



Chapter 2 - Computer Security Threats and Attacks

2.1 Threats and Attacks

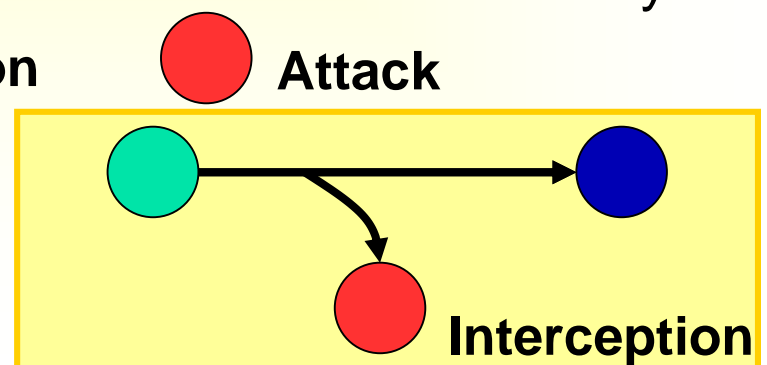
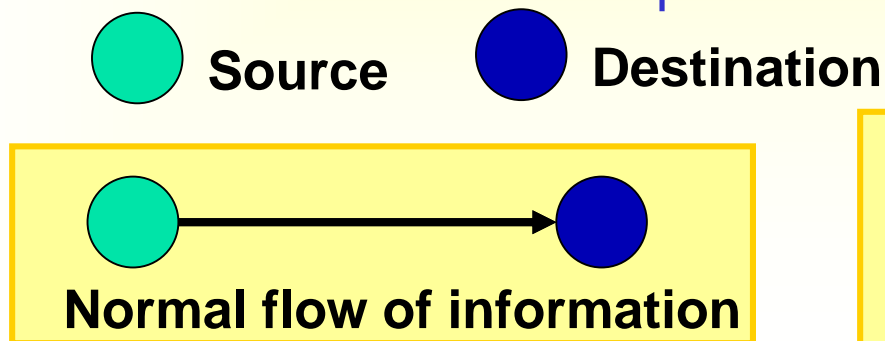
- A computer security **threat** is a **potential** violation of **security**; it is any person, act, or object that poses a danger to computer security/privacy
- The violation need not actually occur for there to be a threat
- The fact that the violation might occur means that those actions that could cause it to occur must be guarded against (or prepared for)
- Those actions are called **attacks**
- Those who execute such actions, or cause them to be executed, are called **attackers**
- The computer world is full of threats; viruses, worms, crackers, etc.
- And so is the real world; thieves, pick-pockets, burglars, murderers, drunk drivers, ...
- Note: the terms **threat** and **attack** are commonly used to mean more or less the same thing

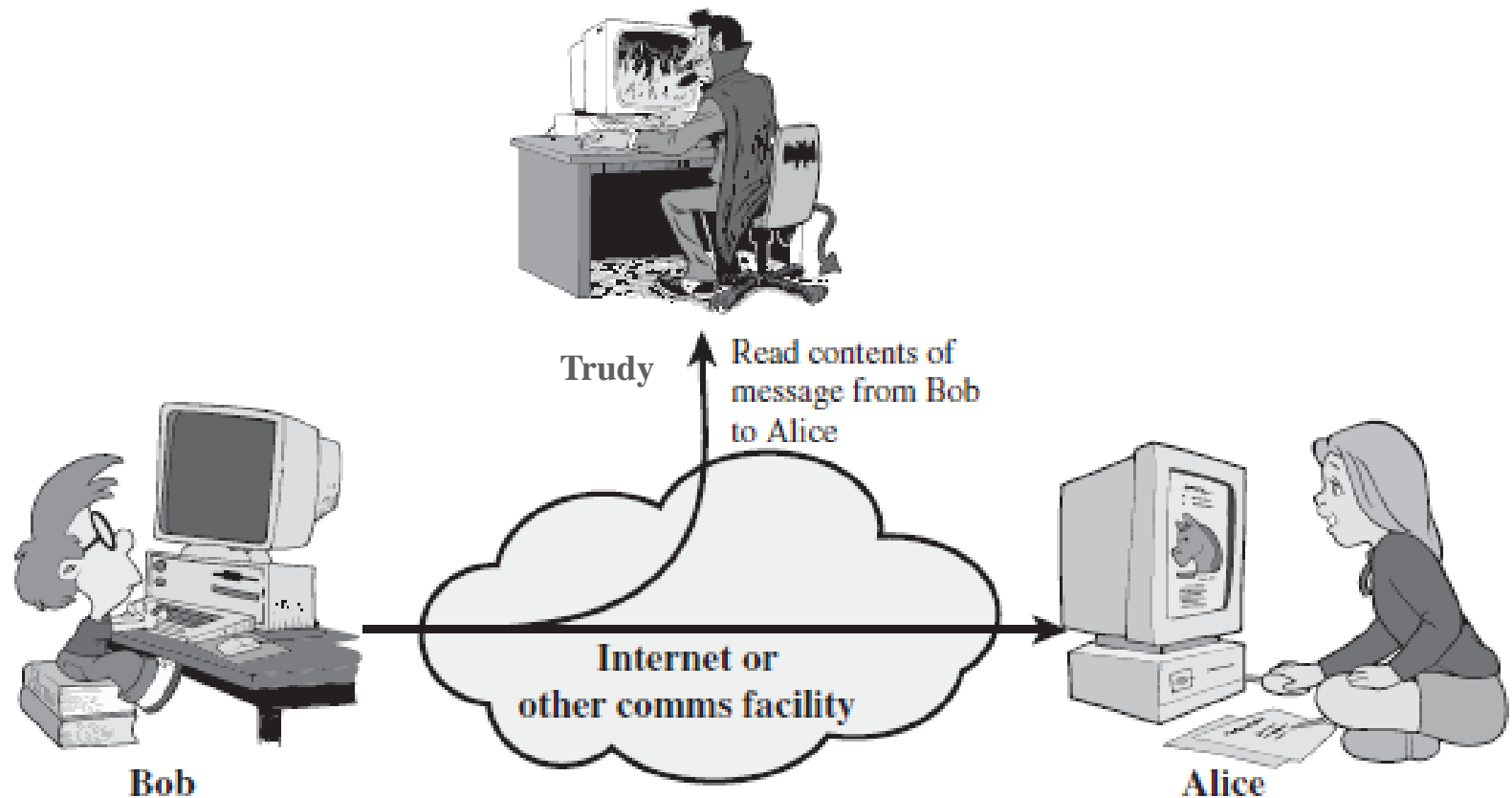
- Types of threats
 - **Disclosure**: unauthorized access to information (also called **Snooping or Interception**)
 - e.g., Snooping: unauthorized interception of information
 - **Deception**: acceptance of false data (**modification**, **spoofing**, **repudiation of origin**, **denial of receipt**)
 - e.g., Modification: unauthorized change of information
 - **Disruption**: interruption or prevention of correct operation
 - Disrupting access to or use of information or an information system; disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance
 - **Usurpation**: unauthorized control of some part of a system
 - e.g., Identity theft; Denial of service

