Chapter 3

Attack Types and Protection Schemes

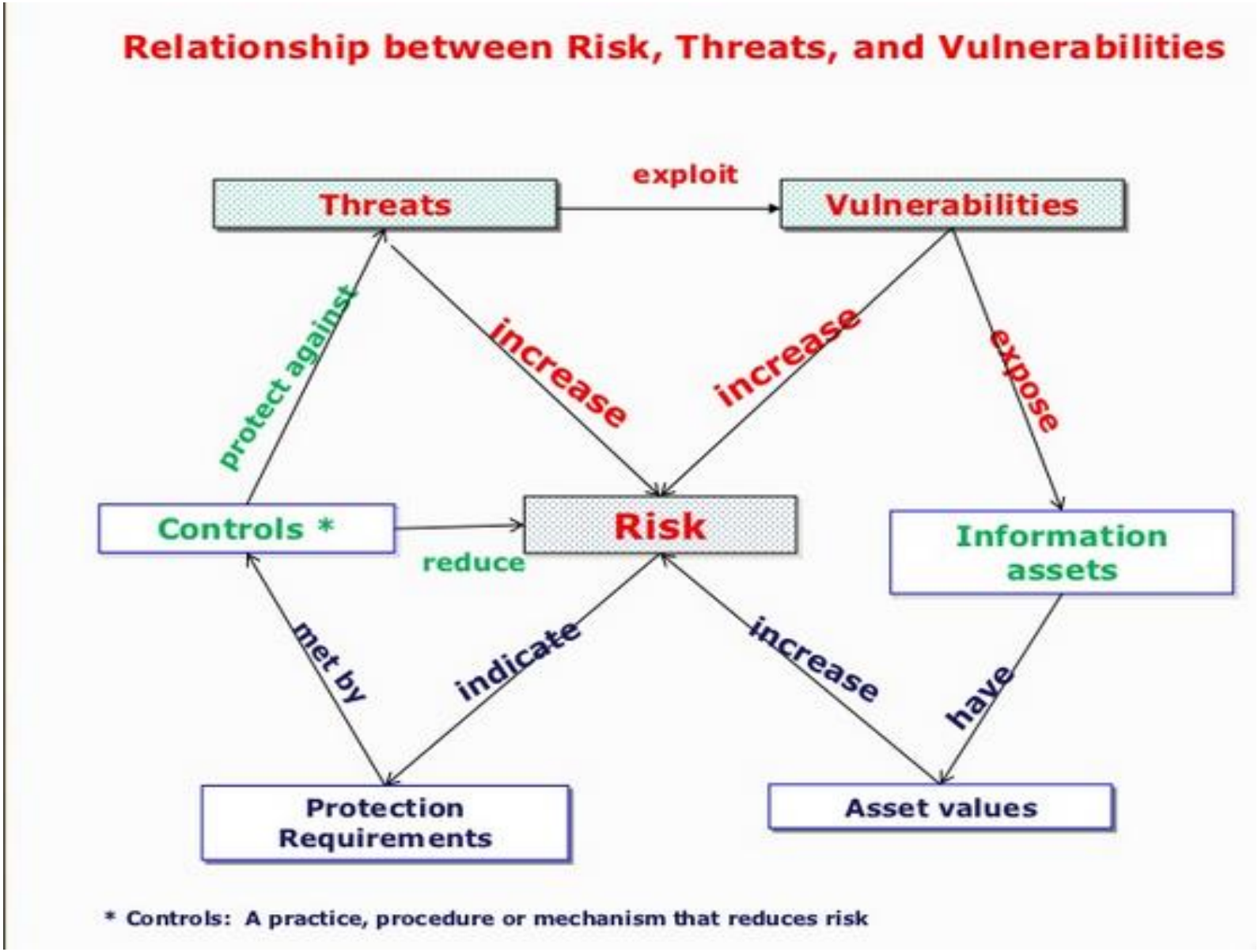
Compiled By: Tsegaye B.

Objectives

- Definition of terms
- Categories of Attack Types and Security threats
- Vulnerabilities of Information Systems
  - Malicious Codes
  - Hoaxes
  - Back Doors
  - Password Cracking
  - Brute force Attack
  - Dictionary Attack
  - DoS/DDoS
  - Spam/Mail Bombing
  - Social Engineering
  - Pharming and Phishing
- Categories of Security Controls (protection schemes)

Defining: Risk, Vulnerability, Threat, Attack and Countermeasures

- Risk: The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability
- Vulnerability: is a point where a system is susceptible to an *Attack*.(point of weakness)
- Threat: is a possible Danger to a System. It could be a person , a thing or an event that exploits a *Vulnerability*.
  - Has three elements
    - Agent
    - Motive
    - Result
- Attack: is an actual security breach that has been made (Violation of a security policy) by a *Threat*.
- Countermeasures(Controls): Techniques applied to protect a system from any attack a threat can make.


Relationship between Risk, Threats, and Vulnerabilities
Threats
exploit
Vulnerabilities
protect against
increase
increase
expose
Controls *
reduce
Risk
Information assets
met by
indicate
increase
have
Protection Requirements
Asset values
* Controls: A practice, procedure or mechanism that reduces risk

Threats

- A computer security threat is any person, act, or object that poses a danger to computer security
- Computer world is full of threats!
  - Virus, worms, etc.
- So is the real world!
  - Thieves, pick-pockets, burglars, murderers, drunk drivers, …

What we need to do

- What is the right thing?
  - To do what you do in real life
- What do you do in real life?
  - You learn about the threats
    - What are the threats
    - How can these threats affect you
    - What is the risk for you to be attacked by these threats
    - How you can protect yourself from these risks
    - How much does the protection cost
    - What you can do to limit the damage in case you are attacked
    - How you can recover in case you are attacked
  - Then, you protect yourself in order to limit the risk but to continue to live your life
- You need to do exactly the same thing with computers!

