (Cybercrime)



The E-commerce Security Environment

Figure 5.4, Page 263



Data

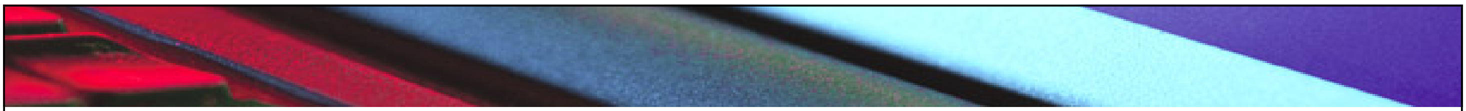
Technology Solutions

Organizational Policies and Procedures

Laws and Industry Standards

Dimensions of E-commerce Security

- Integrity: ability to ensure that information being displayed on a Web site or transmitted/received over the Internet has not been altered in any way by an unauthorized party
- Nonrepudiation: ability to ensure that e-commerce participants do not deny (repudiate) online actions
- Authenticity: ability to identify the identity of a person or entity with whom you are dealing on the Internet
- Confidentiality: ability to ensure that messages and data are available only to those authorized to view them
- Privacy: ability to control use of information a customer provides about himself or herself to merchant
- Availability: ability to ensure that an e-commerce site continues to function as intended



Customer and Merchant Perspectives on the Different Dimensions of E-commerce Security

Table 5.1, Page 264

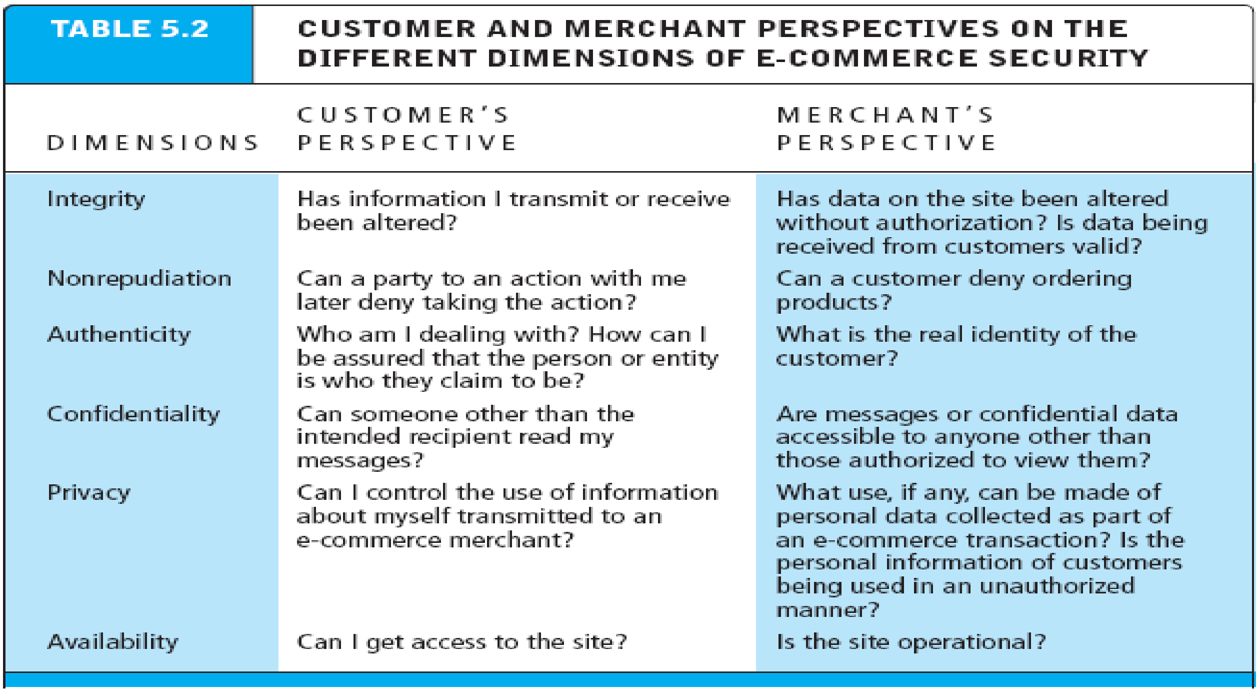
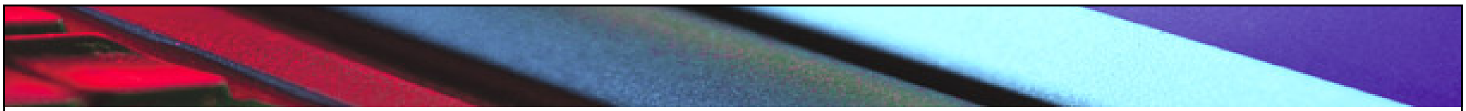


TABLE 5.2 CUSTOMER AND MERCHANT PERSPECTIVES ON THE DIFFERENT DIMENSIONS OF E-COMMERCE SECURITY

DIMENSIONS	CUSTOMER'S PERSPECTIVE	MERCHANT'S PERSPECTIVE
Integrity	Has information I transmit or receive been altered?	Has data on the site been altered without authorization? Is data being received from customers valid?
Nonrepudiation	Can a party to an action with me later deny taking the action?	Can a customer deny ordering products?
Authenticity	Who am I dealing with? How can I be assured that the person or entity is who they claim to be?	What is the real identity of the customer?
Confidentiality	Can someone other than the intended recipient read my messages?	Are messages or confidential data accessible to anyone other than those authorized to view them?
Privacy	Can I control the use of information about myself transmitted to an e-commerce merchant?	What use, if any, can be made of personal data collected as part of an e-commerce transaction? Is the personal information of customers being used in an unauthorized manner?
Availability	Can I get access to the site?	Is the site operational?



The Tension Between Security and Other Values

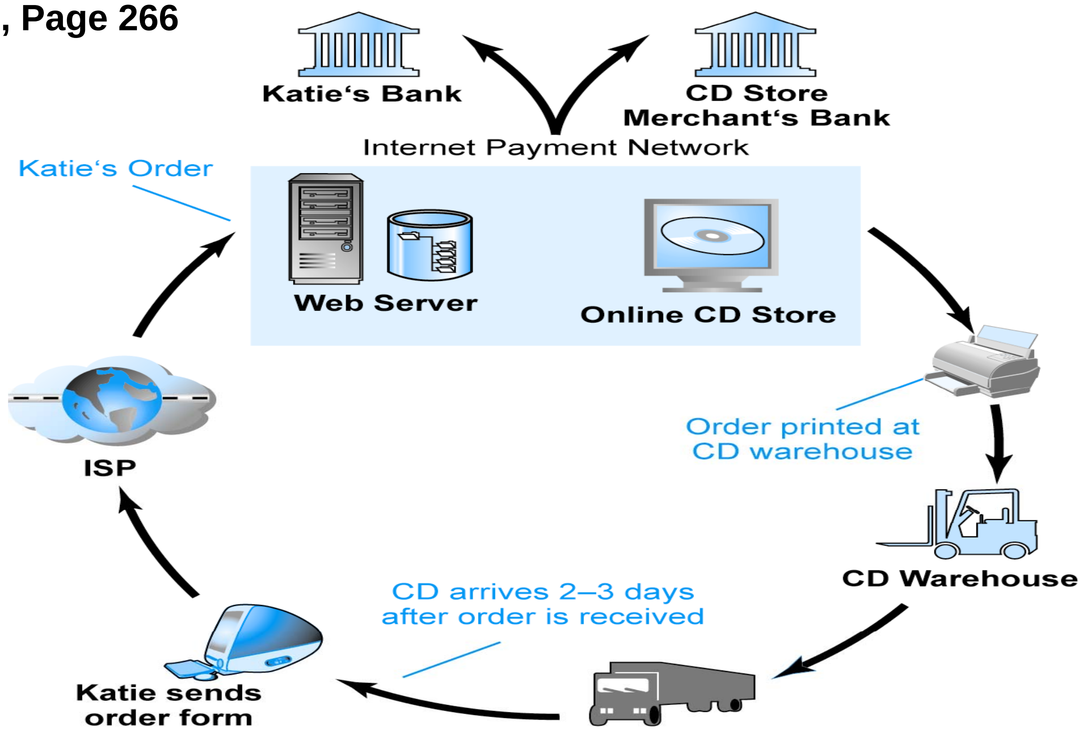
- Security vs. ease of use: the more security measures added, the more difficult a site is to use, and the slower it becomes
- Too much security can harm profitability, while not enough security can put you out of business
- Tension between the desire of individuals to act anonymously (to hide their identity) and the needs to maintain public safety that can be threatened by criminals or terrorists.
- The Internet is both anonymous and pervasive, an ideal communication tool for criminal and terrorist groups (Coll and Glasser, 2005).

Security Threats in the E-commerce Environment

- Three key points of vulnerability:
  - Client
  - Server
  - Communications channel

A Typical E-commerce Transaction

Figure 5.5, Page 266



Katie's Bank

CD Store Merchant's Bank

Internet Payment Network

Katie's Order

Web Server

Online CD Store

Order printed at CD warehouse

CD Warehouse

CD arrives 2–3 days after order is received

Katie sends order form

ISP

SOURCE: Boncella, 2000.

Vulnerable Points in an E-commerce Environment

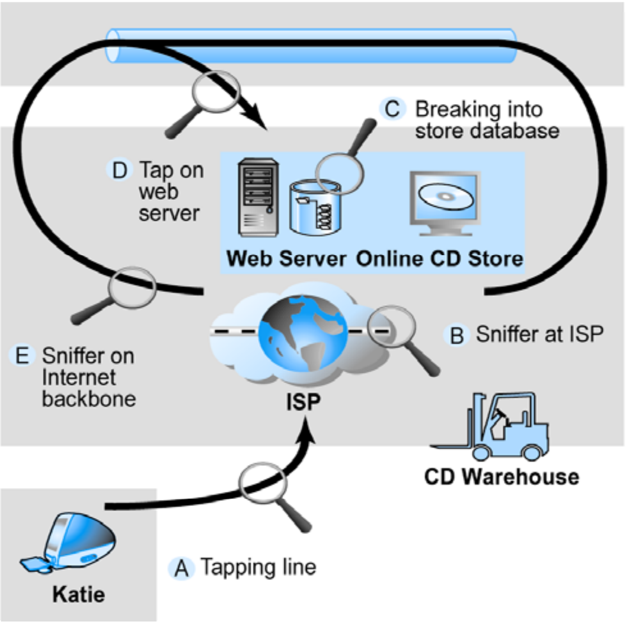
Figure 5.6, Page 267

Security Risks

Internet communications

Servers
- ISP
- Merchant
- Banks

Clients
- Business
- Home



Tapping and sniffing
Alteration of messages
Theft and fraud

DoS attack
Hacking
Malicious code attack
Theft and fraud
Line taps
Vandalism

Malicious code attack
Line taps
Physical loss of computer

SOURCE: Boncella, 2000.