- 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 can you do to limit the damage in case you are attacked
 - How can you 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!

- Types of attacks: One way of categorizing attacks is as **passive** and **active**
 - **Passive Attacks**
 - A passive attack attempts to learn or make use of information from the system but does not affect system resources
 - There are two types of passive attacks: **release of message contents** (or **sniffing**) and **traffic analysis**
 - **Release of message contents**: A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information; we would like to prevent an opponent from learning the contents of these transmissions
 - It is also called **interception**: An attack on confidentiality

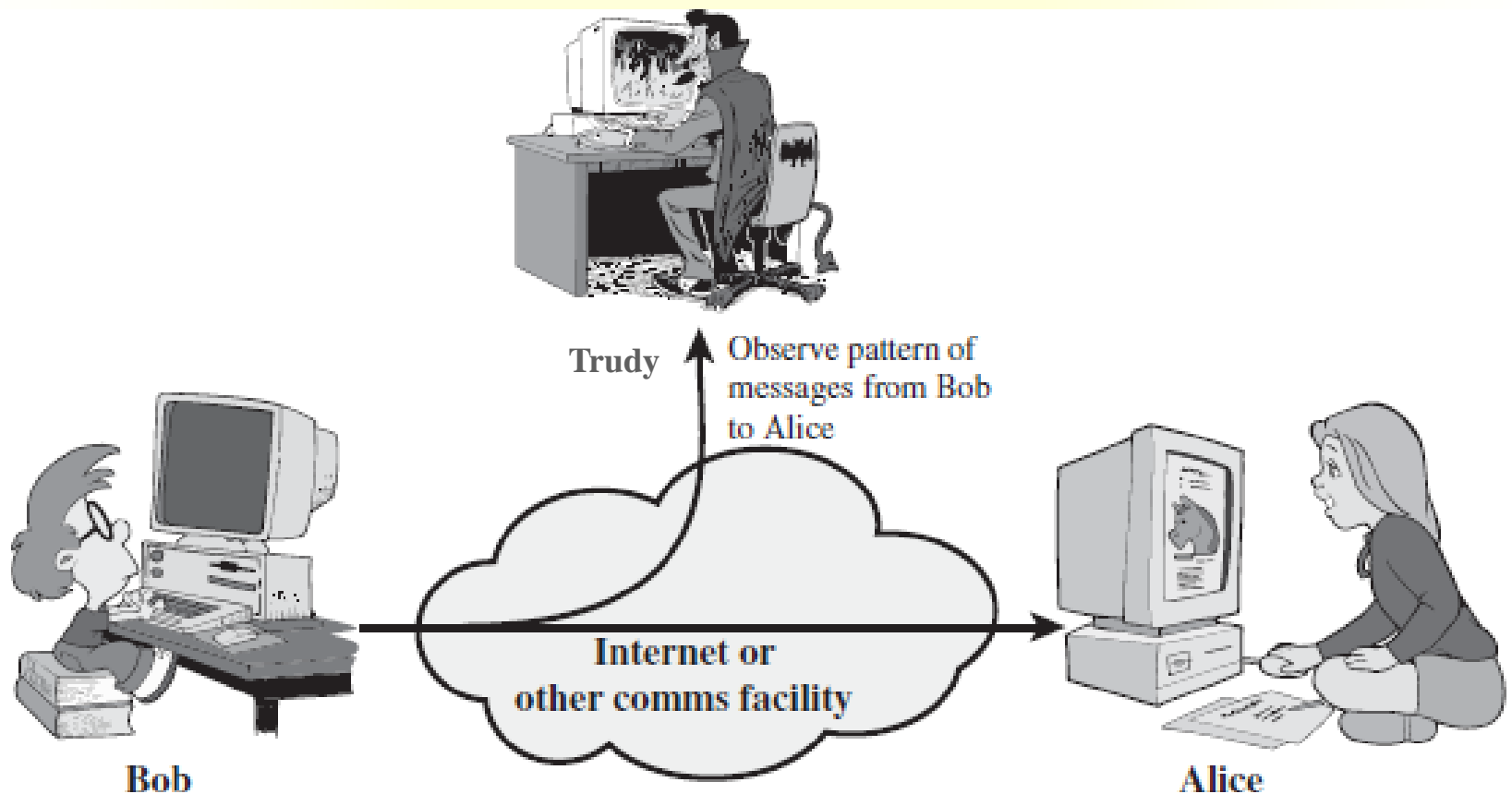




- Friends and Enemies: Alice, Bob, Trudy
 - Well-known in the network security world
 - Alice and Bob (lovers!) want to communicate “securely”
 - Trudy (the intruder) may intercept, delete, or add messages

- Alice and Bob could be
 - two routers that want to exchange router tables securely
 - a client and a server that want to establish a secure transport connection
 - two e-mail applications or persons that want to exchange secure e-mail
 - a person transferring his credit card number securely to a web server
 - a person interacting with his/her bank online
 - etc.