Security threats

- The Management must be informed of the different threats facing the organization

- By examining each threat category, management effectively protects information through policy, education, training, and technology controls

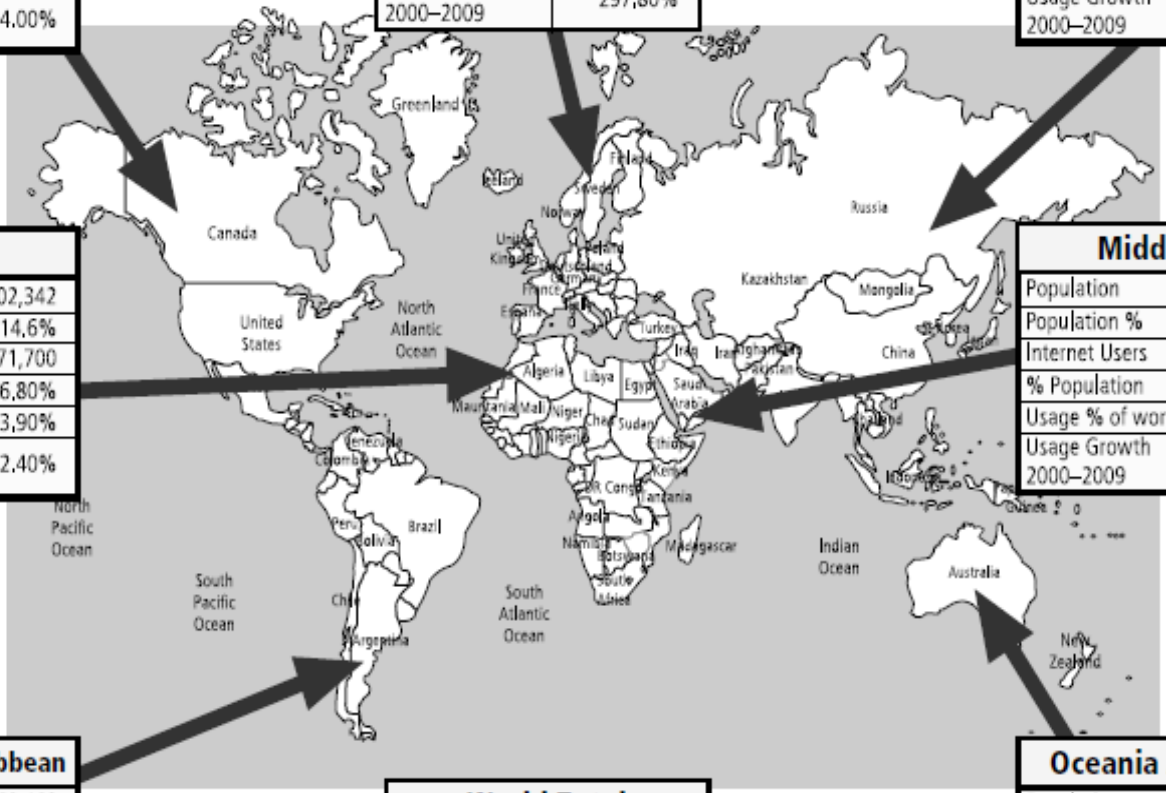
Security threats cont'd...

- The number of Internet users continues to grow; about 26 percent of the world's 6.8 billion people—that is, 1.7 billion people—have some form of Internet access.
- The 2009 Computer Security Institute (CSI) study found that 64 percent of organizations responding to the survey suffered malware infections, with only 14 percent indicating system penetration by an outsider.
- Organizations reported losses of approximately $234,244 per respondent, down from an all-time high of more than $3 million in 2001.

North America	
Population	340,831,831
Population %	5.0%
Internet Users	252,908,000
% Population	74.20%
Usage % of world	14.60%
Usage Growth 2000–2009	134.00%

Europe	
Population	803,850,858
Population %	11.9%
Internet Users	418,029,796
% Population	52.00%
Usage % of world	24.10%
Usage Growth 2000–2009	297.80%

Asia	
Population	3,808,070,503
Population %	56.3%
Internet Users	738,257,230
% Population	19.40%
Usage % of world	42.60%
Usage Growth 2000–2009	545.90%



Africa	
Population	991,002,342
Population %	14.6%
Internet Users	67,371,700
% Population	6.80%
Usage % of world	3.90%
Usage Growth 2000–2009	1392.40%

Middle East	
Population	202,687,005
Population %	3.0%
Internet Users	57,425,046
% Population	28.30%
Usage % of world	3.30%
Usage Growth 2000–2009	1648.20%

Latin America / Caribbean	
Population	586,662,468
Population %	8.7%
Internet Users	179,031,479
% Population	30.50%
Usage % of world	10.30%
Usage Growth 2000–2009	890.80%

World Total	
Population	6,767,805,208
Internet Users	1,733,993,741
% Population	25.60%
Usage Growth 2000–2009	380.30%

Oceania / Australia	
Population	34,700,201
Population %	0.5%
Internet Users	20,970,490
% Population	60.40%
Usage % of world	1.20%
Usage Growth 2000–2009	175.20%

Threats to information Systems

	Category of Threat	Examples
1.	Compromises to intellectual property	Piracy, copyright infringement
2.	Software attacks	Viruses, worms, macros, denial of service
3.	Deviations in quality of service	ISP, power, or WAN service issues from service providers
4.	Espionage or trespass	Unauthorized access and/or data collection
5.	Forces of nature	Fire, flood, earthquake, lightning
6.	Human error or failure	Accidents, employee mistakes
7.	Information extortion	Blackmail, information disclosure
8.	Missing, inadequate, or incomplete	Loss of access to information systems due to disk drive failure without proper backup and recovery plan organizational policy or planning in place
9.	Missing, inadequate, or incomplete controls	Network compromised because no firewall security controls
10.	Sabotage or vandalism	Destruction of systems or information
11.	Theft	Illegal confiscation of equipment or information
12.	Technical hardware failures or errors	Equipment failure
13.	Technical software failures or errors	Bugs, code problems, unknown loopholes
14.	Technological obsolescence	Antiquated or outdated technologies

Rank of Category of Threats (2009 & 2003, Comparison)

Categories of Threats Ranked by Greatest to Least Threat	2009 Ranking	2003 Ranking
Espionage or trespass	1	4
Software attacks	2	1
Human error or failure	3	3
Missing, inadequate, or incomplete organizational policy or planning	4	—
Missing, inadequate, or incomplete controls	5	—
Theft	6	7
Compromises to intellectual property	7	9
Sabotage or vandalism	8	5
Technical software failures or errors	9	2
Technical hardware failures or errors	10	6
Forces of nature	11	8
Quality of service deviations from service providers	12	10
Technological obsolescence	13	11
Information extortion	14	12

Acts of Human Error....