Most Common Security Threats in the E-commerce Environment

- Malicious code (viruses, worms, Trojans)
- Unwanted programs (spyware, browser parasites)
- Phishing/identity theft
- Hacking and cybervandalism
- Credit card fraud/theft
- Spoofing (pharming)/spam (junk) Web sites
- DoS and dDoS attacks
- Sniffing
- Insider attacks
- Poorly designed server and client software

Malicious Code

- Try to impair computers, steal email addresses, logon credentials, personal data, and financial info.
- Viruses: computer programs that have ability to replicate and spread to other files; most also deliver a “payload” of some sort (destructive or benign); include macro viruses, file-infecting viruses, and script viruses
- Worms: Designed to spread from computer to computer; can replicate without being executed by a user or program like virus
- Trojan horse: Appears to be benign, but then does something other than expected
- Bots: Can be covertly installed on computer; responds to external commands sent by the attacker to create a network of compromised computers for sending spam, generating a DDoS attack, and stealing info from computers
- See Table 5.3 for notable examples of malicious code

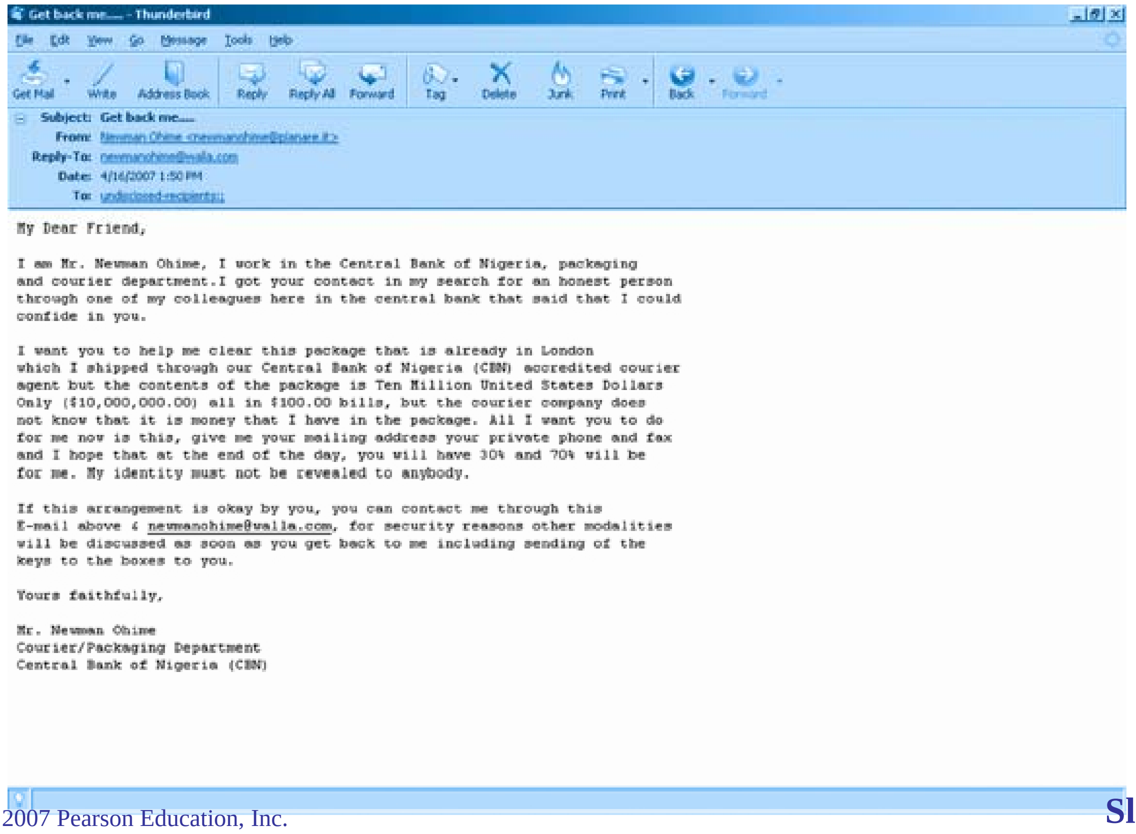
Unwanted Programs

- Installed without the user’s informed consent
  - Browser parasites: Can monitor and change settings of a user’s browser
  - Adware: Calls for unwanted pop-up ads
  - Spyware: Can be used to obtain information, such as a user’s keystrokes, e-mail, IMs, etc.

Phishing and Identity Theft

- Any deceptive, online attempt by a third party to obtain confidential information for financial gain
  - Most popular type: e-mail scam letter, e.g., Nigerian's rich former oil minister seeking a bank account to deposit millions of dollars, fake "account verification" emails from eBay or CitiBank asking to give up personal account info, bank account no., and credit card no.
  - One of fastest growing forms of e-commerce crime
    - 197,000 unique new phishing emails sent within the first 6 months of 2007, 18% increase compared to 2nd half of 2006.

An Example of a Nigerian Letter E-Mail Scam



Subject: Get back me....
From: Newman Ohime <newmanohime@planare.it>
Reply-To: newmanohime@walla.com
Date: 4/16/2007 1:50 PM
To: undisclosed-recipients:;

My Dear Friend,

I am Mr. Newman Ohime, I work in the Central Bank of Nigeria, packaging and courier department.I got your contact in my search for an honest person through one of my colleagues here in the central bank that said that I could confide in you.

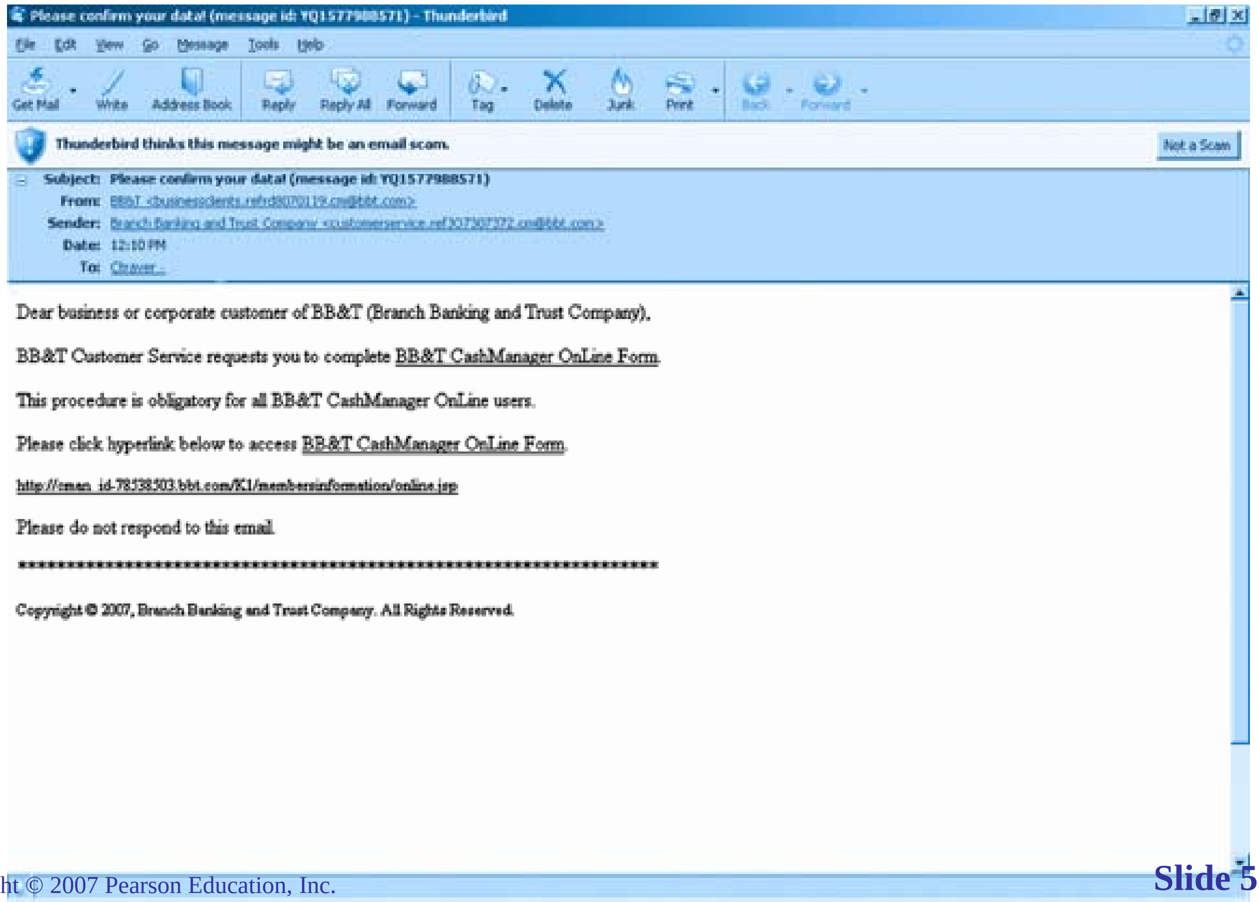
I want you to help me clear this package that is already in London which I shipped through our Central Bank of Nigeria (CBN) accredited courier agent but the contents of the package is Ten Million United States Dollars Only ($10,000,000.00) all in $100.00 bills, but the courier company does not know that it is money that I have in the package. All I want you to do for me now is this, give me your mailing address your private phone and fax and I hope that at the end of the day, you will have 30% and 70% will be for me. My identity must not be revealed to anybody.

If this arrangement is okay by you, you can contact me through this E-mail above & newmanohime@walla.com, for security reasons other modalities will be discussed as soon as you get back to me including sending of the keys to the boxes to you.

Yours faithfully,

Mr. Newman Ohime
Courier/Packaging Department
Central Bank of Nigeria (CBN)

An Example of a Phishing Attack


Please confirm your data! (message id: YQ1577988571) - Thunderbird
File Edit View Go Message Tools Help
Get Mail
Write
Address Book
Reply
Reply All
Forward
Tag
Delete
Junk
Print
Back
Forward
Not a Scam

Thunderbird thinks this message might be an email scam.

Subject: Please confirm your data! (message id: YQ1577988571)
From: BB&T <businessclients.refrd8070119.cm@bbt.com>
Sender: Branch Banking and Trust Company <customerservice.ref307307372.cm@bbt.com>
Date: 12:10 PM
To: Clraver...

Dear business or corporate customer of BB&T (Branch Banking and Trust Company),

BB&T Customer Service requests you to complete BB&T CashManager OnLine Form.

This procedure is obligatory for all BB&T CashManager OnLine users.

Please click hyperlink below to access BB&T CashManager OnLine Form.

http://cman_id-78538503.bbt.com/K1/membersinformation/online.jsp

Please do not respond to this email.

****

Copyright © 2007, Branch Banking and Trust Company. All Rights Reserved.

Hacking and Cybervandalism

- Hacker: Individual who intends to gain unauthorized access to computer systems
- Cracker: Hacker with criminal intent (two terms often used interchangeably)
- Cybervandalism: Intentionally disrupting, defacing or destroying a Web site
- Types of hackers include:
  - White hats– hired by corporate to find weaknesses in the firm’s computer system
  - Black hats – hackers with intention of causing harm
  - Grey hats – hackers breaking in and revealing system flaws without disrupting site or attempting to profit from their finds.