- **Traffic analysis:** to determine the location and identity of communicating hosts and to observe the frequency and length of messages being exchanged (even if the message is encrypted). This information might be useful in guessing the nature of the communication that was taking place




- Packet sniffer: a program that records a copy of every packet that flies by including such sensitive information as passwords, trade secrets, private personal messages, etc.
- Sniffed packets can then be analysed offline for sensitive information
- Broadcast media (Ethernet LANs and wireless LANs) are the most vulnerable
- Sniffers can also be planted at an institution's router and copy all packets going to/from the organization
- Packet sniffer software are freely available and some are commercial; e.g., [Wireshark](#) is a (free) packet sniffer; others include [etherfind](#), [windump](#), [tcpdump](#), and network management utilities such as [SnifferPro](#) (they usually require administrator privilege)
- Note: sniffer programs are two-edged!
 - attacker uses them for eavesdropping
 - defender uses them for defense purposes: intrusion detection

- It is usually difficult to detect passive attacks because they do not involve any alteration of the data
- **Snooping**
 - Snooping is a passive attack; it is unauthorized interception of information, e.g., **passive wiretapping** (not necessarily physical wiring)
 - It is a form of **disclosure**
- **Active Attacks**
 - An active attack attempts to alter system resources or affect their operation
 - The transmitted data is fully controlled by the **intruder**
 - The attacker can **modify**, **delete** or **view** any data
 - This is quite possible in TCP/IP since the frames and packets are not protected in terms of authenticity and integrity (more later in Chapter 4 - Network Security Concepts and Mechanisms)

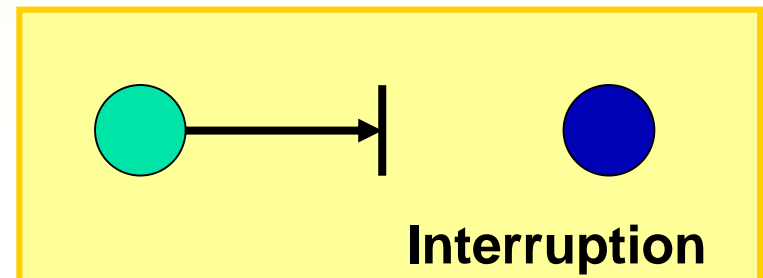
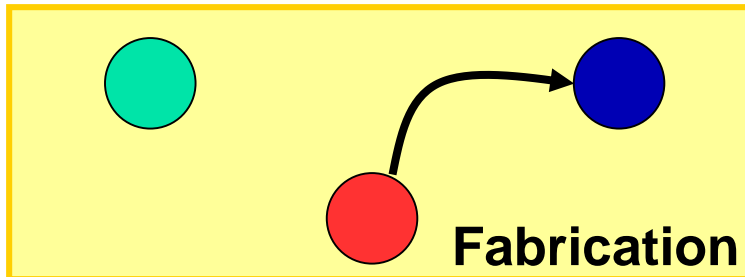
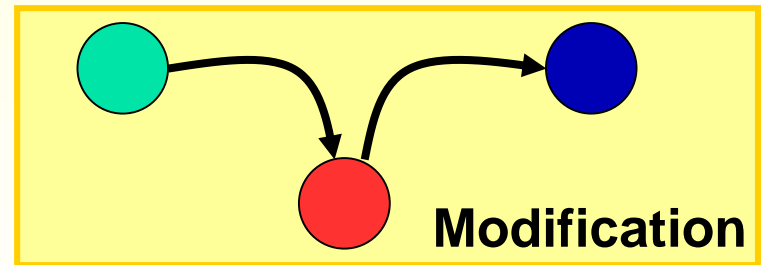
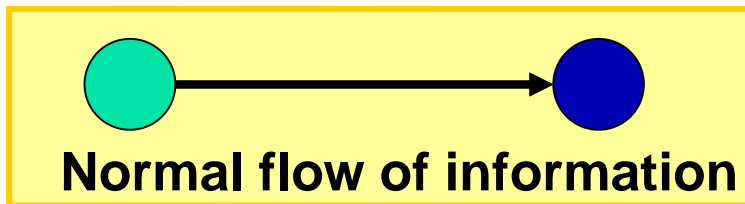
■ Categories of Active Attacks

1. **Spoofing or Masquerading**: also called **fabrication**: An attack on **authenticity**
2. **Modification or Alteration**: An attack on **integrity**
3. **Delay**: Could be classified as an attack on **availability**
4. **Denial of Service (DOS)** or **degrading of service** or **Interruption**: An attack on **availability**