- Includes acts performed without malicious intent
- Causes include:
  - Inexperience
  - Improper training
  - Incorrect assumptions
- Employees are among the greatest threats to an organization's data- RSA – malicious e-mail was opened by the RSA's own Employee.

Acts of Human Error...

- Employee mistakes can easily lead to:
  - Revelation of classified data
  - Entry of erroneous data
  - Accidental data deletion or modification
  - Data storage in unprotected areas
  - Failure to protect information
- Many of these threats can be prevented with controls

Acts of Human Error

Who is the biggest threat to your organization?

Tom Twostory
convicted burglar

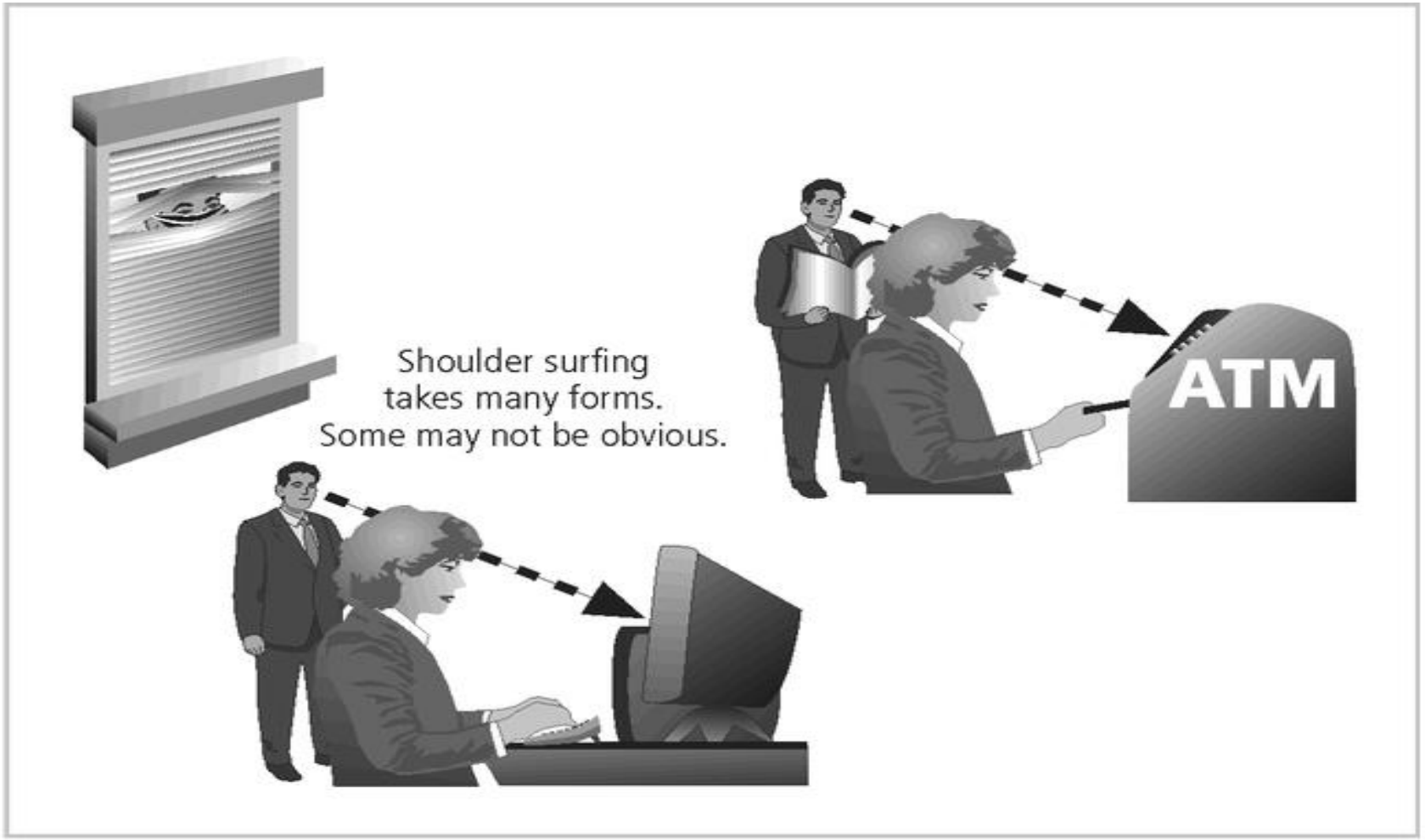
Dick Davis a.k.a.
"wannabe amateur hacker"

Harriet Allthumbs
Employee
accidentally
deleted the one copy
of a critical report

Deliberate Acts of Espionage or Trespass

- Access of protected information by unauthorized individuals
- Competitive intelligence (legal) vs. industrial espionage (illegal- china has been accused of doing this on some American companies including Google).
- Shoulder surfing occurs anywhere a person accesses confidential information
- Controls let trespassers know they are encroaching on organization's cyberspace
- Hackers use skill, guile(being tricky), or fraud to bypass controls protecting others' information

Shoulder surfing



Deliberate Acts of Theft

- Illegal taking of another's physical, electronic, or intellectual property
- Physical theft is controlled relatively easily
- Electronic theft is a more complex problem; evidence of crime not readily apparent (readily available)