Credit Card Fraud

- Fear that credit card information will be stolen deters online purchases
- Overall rate of credit card fraud is lower than users think, 1.6-1.8% of all online card transactions (CyberSource Corporation, 2007).
- US’s federal law limits liability of individuals to $50 for a stolen credit card.
- Hackers target credit card files and other customer information files on merchant servers; use stolen data to establish credit under false identity
- One solution: New identity verification mechanisms

Spoofing (Pharming) and Spam (Junk) Web Sites

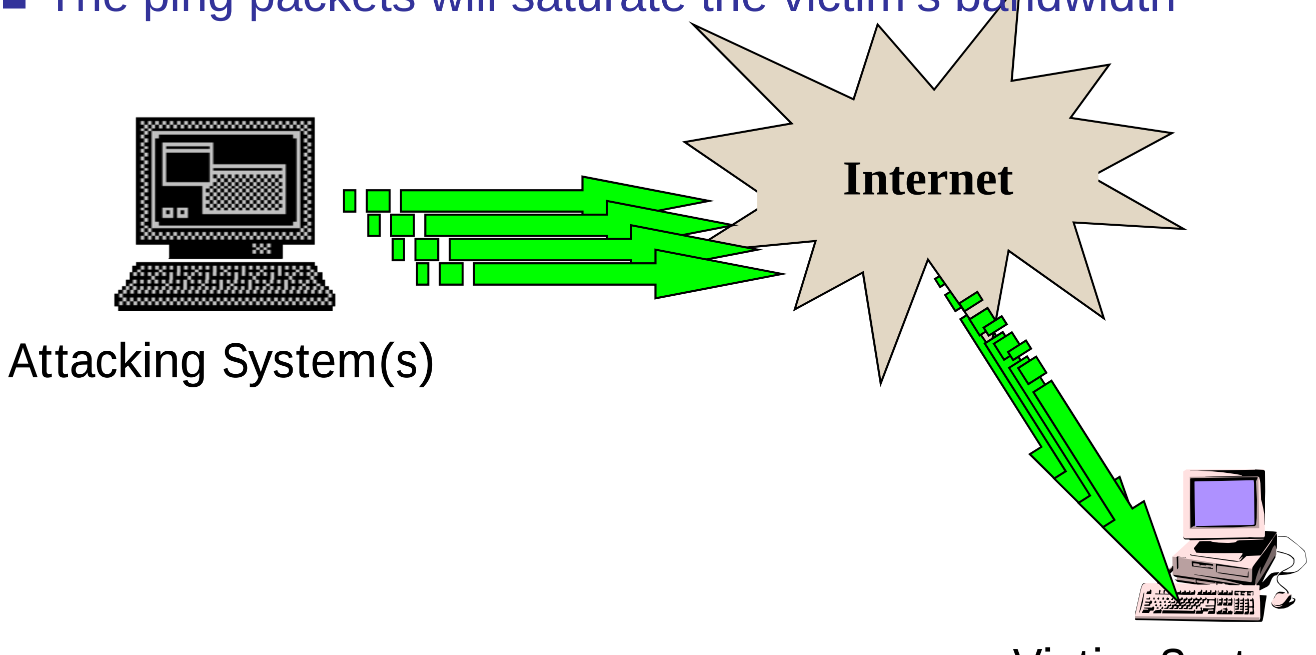
- Spoofing (Pharming)
  - Misrepresenting oneself by using fake e-mail addresses or masquerading as someone else
  - Threatens integrity of site; authenticity
- Spoofing a Web site is called “pharming,” which involves redirecting a Web link to another IP address different from the real one
- Pharming is carried out by hacking local DNS servers.
- Threatens integrity of site by stealing business from the true site, or altering orders and sending them to the true site for processing and delivery.
- Threatens authenticity by making it hard to discern the true sender of a message.
- Spam (Junk) Web sites
  - Use domain names similar to legitimate one, redirect traffic to spammer-redirection domains

DoS and DDoS Attacks

- Denial of service (DoS) attack
  - Hackers flood Web site with useless traffic to inundate and overwhelm network
- Use of bot networks built from hundreds of compromised workstations.
- No. of DoS attacks per day grew from 119 during last 6 months of 2004 to 927 during first 6 months of 2005, a 679% increase (Symantec 2005).
- Distributed denial of service (DDoS) attack
  - Hackers use numerous computers to attack target network from numerous launch points
  - Microsoft and Yahoo have experienced such attacks

Denial of Service

- Ping Flooding
  - Attacker sends a flood of pings to the intended victim
  - The ping packets will saturate the victim's bandwidth

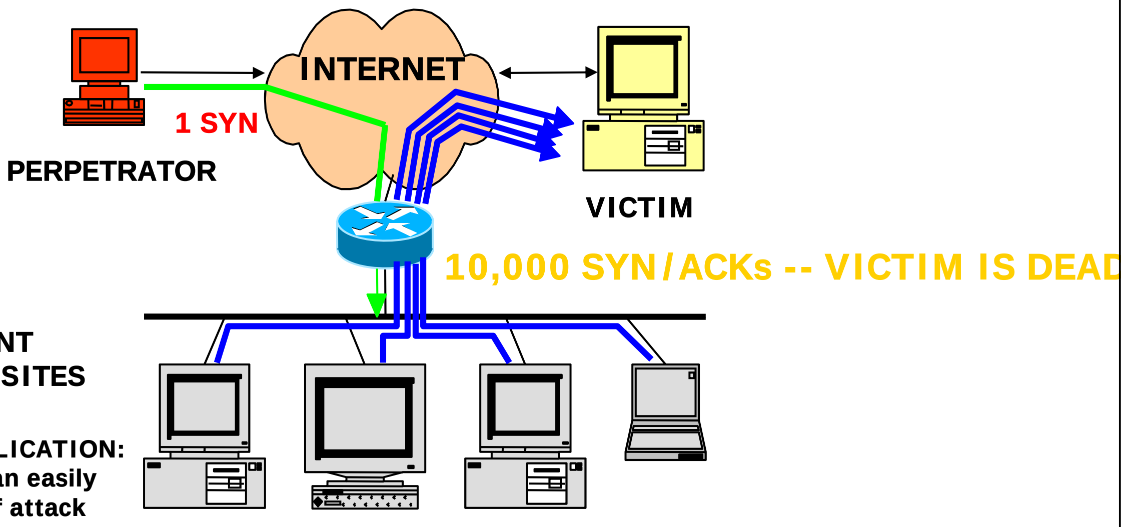


SOURCE: PETER SHIPLEY

Denial of Service

- SMURF ATTACK
  - Uses a ping packet with two extra twist
  - Attacker chooses an unwitting victim
  - Spoofs the source address
  - Sends request to network in broadcast mode

ICMP = Internet Control Message Protocol



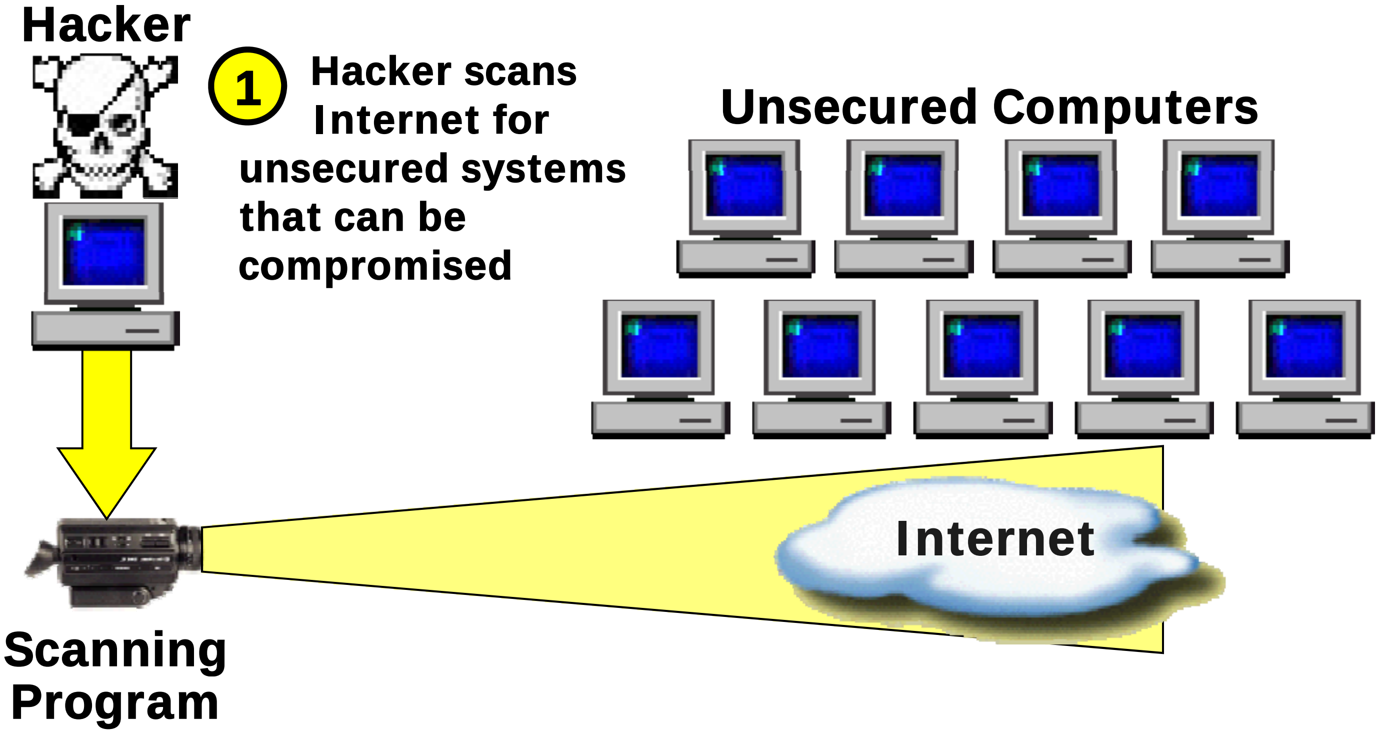
BANDWIDTH MULTIPLICATION:
A T1 (1.54 Mbps) can easily
yield 100 MBbps of attack