 **Source**

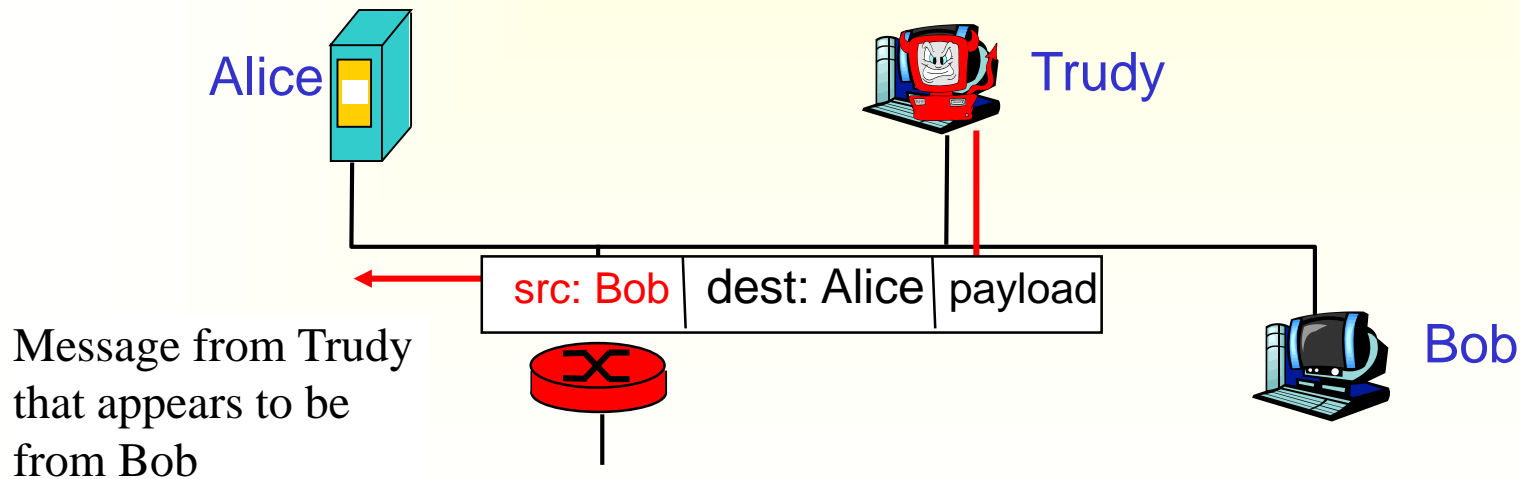
 **Destination**

 **Attack**



1. Spoofing or Masquerading

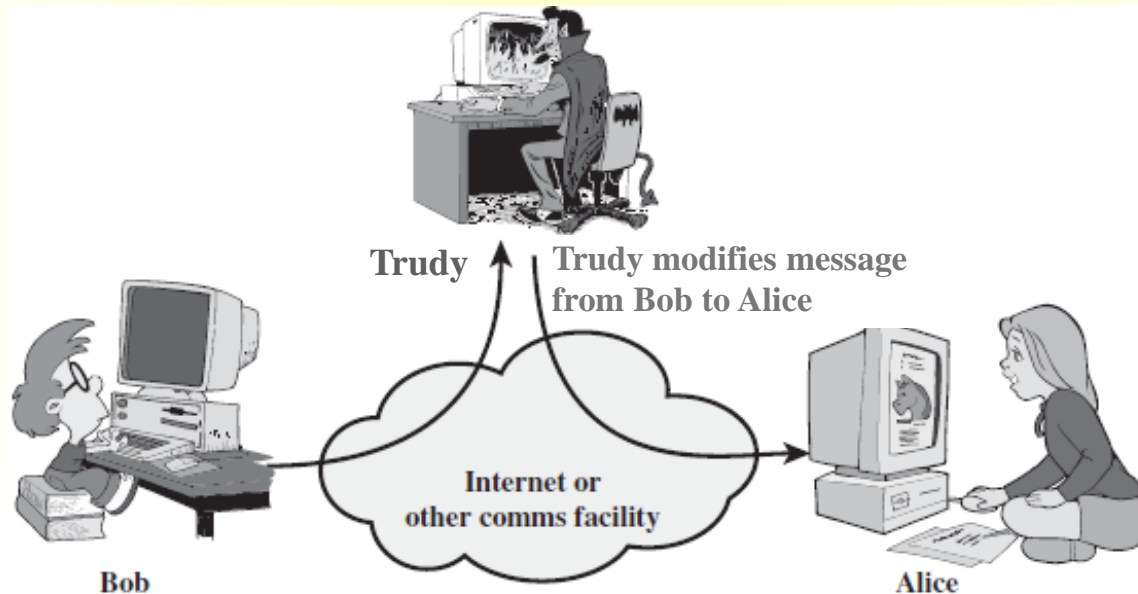
- A situation in which one person or program successfully imitates another (impersonation) by falsifying data and thereby gaining an illegitimate advantage
- It lures a victim into believing that the entity with which it is communicating is a different entity. For example, if a user tries to log into a computer across the Internet but instead reaches another computer that claims to be the desired one



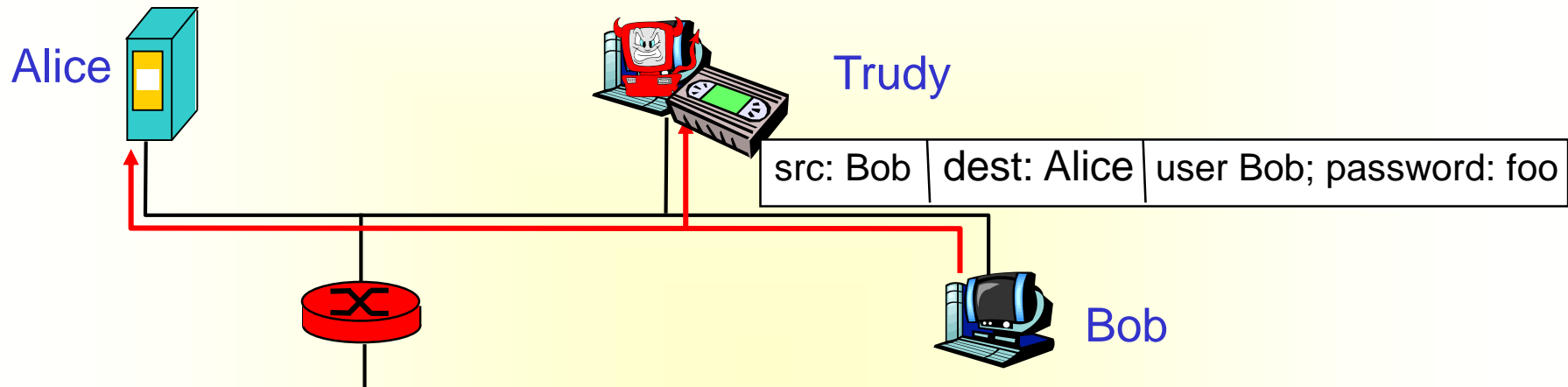
- It is a form of both deception and usurpation
- **Note: Delegation** is a form of Masquerading that occurs when one entity authorizes a second entity to perform functions on its behalf and is **not** a violation of security
- Common examples of spoofing
 - **IP spoofing**: the ability to inject packets to the Internet with a false source address; then the receiver performs some commands embedded in the packet's payload (say modifies its forwarding table)
 - **DNS spoofing**
 - Changing the DNS information so that it directs to a wrong machine
 - **URL spoofing/Webpage phishing**
 - A legitimate web page such as a bank's site is reproduced in "look and feel" on another server under the control of the attacker (More later in Section 2.3)
 - **E-mail address spoofing**