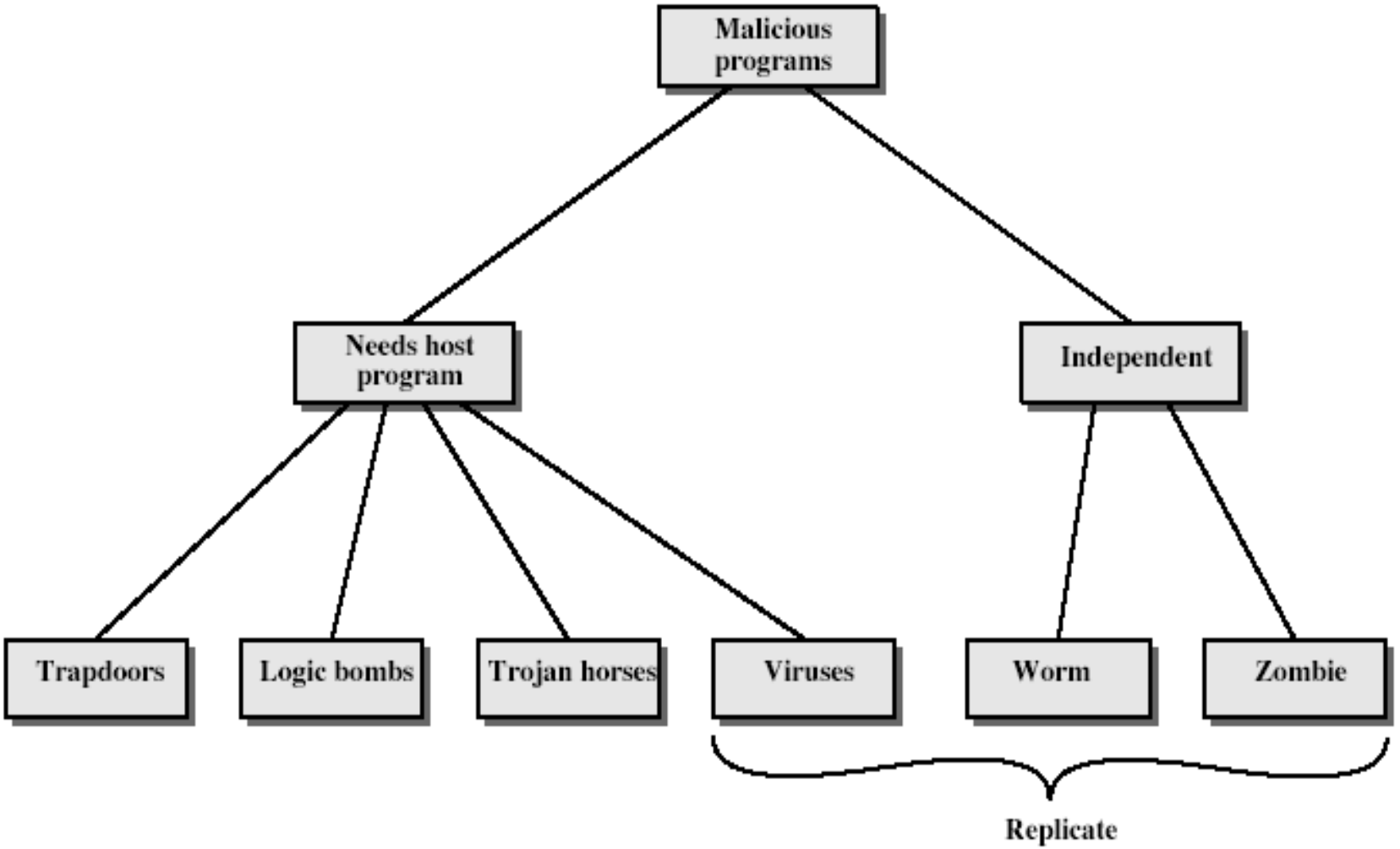
Forces of Nature

- Forces of nature are among the most dangerous threats
- Disrupt not only individual lives, but also storage, transmission, and use of information
- Organizations must implement controls to limit damage and prepare contingency plans for continued operations(Business Continuity Plan)
- These kind of threats *cannot be prevented*

Vulnerabilities of Information Systems

- Physical vulnerabilities (Eg. buildings)
- Natural vulnerabilities (Eg. Earthquake)
- Hardware and Software vulnerabilities (Eg. Failures)
- Media vulnerabilities (Eg. Disks can be stolen)
- Communication vulnerabilities (Eg. Wires can be tapped)
- Human vulnerabilities (Eg. Insiders, Outsiders)

Malicious Codes (Software)



Security Threats

Malware Attack:

- A generic term for software that has malicious(destruction, vandalism.. etc) purpose
- Examples
  - Viruses
  - Trojan horses
  - Spy-wares
  - Trapdoors
  - Logic bombs
  - Zombie

Malicious Codes (Software)

- The state-of-the-art malicious code attack is the *polymorphic*, or *multi-vector* worm.
- These attack programs use up to six *known attack replication vectors* to exploit a variety of vulnerabilities in commonly found information system devices.

Attack Replication Vectors

Vector	Description
IP scan and attack	The infected system scans a random or local range of IP addresses and targets any of several vulnerabilities known to hackers or left over from previous exploits such as Code Red, Back Orifice, or PoizonBox.
Web browsing	If the infected system has write access to any Web pages, it makes all Web content files (.html, .asp, .cgi, and others) infectious, so that users who browse to those pages become infected.
Virus	Each infected machine infects certain common executable or script files on all computers to which it can write with virus code that can cause infection.
Unprotected shares	Using vulnerabilities in file systems and the way many organizations configure them, the infected machine copies the viral component to all locations it can reach.
Mass mail	By sending e-mail infections to addresses found in the address book, the infected machine infects many users, whose mail-reading programs also automatically run the program and infect other systems.
Simple Network Management Protocol (SNMP)	By using the widely known and common passwords that were employed in early versions of this protocol (which is used for remote management of network and computer devices), the attacking program can gain control of the device. Most vendors have closed these vulnerabilities with software upgrades.