🟩 ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

🟦 ICMP echo reply

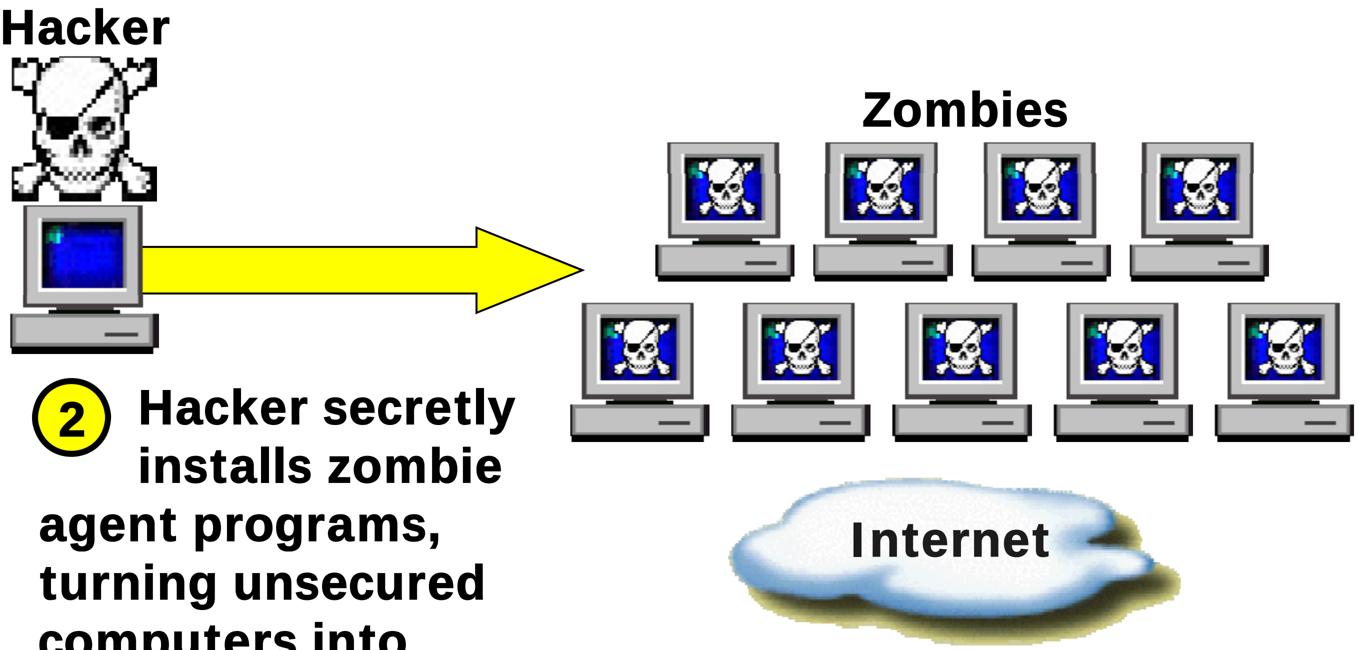
SOURCE: CISCO

DDoS Attack Illustrated



1 Hacker scans Internet for unsecured systems that can be compromised

DDoS Attack Illustrated



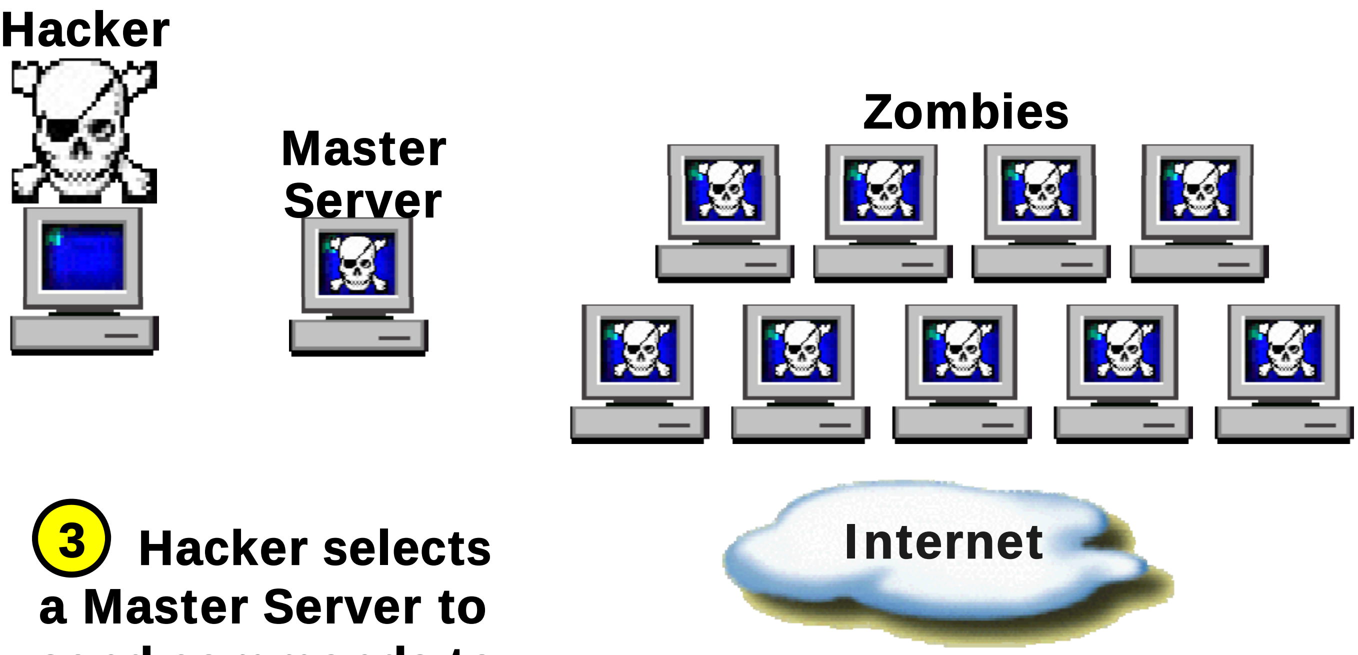
Hacker

Zombies

Internet

2 Hacker secretly installs zombie agent programs, turning unsecured computers into zombies

DDoS Attack Illustrated



Hacker

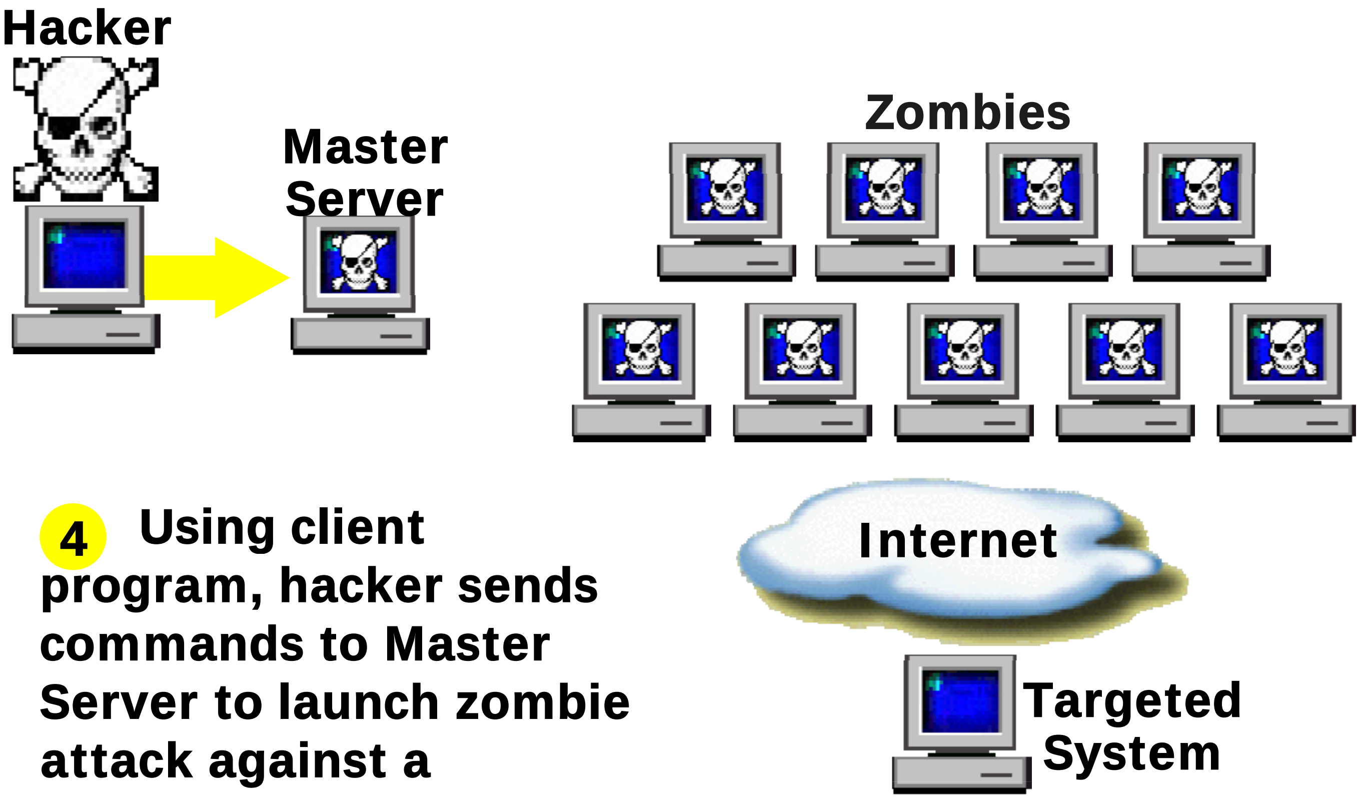
Master Server

Zombies

Internet

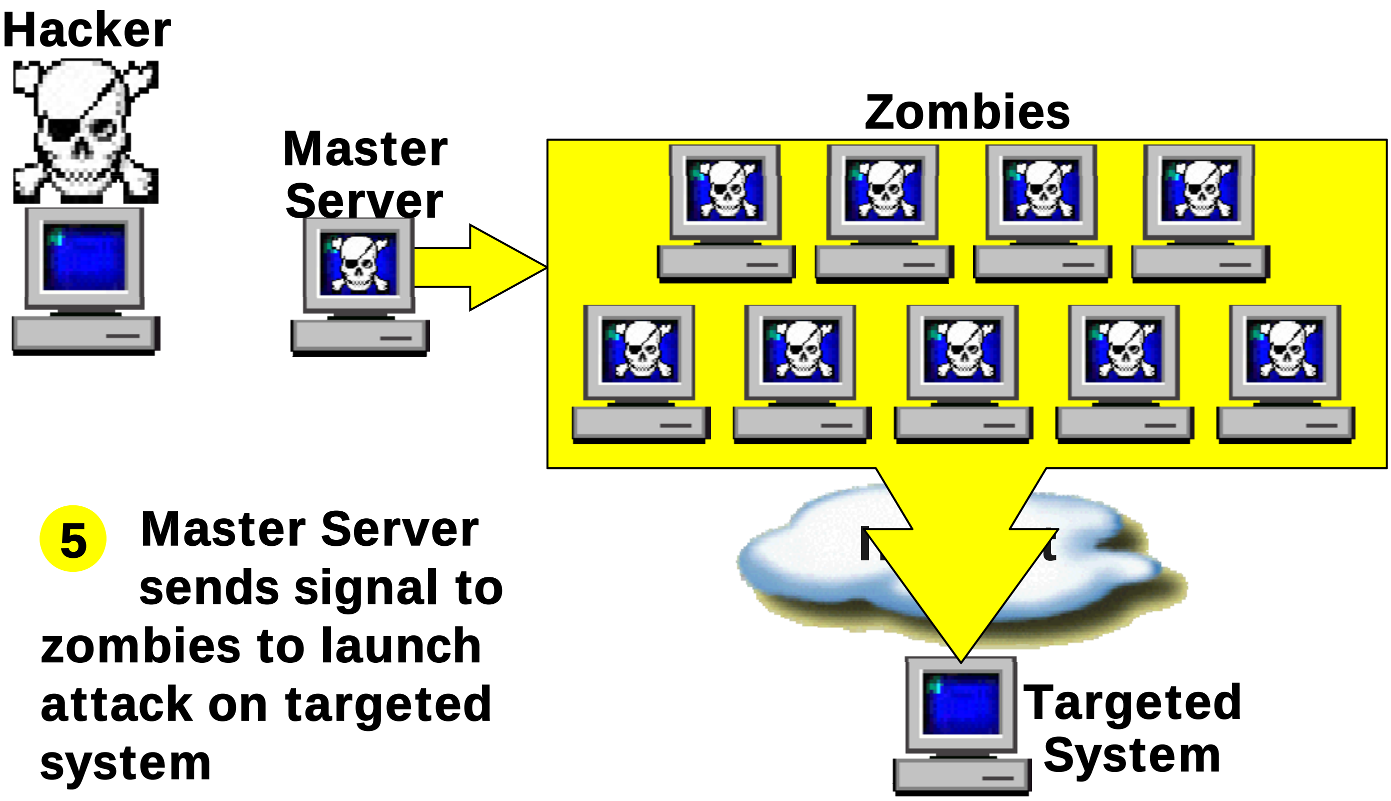
3 Hacker selects a Master Server to send commands to the zombies