2. Modification or Alteration

- An unauthorized change of information
- Covers three classes of threats
 - **Deception**: if some entity relies on the modified data to determine which action to take
 - **Disruption** and **usurpation**: if the modified data controls the operation of the system
- **Active wiretapping** is a form of modification in which data moving across a network is altered



- An example is the **man-in-the-middle** attack, in which an intruder reads messages from the sender and sends (possibly modified) versions to the recipient



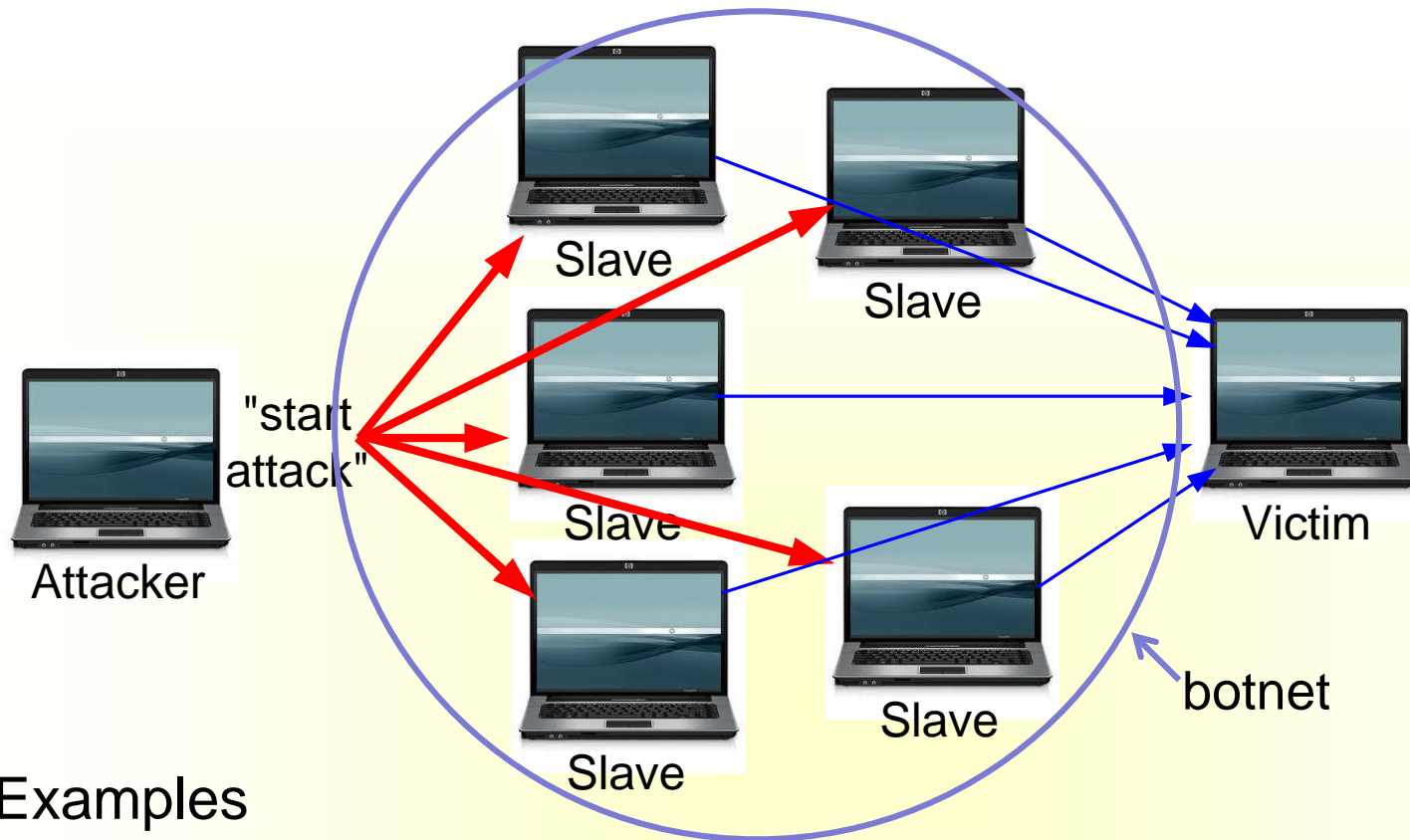
3. Delay

- A temporary inhibition of a service
- Is a form of usurpation
- If an attacker can force the delivery to take more time for a message through manipulation of system control structures, such as network components or server components

4. Denial of Service (DOS) or degrading of service attack

- Attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming with bogus traffic
- It is blocking access (prevention) of legitimate users to a service/system
- Is a form of usurpation
- The denial may occur at the source (by preventing the server from obtaining the resources needed to perform its function), at the destination (by blocking the communications from the server), or along the intermediate path (by discarding messages from either the client or the server, or both)

- Any device has operational limits (**workload**)
- A **workload** for a computer system may be defined by the number of simultaneous users, the size of files, the speed of data transmission, or the amount of data stored
- If the requests exceed any of those limits, the excess load will stop the system from responding. For example, if one can flood a web server with more requests than it can process, it will be overloaded and will no longer be able to respond to further requests
- **Distributed DoS**: attacking a target (victim) by many computers called **Zombies** (or **Slaves** or **bots**) which are members of a **botnet** simultaneously with large number of packets since just one machine is not going to adversely affect the target (or can be easily traced)
 - How many machines to use to deny service depends on the capacity of the target