Threats/Attacks …

Hoaxes

- A hoax is a falsehood deliberately fabricated to masquerade as the truth
- A more devious attack on computer systems is the transmission of a virus hoax with a real virus attached. When the attack is masked in a seemingly legitimate message, unsuspecting users more readily distribute it.

Physical Attack (Vandalism)

- Stealing, breaking or damaging of computing devices

Malware Attack

- Viruses
  - "A small program that replicates and hides itself inside other programs usually without your knowledge.
  - Similar to biological virus: Replicates and Spreads
- Worms
  - An independent program that reproduces by copying itself from one computer to another
  - It can do as much harm as a virus
  - It often creates denial of service
- Virus and Worm Hoaxes
  - Send group e-mails warning of supposedly dangerous viruses that don't exist.
    - Ex. msgs on Facebook

Malware Attacks…

- Trojan horses
  - (Ancient Greek tale of the city of Troy and the wooden horse) - ??
  - Seems to do something good but covertly doing something else
  - Secretly downloading a virus or some other type of malware on to your computers.
  - Popular mechanism for disguising a virus or a worm

Malware Attack...

- Spy-wares
  - "A software that literally spies on what you do on your computer."
  - Example: Simple Cookies and Key Loggers
- Logic Bomb
  - one of oldest types of malicious software
  - code embedded in legitimate program (Trojan horse)
  - activated when specified conditions met
    - eg presence/absence of some file
    - particular date/time
    - particular user
    - particular series of keystrokes
  - when triggered typically damage system
    - modify/delete files/disks

Threats/Attacks…

Denial of Service (DoS) Attack

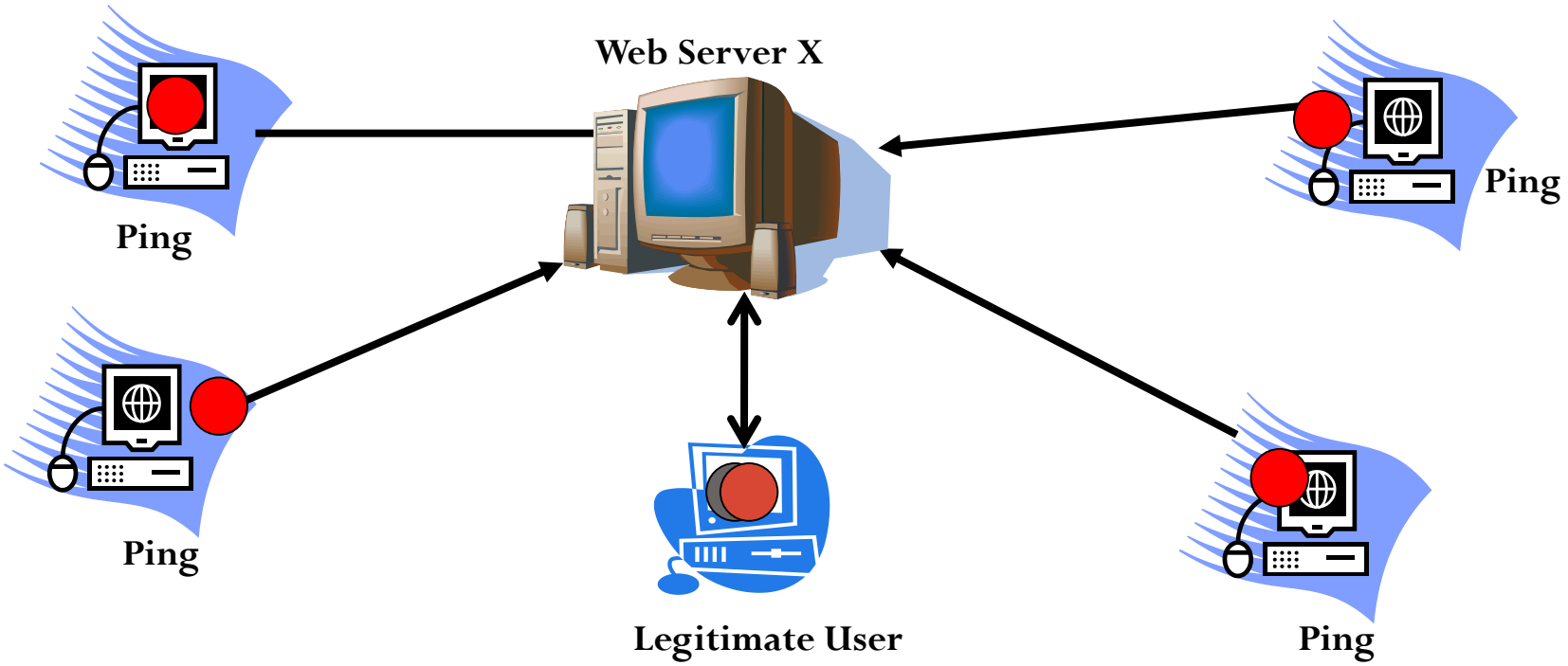
- Blocking access from legitimate users
- In a denial-of-service (DoS) attack, the attacker sends a large number of connection or information requests to a target

Distributed DoS Attack

- A distributed denial-of-service (DDoS) is an attack in which a coordinated stream of requests is launched against a target from many locations at the same time.
- Exploits known flaws in network systems
- A botnet (also known as a zombie army) is a number of Internet computers that, although their owners are unaware of it, have been set up to forward transmissions (including spam or viruses) to other computers on the Internet. Eg. IoT devices stream of data→used for the recent attack on America and UK.