DDoS Attack Illustrated



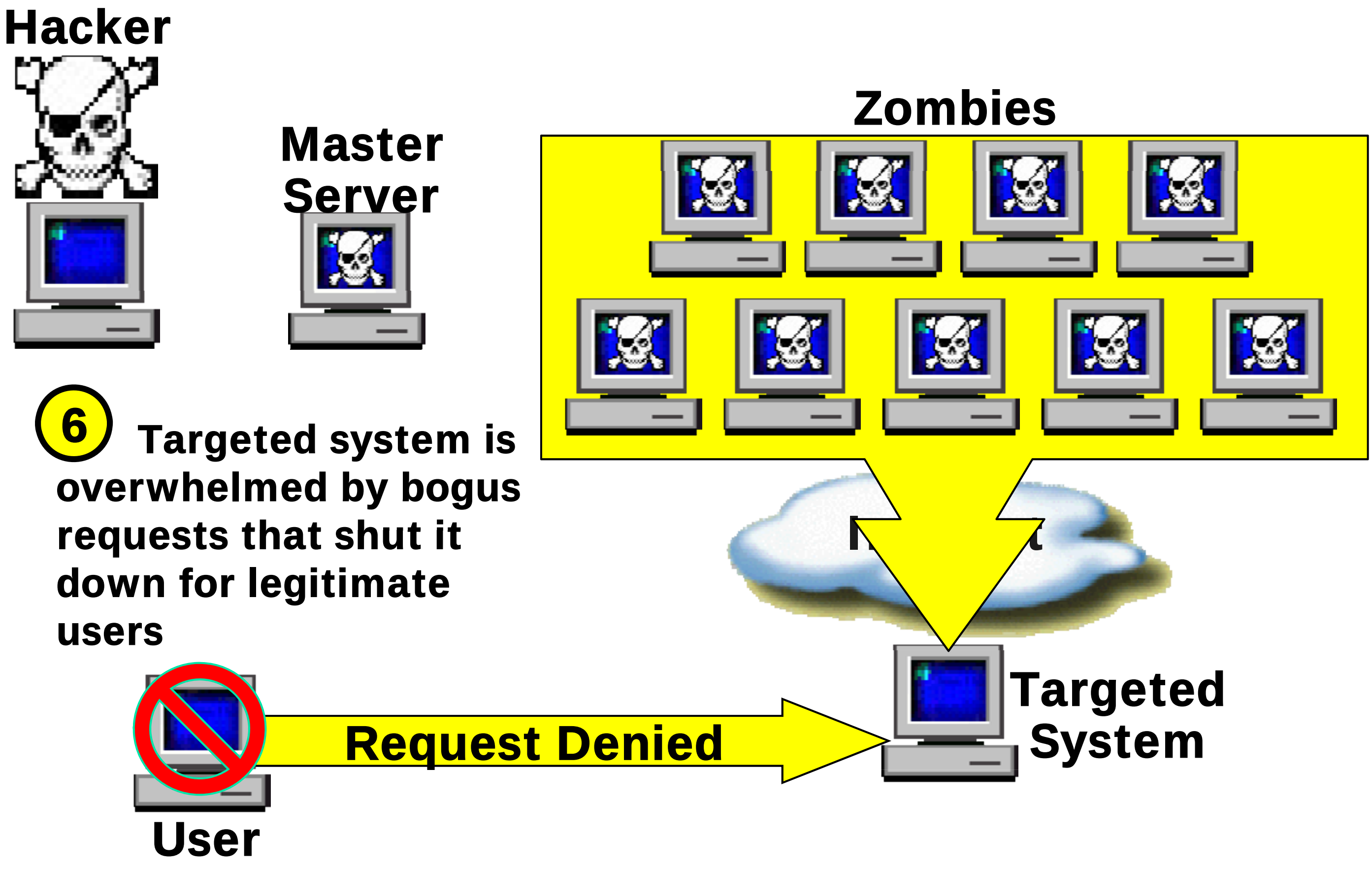
4 Using client program, hacker sends commands to Master Server to launch zombie attack against a targeted system

DDoS Attack Illustrated



5 Master Server sends signal to zombies to launch attack on targeted system

DDoS Attack Illustrated



6 Targeted system is overwhelmed by bogus requests that shut it down for legitimate users

Other Security Threats

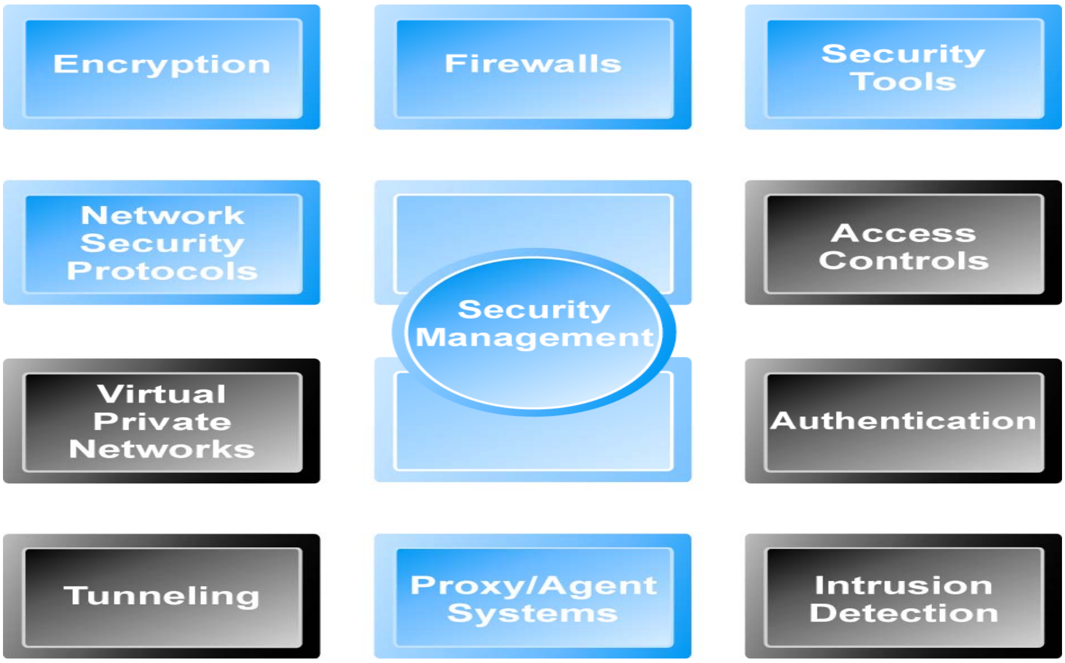
- Sniffing: Type of eavesdropping program that monitors information traveling over a network; enables hackers to steal proprietary information from anywhere on a network
- Insider jobs: Single largest financial threat
  - 64% of business firms experienced an “inside security breach” in their systems in 2006 (Computer Security Institute, 2007).
- Poorly designed server and client software: Increase in complexity of software programs (e.g., MS’s Win32 API) has contributed to increase is vulnerabilities that hackers can exploit

Technology Solutions

- Protecting Internet communications (encryption)
- Securing channels of communication (SSL, S-HTTP, VPNs)
- Protecting networks (firewalls)
- Protecting servers and clients

Tools Available to Achieve Site Security

Figure 5.9, Page 279



Encryption

Firewalls

Security Tools

Network Security Protocols

Security Management

Access Controls

Virtual Private Networks

Authentication

Tunneling

Proxy/Agent Systems

Intrusion Detection

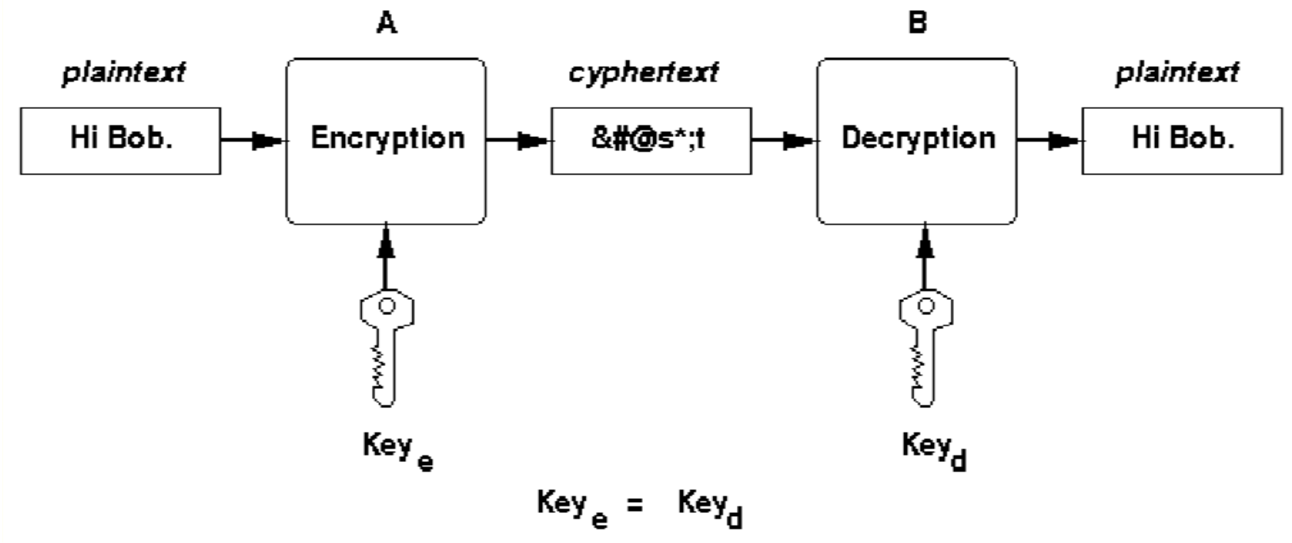
Protecting Internet Communications: Encryption

- Encryption: Process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and receiver
- Purpose: Secure stored information and information transmission
- Provides:
  - Message integrity
  - Nonrepudiation
  - Authentication
  - Confidentiality

Symmetric Key Encryption

- Also known as secret key encryption
- Both the sender and receiver use the same digital key to encrypt and decrypt message
- Requires a different set of keys for each transaction
- Advanced Encryption Standard (AES): Most widely used symmetric key encryption today; offers 128-, 192-, and 256-bit encryption keys; other standards use keys with up to 2,048 bits

Symmetric Encryption and Decryption



A

B

plaintext

Hi Bob.