- Examples
 - **E-mail bombing**: flooding someone's mail store
 - **Smurf attack**: is a DDoS attack in which large numbers of ICMP packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address. The recipients will respond to the victim flooding it
 - There had been reports of incidences of DDoS **attacks** against major sites such as **Amazon**, **Yahoo**, **CNN** and **eBay**

- Common DDOS tools used

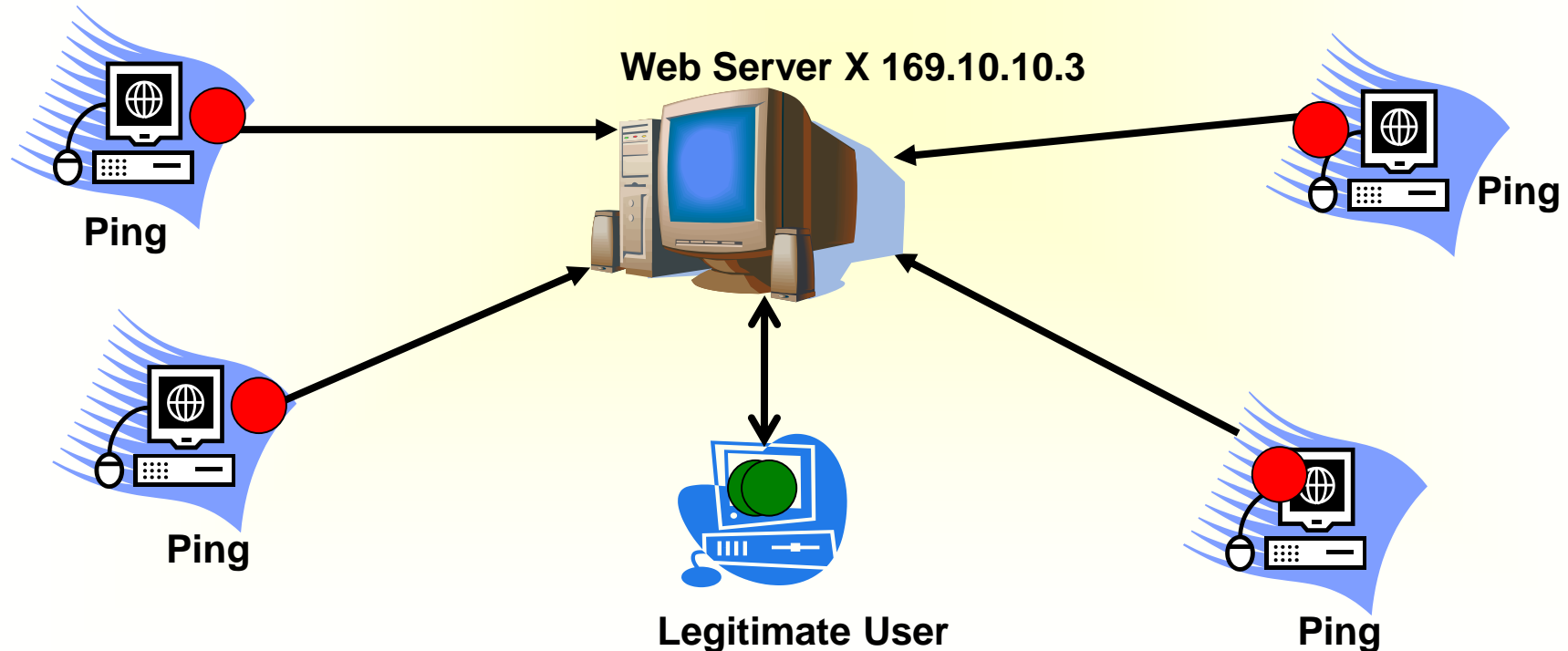
- TFN (Tribal Flood Network), TFN2K, and Stacheldraht (means barbed wire in German)

- -l 65000 buffer size

- -t continue until stopped (Ctrl-C)

Simple illustration of DDoS attack (from Easttom)

```
C:\>Ping 169.10.10.3 -l 65000 -t
```



■ More on Botnets

- A **botnet** is a collection of machines that have been compromised (a.k.a **zombies**) and are being controlled remotely by one or more individuals
- It is a huge **distributed network** of infected computers that are commanded through **command-and-control** servers (or **C2** servers)
- Bot software is usually delivered as a payload within a virus or worm
- It travels from machine to machine creating an army of zombies
- The zombies log on to a C2 server and wait for orders
- A user has no idea that his machine is a zombie, but the machine may suddenly become slower

- Once a botnet has been established, it can be leased to send **spam**, to enable **phishing scams** geared toward **identity theft**, to perform **DDoS attacks**, etc.
- e.g., in September 2005, police in the Netherlands uncovered a botnet consisting of 1.5 million zombies

- **Types of Threats/Attacks** – another way of categorizing attacks
 - **Physical Attack**
 - Stealing, breaking or damaging of computing devices
 - Covered in Chapter 1
 - **Denial of Service (DoS) Attack**
 - Already Covered
 - **Malware Attack**
 - A generic term for software that has malicious purpose
 - **Hacking (Intrusion) Attack**
 - **Hacking**: is any attempt to intrude or gain unauthorized access to a system either via some operating system flaw or other means. The purpose may or may not be malicious

- There are three groups of hackers
 - A **white hat hacker**, upon finding some flaw in a system, will report the flaw to the vendor of that system (probably anonymously) and explain exactly what the flaw is and how it was exploited. White hat hackers, also called **Sneakers**, are often hired specifically by companies to do penetration tests. The European Council even has a certification test for white hat hackers, the **Certified Ethical Hacker test**
 - A **black hat hacker** is the person normally depicted in the media. Once s/he gains access to a system, her/his goal is to cause some type of harm. S/he might steal data, erase files, etc. Black hat hackers are sometimes referred to as crackers. **Cracking** is hacking conducted for malicious purposes
 - **There is always an ongoing arms race between Black Hats and White Hats**
 - A **gray hat hacker** is normally a law-abiding citizen, but in some cases will venture into illegal activities