Simple illustration of DDoS attack (from Easttom)

```
C:\>Ping <address of X> -l 65500 –w 0 -t
```



Malware Attack…

- Trap door/Backdoor
  - Is a mechanism built into a system by its designer
  - A trapdoor usually gives the designer away to sneak back into the system
  - Gives the original designer a secret route into the system

Threats/Attacks Cont'd...

- **Password Cracking:**
  - Attempting to reverse-calculate a password is often called **cracking**. A cracking attack is a component of many dictionary attacks.
- **Brute Force Attack:**
  - The application of computing and network resources to try every possible password combination is called a **brute force attack**. Since the brute force attack is often used to obtain passwords to commonly used accounts, it is sometimes called a **password attack**.

Brute Force on Case insensitive password

Using a standard alphabet set (case *in*sensitive) without numbers or special characters = 26 characters in set, on an average 2008-era dual-core PC performing 30,000 MIPS (million instructions per second):

Password Length	Maximum Number of Operations (guesses)	Maximum Time to Crack
8	208,827,064,576	7.0 seconds
9	5,429,503,678,976	3.0 minutes
10	141,167,095,653,376	1.3 hours
11	3,670,344,486,987,780	34.0 hours
12	95,428,956,661,682,200	36.8 days
13	2,481,152,873,203,740,000	2.6 years
14	64,509,974,703,297,200,000	68.2 years
15	1,677,259,342,285,730,000,000	1,772.9 years
16	43,608,742,899,428,900,000,000	46,094.1 years

Brute Force on case sensitive password

Using an extended data set with case sensitive letters (upper and lower case), numbers, and 20 special characters = 82 characters in set, on the same 2008-era dual-core PC:

Password Length	Maximum Number of Operations (guesses)	Maximum Time to Crack
8	2,044,140,858,654,980	18.9 hours
9	167,619,550,409,708,000	64.7 days
10	13,744,803,133,596,100,000	14.5 years
11	1,127,073,856,954,880,000,000	1,191.3 years
12	92,420,056,270,299,900,000,000	97,687.4 years
13	7,578,444,614,164,590,000,000,000	8,010,363.4 years
14	621,432,458,361,496,000,000,000,000	656,849,799.6 years
15	50,957,461,585,642,700,000,000,000,000	53,861,683,563.4 years
16	4,178,511,850,022,700,000,000,000,000,000	4,416,658,052,197.2 years

Threats/Attacks Cont'd...

- **Dictionary Attack:**
  - The **dictionary attack** is a variation of the brute force attack which narrows the field by selecting specific target accounts and using a list of commonly used passwords (the dictionary) instead of random combinations
- **Spam:** is unsolicited commercial e-mail.
- **Mail Bombing:**
  - Another form of e-mail attack that is also a DoS, is called a **mail bomb**, in which an attacker routes large quantities of e-mail to the target.

Hackers/Intrusion Attack:

Hacking Attack:

- Any attempt to gain unauthorized access to your system but without causing a damage

Cracking:

- Criminal who breaks into computer systems for the purpose of doing damage.