Encryption

cyphertext

&#@s*;t

Decryption

plaintext

Hi Bob.

Key_e

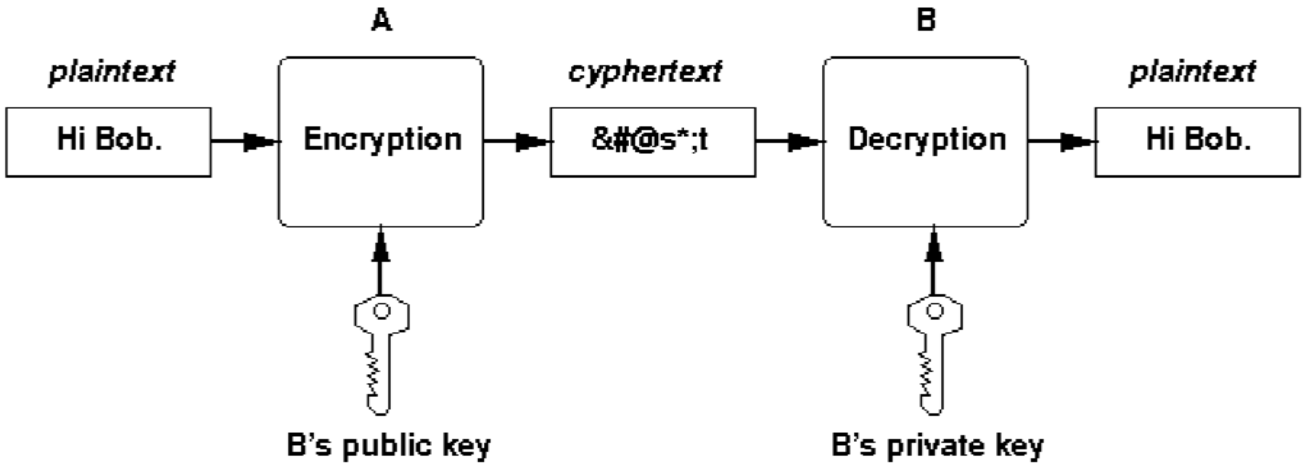
Key_d

$\text{Key}_e = \text{Key}_d$

Public Key Encryption

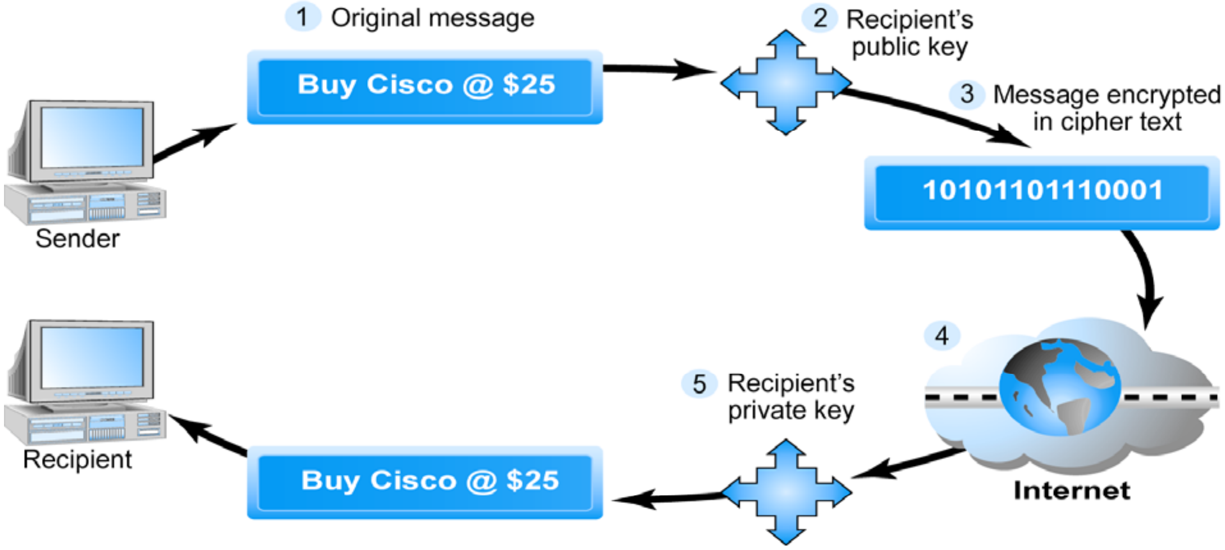
- Solves symmetric key encryption problem of having to exchange secret key
- Uses two mathematically related digital keys – public key (widely disseminated) and private key (kept secret by owner)
- Both keys used to encrypt and decrypt message
- Once key used to encrypt message, same key cannot be used to decrypt message
- For example, sender uses recipient’s public key to encrypt message; recipient uses his/her private key to decrypt it

Public Key Encryption and Decryption



Public Key Cryptography – A Simple Case

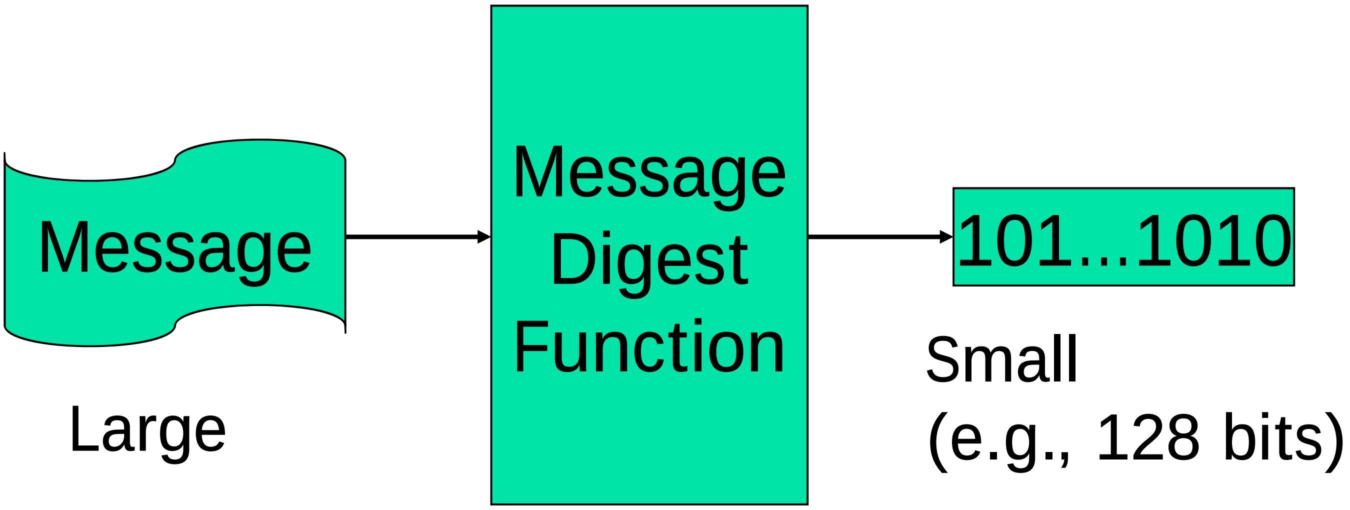
Figure 5.10, Page 283



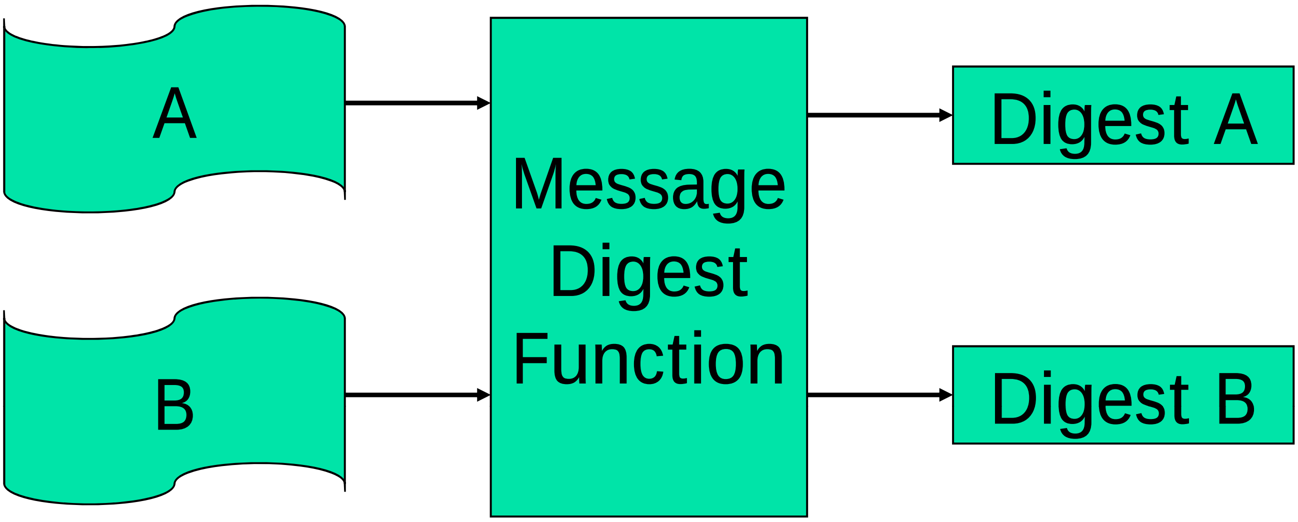
Public Key Encryption using Digital Signatures and Hash Digests

- Public key encryption provides confidentiality, but not authentication, integrity, and nonrepudiation
- Application of hash function (mathematical algorithm) by sender prior to encryption produces hash (message) digest that recipient can use to verify integrity of data
- Hash function produces a fixed-length number called hash or message digest.
- Examples of hash function include MD4 and MD5.
- Double encryption with sender’s private key (digital signature) helps ensure authenticity and nonrepudiation