- **Script Kiddies**
 - A hacker is an expert in a given system; as with any profession it includes its share of frauds
 - So what is the term for someone who calls himself or herself a hacker but lacks the expertise?
 - The most common term for this sort of person is **script kiddy**
 - The name comes from the fact that the Internet is full of utilities and scripts that one can download to perform some hacking tasks
- **Phreaking**
 - One specialty type of hacking involves breaking into telephone systems
 - It is the action of using mischievous and mostly illegal ways in order not to pay for some sort of telecommunications bill, order, transfer, or other service
 - Phreaking requires a significant knowledge of telecommunications

2.2 Malware Attack

- Examples are
 - Viruses
 - Worms
 - Trojan horses
 - Spywares and Adwares
 - Logic bombs
 - Bacteria or Rabbit
 - A Nonvirus Virus or a Hoax
 - Scam, Identity theft, and Phishing
 - Rootkit, Malicious Web-Based Code, e-payment frauds, and Spam
- **Virus**
 - “A program fragment that replicates and hides itself inside other programs usually without your knowledge.”
 - Similar to a **biological** virus: replicates and spreads by its own
 - Damage varies on what the writer thinks

■ Worm

- An independent program that reproduces by copying itself from one computer to another (usually through networks)
- It can do as much harm as a virus
- It often creates denial of service
- Note: the classification of a malware as a virus or a worm is not universally agreed upon

■ Trojan Horse

- Ancient Greek tale of the city of Troy and the wooden horse which was full of soldiers
- A Trojan horse, appearing to be benign software, may secretly download a virus or some other type of malware on to your computers
- The program does what the user expects but it does more, unnoticed by the user

■ Spyware

- “A software that literally spies on what you do on your computer”
- Examples
 - Cookies: Any data that the cookie saves can be retrieved by any website, so your entire Internet browsing history can be tracked
 - Key Loggers: a computer program that records every keystroke made by a computer user, in order to gain access to passwords and other confidential information
- Legal Uses of Spyware
 - Employers may use spyware as a means of monitoring employee use of company technology
 - Parents may use this type of software on their home computer to monitor the activities of their children on the Internet to protect their children from online predators

- **Adware**: a piece of spyware that downloads to your PC when you visit certain websites. It is benign in that it causes no direct harm to a system or files, nor does it gather sensitive information from a PC. However, it is incredibly annoying as it saturates a machine with unwanted ads
- For a list of known spyware products on the Internet and for information about methods one can use to remove them, visit the Counterexploitation website at www.cexx.org
- The Spyware Guide website (www.spywareguide.com) also lists spyware that you can get from the Internet
- **Logic bomb**
 - Software that lays dormant until some specific condition is met; that condition is usually a date and time; when the condition is met, the software does some malicious act such as deleting files, altering system configuration, or perhaps releasing a virus

- A **Nonvirus Virus** or a **Hoax**
 - Another new type of virus
 - Rather than actually writing a virus, a perpetrator sends an e-mail to every address he has. The e-mail claims to be from some well-known antivirus center and warns of a new virus that is circulating. The e-mail instructs people to delete some file from their computer to get rid of the virus. The file, however, is not really a virus but part of a computer's system
 - Some people could even e-mail their friends and colleagues to warn them to delete such a file from their machines
- **Bacteria** or **Rabbit**
 - A **bacterium** or a **rabbit** is a program that absorbs all of some class of resource

- The following piece of code could exhaust disk space

```
while true do
{
    mkdir x
    chdir x
}
```

- Other Forms of Malware

- More on **scam**, **identity theft**, and **phishing** in Section 2.3
- Read about the following: **Rootkit**, **Malicious Web-Based Code**, **e-payment frauds**, and **Spam**

- Most software based attacks are viruses/worms: How do they work? Or what are the major steps?

1. Infection (Mechanisms)

- First, the virus should search for and detect objects to infect
- Installation into the infectable object
 - Writing on the boot sector (but becoming outdated)
 - Scan the computer for connections to a network, then copy itself to other machines on the network to which the infected computer has access
 - Read your email address book and email itself to everyone in your address book
 - Add some code to executable programs
 - Add some code to initialization/auto-executable programs
 - Write a macro in a word file, etc.
- The term **virulent** is a measure of how rapidly the infection spreads and how easily it infects new targets

2. Trigger Mechanisms

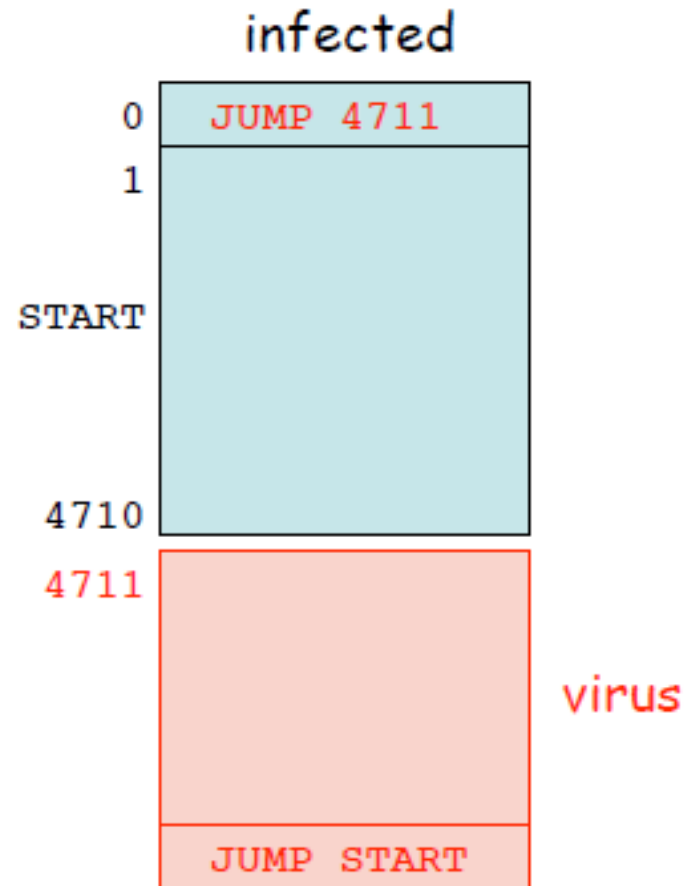
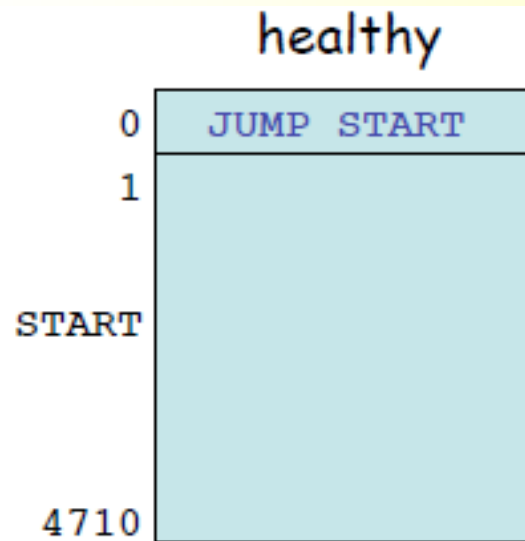
- Date
- Number of infections
- First use