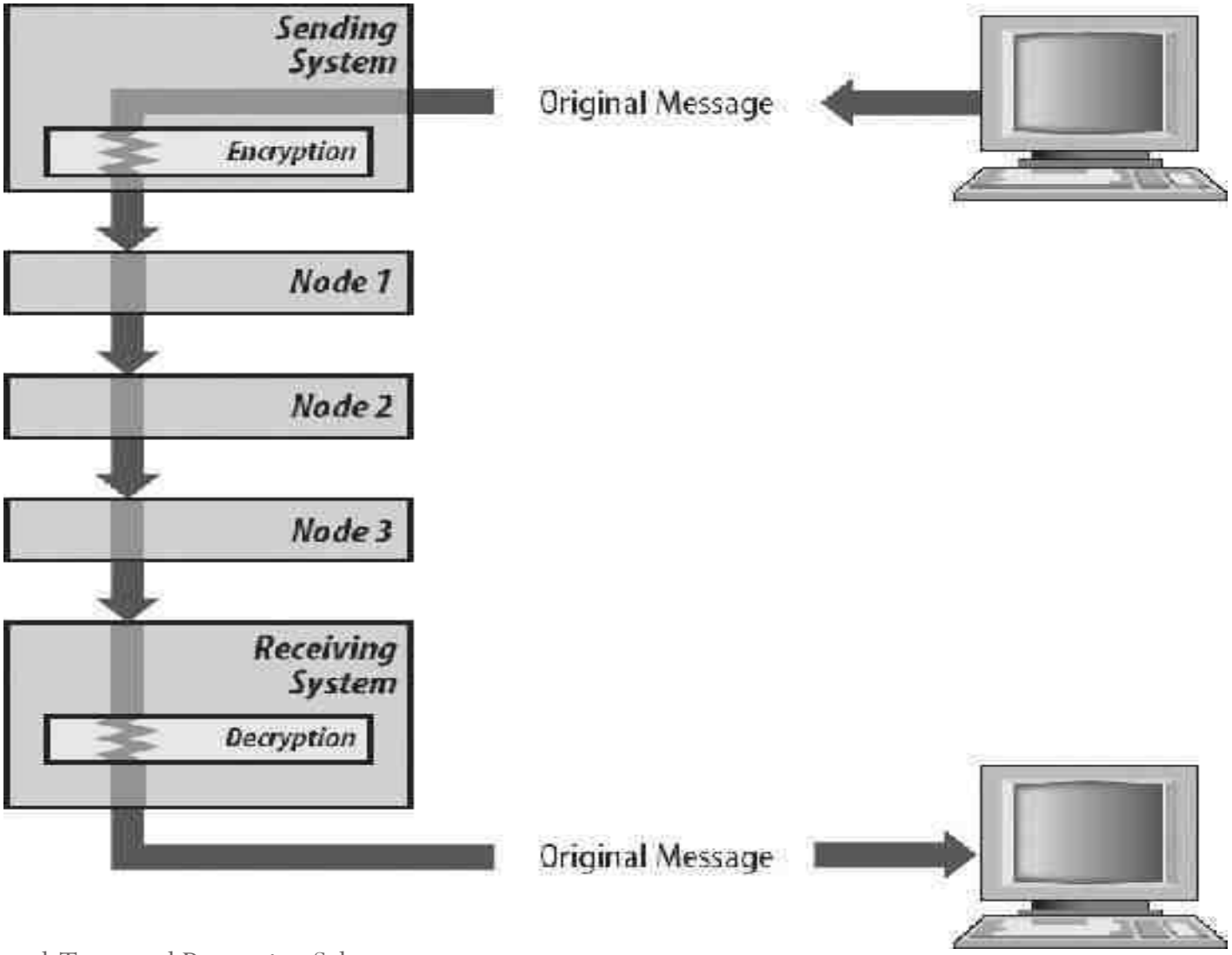
Communication threats

- **Masquerade:** occurs when someone(an imposter) pretends to be an authorized user
- **Playback (a replay):**occurs when someone records a legitimate message (perhaps fund transfer) and resend it latter.
- **A repudiation:** occurs when someone denies that s/he has sent or received a message.
- **Denial of Service:** Occurs when someone or something dominates systems resources and prevents access to legitimate users

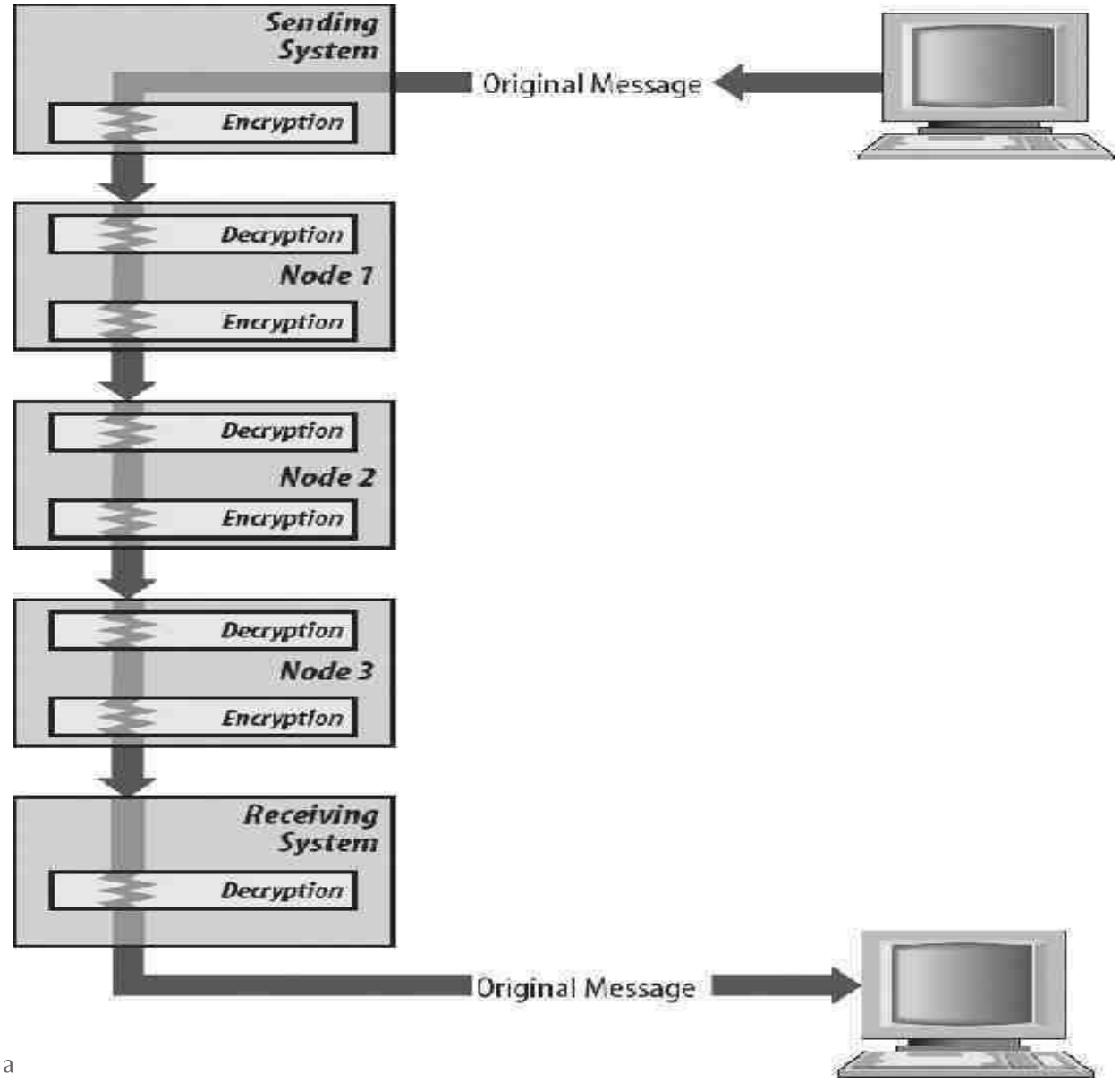
Encrypted Communications

- **Two types of Encryption approaches for protection of Data in Transit**
  - End-to End Encryption(Off-line Encryption)
    - A message is encrypted when it is transmitted and is decrypted when it is received
      - IP Header in clear text- for routing purpose
      - Only payload(Data) is encrypted
  - Link Encryption(Online encryption)
    - A message is Encrypted when it is transmitted and then decrypted and encrypted again each time it passes through a network node.
      - IP Header info encrypted/Decrypted at each node
      - Payload data is not decrypted except at destination.