Message Digest

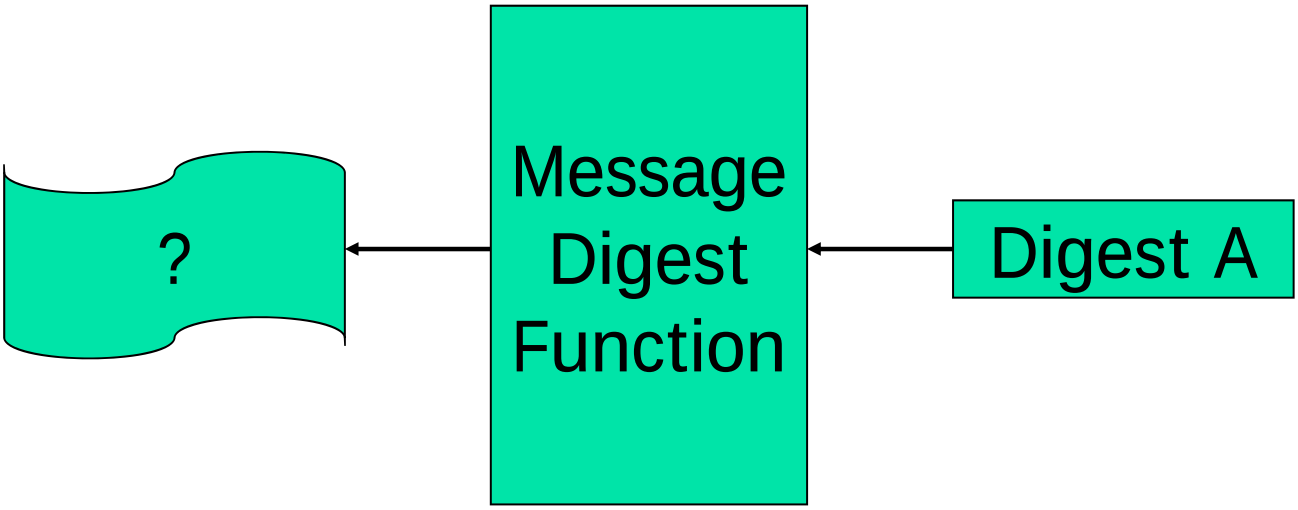


Message Digest



If A ≠B => Digest A ≠ Digest B

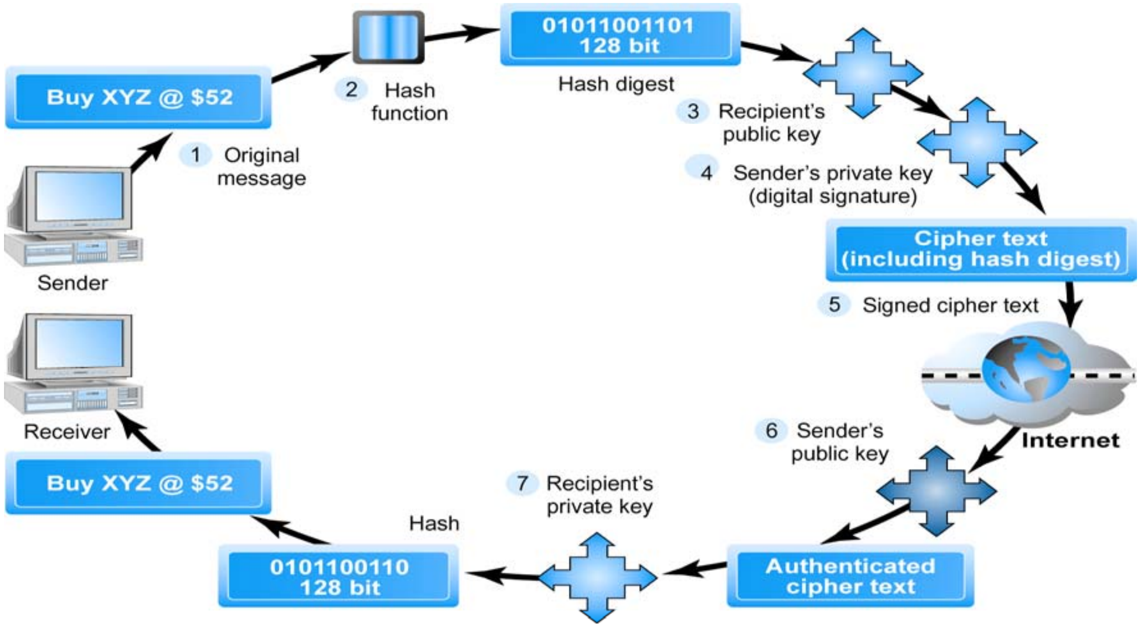
Message Digest



Extremely hard to get A from Digest A!

Public Key Cryptography with Digital Signatures

Figure 5.11, Page 284

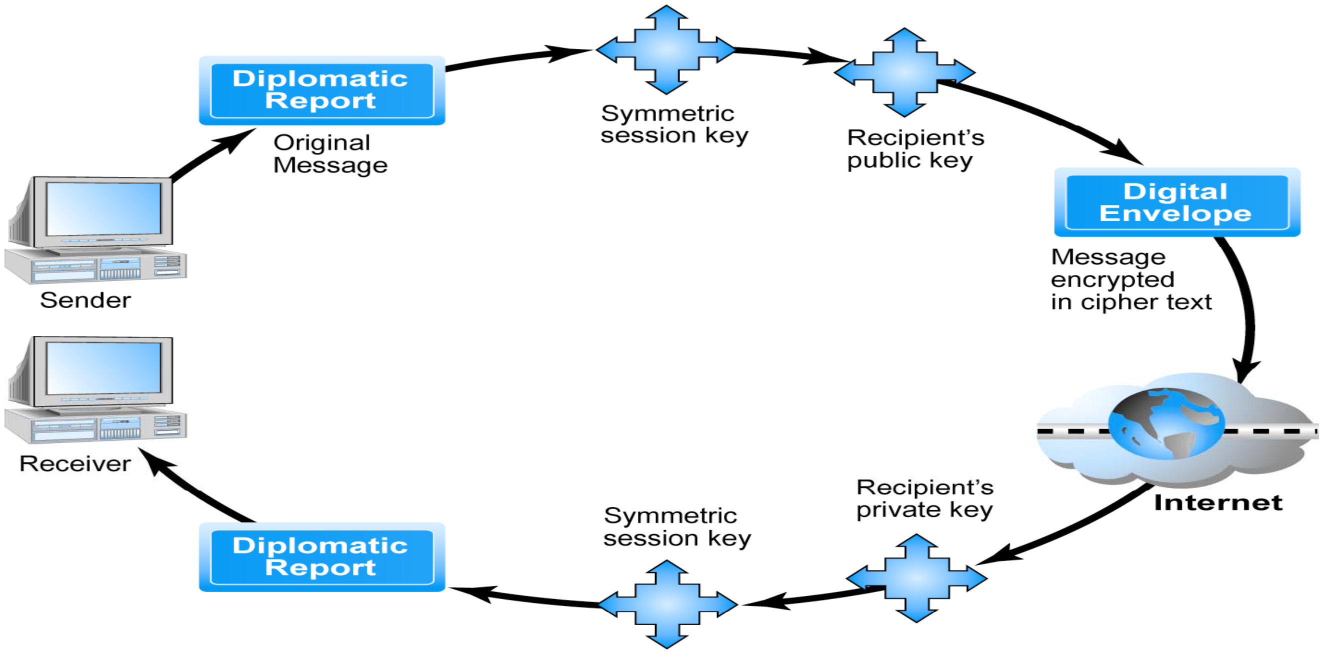


Digital Envelopes

- Addresses weaknesses of public key encryption (computationally slow, decreases transmission speed, increases processing time) and symmetric key encryption (faster, but more secure)
- Uses symmetric key encryption to encrypt document but public key encryption to encrypt and send symmetric key

Public Key Cryptography: Creating a Digital Envelope

Figure 5.12, Page 286



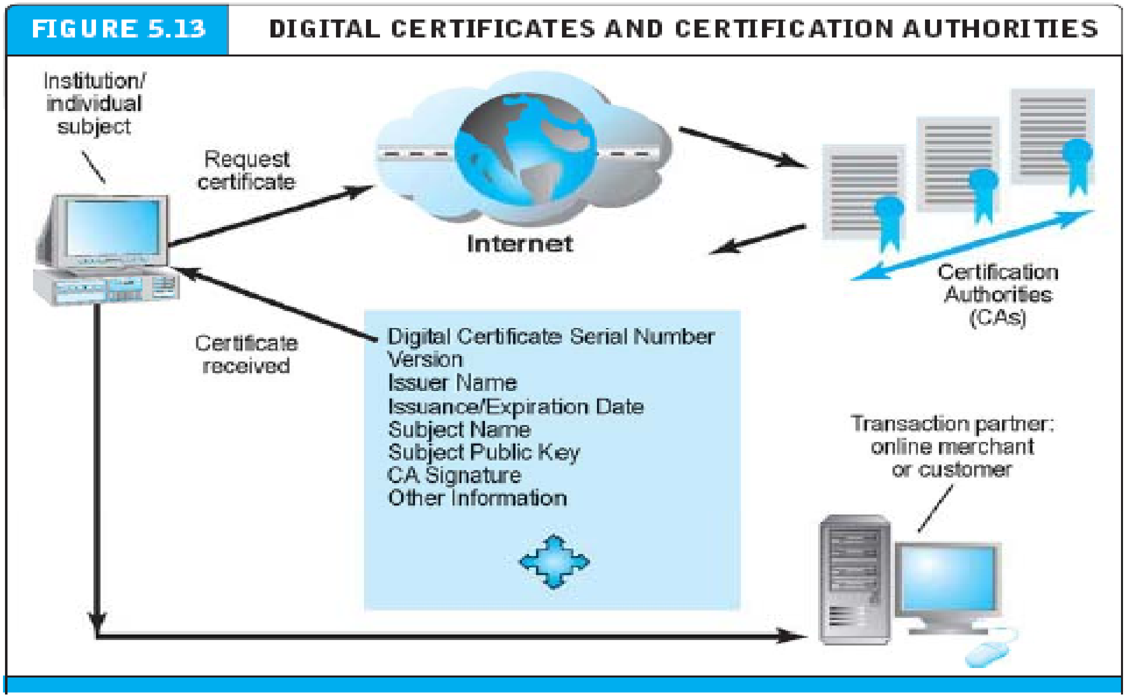
Digital Certificates and Public Key Infrastructure (PKI)

- Still missing a way to verify identity of Web sites.
- By using digital document issued by a trusted third party called certificate authority (CA)
- Digital certificate includes:
  - Name of subject/company
  - Subject's public key
  - Digital certificate serial number
  - Expiration date
  - Issuance date
  - Digital signature of certification authority (trusted third party institution) that issues certificate
  - Other identifying information
- Public Key Infrastructure (PKI): refers to the CAs and digital certificate procedures that are accepted by all parties

Digital Certificates and Certification Authorities

Figure 5.13, Page 287

FIGURE 5.13 DIGITAL CERTIFICATES AND CERTIFICATION AUTHORITIES



Digital Certificate Serial Number
Version
Issuer Name
Issuance/Expiration Date
Subject Name
Subject Public Key
CA Signature
Other Information