3. Effects (or Payload): It can be anything

- In general, once a virus is on a system, it can do anything that any legitimate program can do
 - Displaying a message
 - Deleting files
 - Formatting the hard disk
 - Overloading the processor/memory
 - Changing system settings
 - etc.

- Method: design of a virus
 - **Detection module**: detects programs that are already infected
 - **Infection module**: copies the virus code into non-infected programs
 - **Damage module**: contains the malware proper
 - **Conditions module**: makes the actions mentioned dependent on certain condition
 - **Camouflage module**: tries to avoid detection by anti-virus software
 - Very crude example (encounter around 1989 where we didn't have access to antivirus programs)
 - `debug "infected program"`
 - The virus removes itself
 - Nowadays camouflaging by viruses is highly sophisticated

- Typical binary code layout (simplified)



■ Who Writes Viruses

- It is believed that most virus authors are young men in their teens or early twenties who have a great deal of technical knowledge and have decided for various reasons to use it for destructive purposes
- People who just want to **test the system**; they are delighted in finding a way to insert their code into places where others might not find it
- To “**punish**” users for some perceived breach; for example, to punish users of illegal copies of software (software pirates)
- **Troublemakers** - or may be just troubled individuals - who want to create havoc
- **Revenge**: Sometimes viruses, trojan horses or logic bombs are written by disgruntled employees or others who want to get back at someone

- **As a Challenge:** Some virus writers do it just to see if they can go away with it; as virus detection software gets smarter, virus writers have to employ new tricks to have their "products" evade notice
- **Education:** Writing viruses, especially ones smart enough to avoid detection, requires a great deal of technical know-how; some people take up virus writing to teach themselves how to program at a low-level within the PC; it is ironic, but experienced virus writers are among the most technically skilled programmers in the world
- etc.
- Many viruses specifically target antivirus software programs
- Hence, antivirus programs modify themselves to protect against such attacks
- As some say it, it is a digital war zone and our hard disk is the battleground

- Anti-Virus
 - There are
 - Generic solutions: e.g., Integrity checking
 - Virus specific solutions: e.g., Looking for known viruses
 - Three categories
 - Scanners: to look for a signature (or pattern) that matches a known virus
 - Activity monitors: If the program behaves in a way consistent with virus activity
 - Change detection software
 - Functions of anti-viruses
 - Identification of known viruses
 - Detection of suspected viruses
 - Blocking of possible viruses
 - Disinfection of infected objects
 - Deletion and overwriting of infected objects

- **Tips for Avoiding Viruses and Spyware**
 - Use a virus scanner such as McAfee, Norton, Kaspersky, AVG, etc.
 - If you are not sure about an e-mail attachment, do not open it
 - Do not believe “security alerts” that are sent to you. For instance, Microsoft does not send out alerts in this manner
 - Check antivirus websites regularly; You can read more about any virus, past or current, at the following websites:
 - www.f-secure.com/virus-info/virus-news/
 - www.cert.org/nav/index_red.html
 - <http://securityresponse.symantec.com/>
 - <http://vil.nai.com/vil/>

2.3 Internet Fraud

- Reasons for the popularity of Internet fraud
 - Committing an Internet fraud does not require the technical expertise that hacking and virus creation require
 - There are a great number of people engaging in various forms of online commerce, and this large amount of business creates a great many opportunities for fraud
- Scam
 - Sending out an email that suggests that you can make an outrageous sum of money with a very minimal investment (e.g., the Nigerian fraud)
- Identity theft
 - For one person to take on the identity of another
 - Usually attempted to make purchases
 - But identity theft can be done for other reasons, such as obtaining credit cards in the victim's name, or even driver's licenses, e-payment frauds, etc.

■ Phishing

- One of the more common ways to accomplish identity theft
- It is the process of trying to induce the target to provide you with personal information
- e.g., the attacker sends out an email claiming to be from a bank, and telling recipients that there is a problem with their bank account. The email then directs them to click on a link to the bank website where they can login and verify their account. However, the link really goes to a fake website set up by the attacker. When the target goes to that website and enters his information, he will have just given his username and password to the attacker
- Read about the following: **Investment Advice**, **Auction Frauds** (**Shill Bidding**, **Bid Shielding**, **Bid Siphoning**), **Cyber Stalking**

- Assignment

- Read about DES (Data Encryption Standard) and understand the algorithm so that our next classes become smooth

- The best source of information is

William Stallings, Cryptography and Network Security Principles and Practice, Prentice Hall, 5th edition, 2011.
Pages 77-85