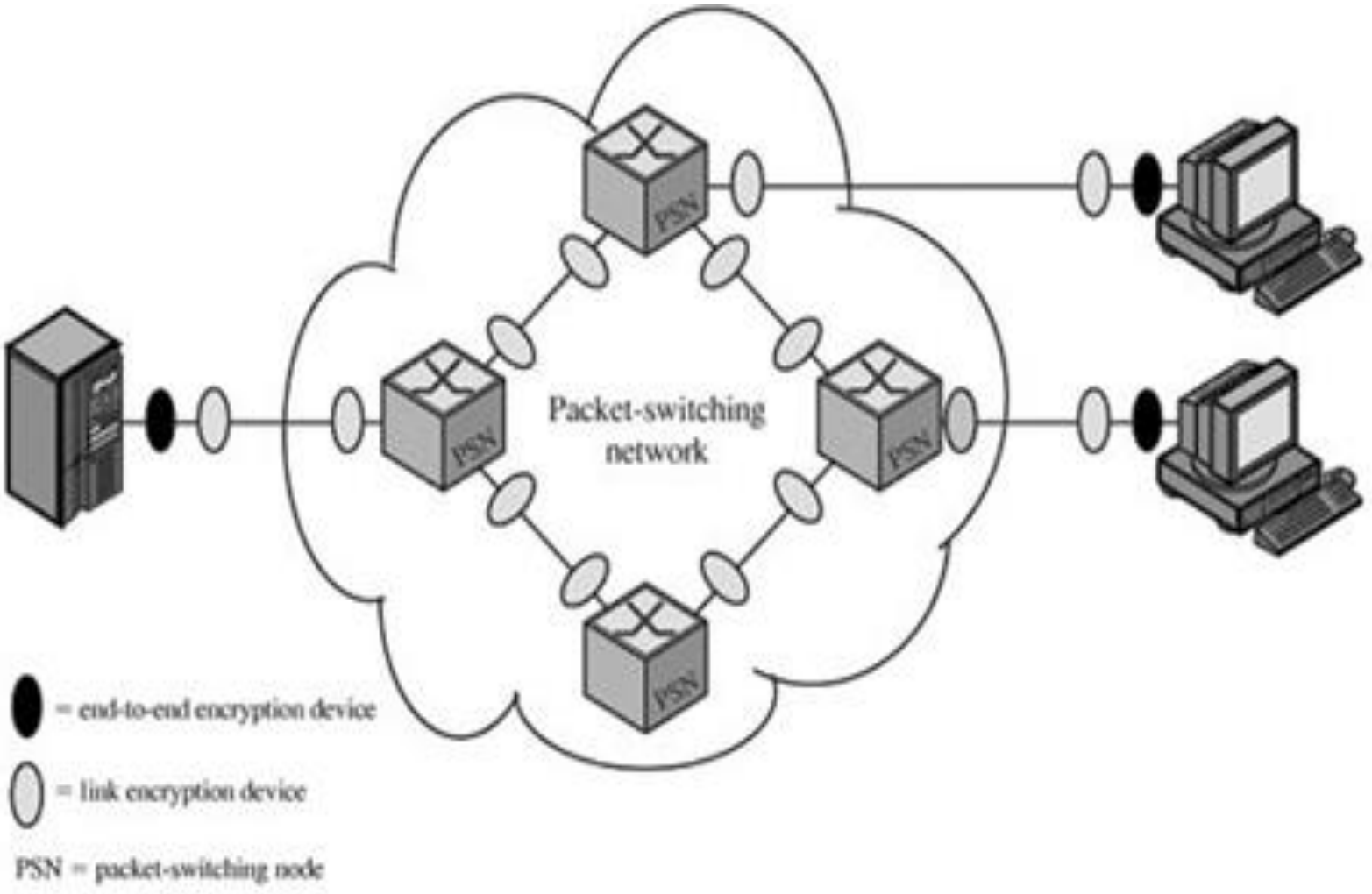
End-to-End-Encryption System



Link Encryption



Encryption across a packet - switching Network- Combination of approaches



Social Engineering

- Social Engineering is a kind of attack that uses the weakest link. (one of the security principles – "secure the weakest link")
- They take advantage of our human characteristics (human psychology) to exploit us, tricking us to break normal security procedures.
- Social Engineering succeeds because people are people- want to be advantageous/get something the shortest way.(egoistic)

Social Engineering

-social engineers are hackers who exploit the weakness that is found in each and every organization(human psychology) Using phone calls and social media, these attackers trick people into offering them access to sensitive information.

-Email spoofing is the creation of email messages with a forged sender address. Because the core email protocols do not have any mechanism for authentication, it is common for spam and phishing emails to use such spoofing to mislead or even prank the recipient about the origin of the message.

-Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business. Although often intended to steal data for malicious purposes, cybercriminals may also intend to install malware on a targeted user's computer

-Vishing is the telephone equivalent of phishing. It is described as the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft.

-SMiShing is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device. SMiShing is short for "SMS phishing.

-Pharming is a cyber attack intended to redirect a website's traffic to another, fake site. Pharming can be conducted either by changing the hosts file on a victim's computer or by exploitation of a vulnerability in DNS server software

Social Engineering

- Social-engineering schemes use 'Spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers by Hijacking brand names of banks, e-retailers and credit card companies.
- Phishing is an attempt to criminally and fraudulently acquire sensitive information, such as usernames, passwords and credit card details, by masquerading as a trustworthy entity in an electronic communication. eBay, PayPal and online banks are common targets.
- Phishers often convince recipients to respond.
- Pharming is crimeware (software for Criminal activity) that misdirects users to fraudulent sites or proxy servers (bogus website), typically through DNS hijacking or poisoning.

Social Engineering Cont'd...

Different types of phishing

- Spear Phishing? Spoofed e-mail
- Vishing ? Voice message
- Smishing? SMS-via mobile

- Phishing and pharming cannot be protected by anti-virus or anti-spyware programs rather need to have specialized programs like anti-phishing and anti-pharming (see www.antiphishing.org)

Protection Schemes (details on Chapter 4)

- Computer security controls
  - Authentication (Password, cards, biometrics, IP)
  - Encryption
  - Auditing
  - Administrative procedures
  - Standards
  - Certifications
  - Physical security
  - Laws
  - Backups