Limits to Encryption Solutions

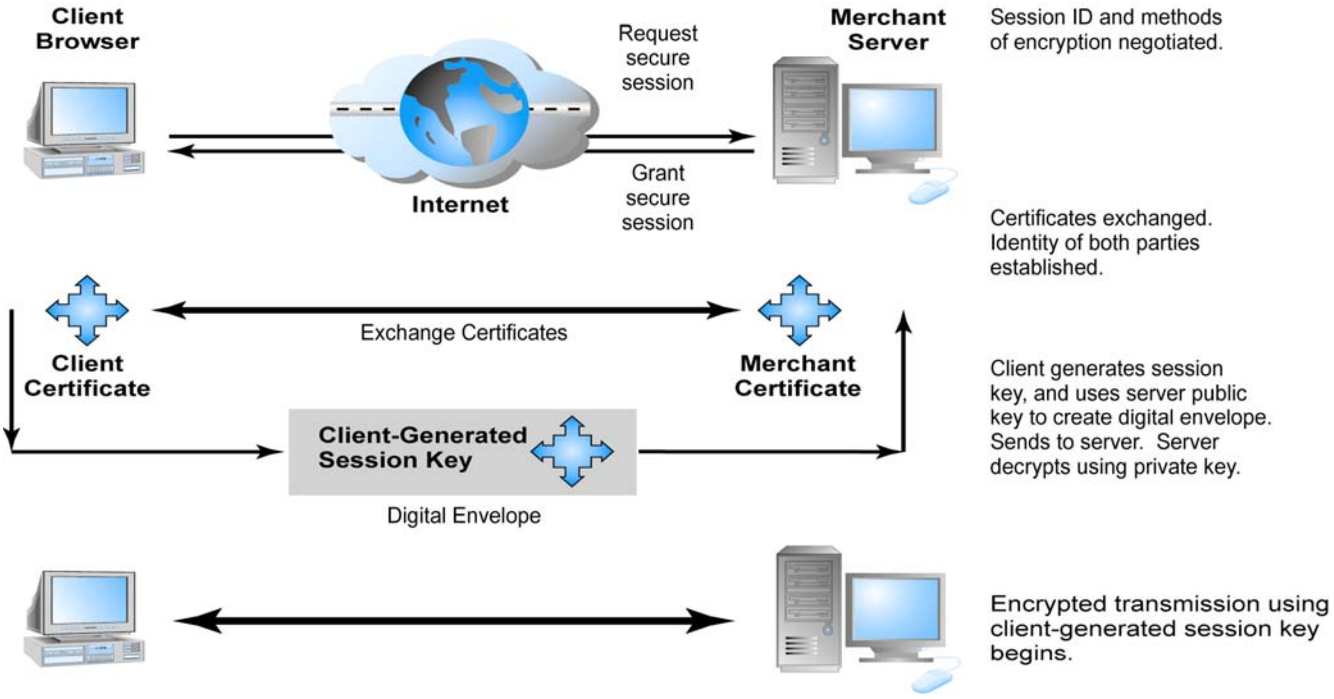
- PKI applies mainly to protecting messages in transit
- PKI is not effective against insiders
- Protection of private keys by individuals may be haphazard
- No guarantee that verifying computer of merchant is secure
- CAs are unregulated, self-selecting organizations

Securing Channels of Communication

- Secure Sockets Layer (SSL): Most common form of securing channels of communication; used to establish a secure negotiated session (client-server session in which URL of requested document, along with contents, is encrypted)
- S-HTTP: Alternative method; provides a secure message-oriented communications protocol designed for use in conjunction with HTTP
- SSL is designed to establish a secure connection between two computers, S-HTTP is designed to send individual messages securely
- Virtual Private Networks (VPNs): Allow remote users to securely access internal networks via the Internet, using Point-to-Point Tunneling Protocol (PPTP)

Secure Negotiated Sessions Using SSL

Figure 5.14, Page 291



Session ID and methods of encryption negotiated.

Certificates exchanged. Identity of both parties established.

Client generates session key, and uses server public key to create digital envelope. Sends to server. Server decrypts using private key.

Encrypted transmission using client-generated session key begins.

Protecting Networks: Firewalls and Proxy Servers

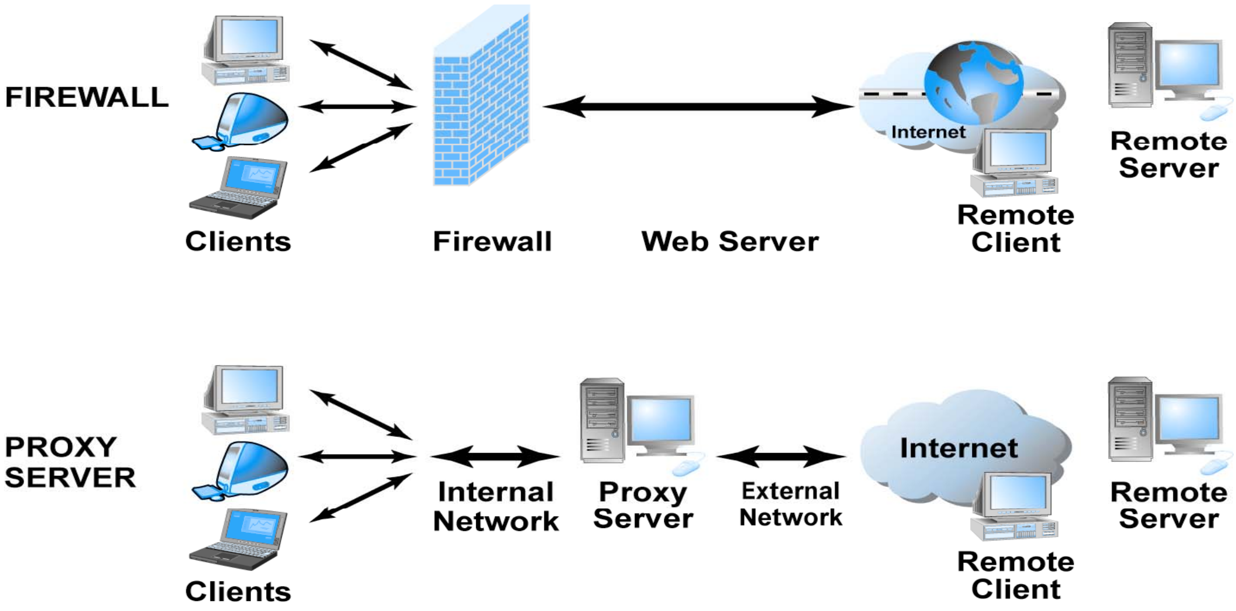
- Firewall: Hardware or software filters communications packets; prevents some packets from entering the network based on a security policy
- Firewall methods include:
  - Packet filters– looks inside data packets to decide whether they are destined for a prohibited port or originate from a prohibited IP address.
  - Application gateways – filters communications based on the application being requested, rather than the source or destination of the message.
- Application gateways provide greater security than packet filters, but can compromise system performance

Protecting Networks: Firewalls and Proxy Servers

- Proxy servers: Software servers that handle all communications originating from or being sent to the Internet
- Initially for limiting access of internal clients to external Internet servers
- Can be used to restrict access to certain types of sites, such as porno, auction, or stock-trading sites, or to cache frequently-accessed Web pages to reduce download times

Firewalls and Proxy Servers

Figure 5.15, Page 293



Protecting Servers and Clients

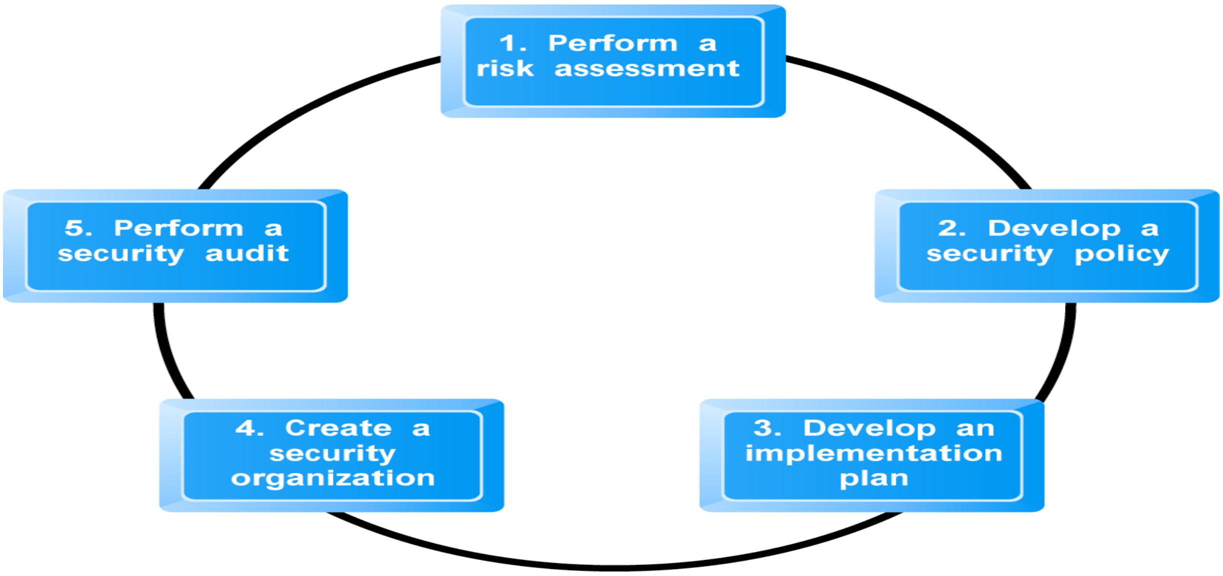
- Operating system controls: Authentication and access control mechanisms
- Anti-virus software: Easiest and least expensive way to prevent threats to system integrity

A Security Plan: Management Policies

- Steps in developing a security plan
  - Perform risk assessment: assessment of risks and points of vulnerability
  - Develop security policy: set of statements prioritizing information risks, identifying acceptable risk targets, and identifying mechanisms for achieving targets
  - Develop implementation plan: action steps needed to achieve security plan goals
  - Create security organization: in charge of security; educates and trains users, keeps management aware of security issues; administers access controls, authentication procedures and authorization policies
  - Perform security audit: review of security practices and procedures

Developing an E-commerce Security Plan

Figure 5.16, Page 295



1. Perform a risk assessment
2. Develop a security policy
3. Develop an implementation plan
4. Create a security organization
5. Perform a security audit

The Role of Laws and Public Policy

- New laws have granted local and national authorities new tools and mechanisms for identifying, tracing and prosecuting cybercriminals
  - National Infrastructure Protection Center – unit within National Cyber Security Division of Department of Homeland Security whose mission is to identify and combat threats against U.S. technology and telecommunications infrastructure
  - USA Patriot Act
  - Homeland Security Act
- Government policies and controls on encryption software