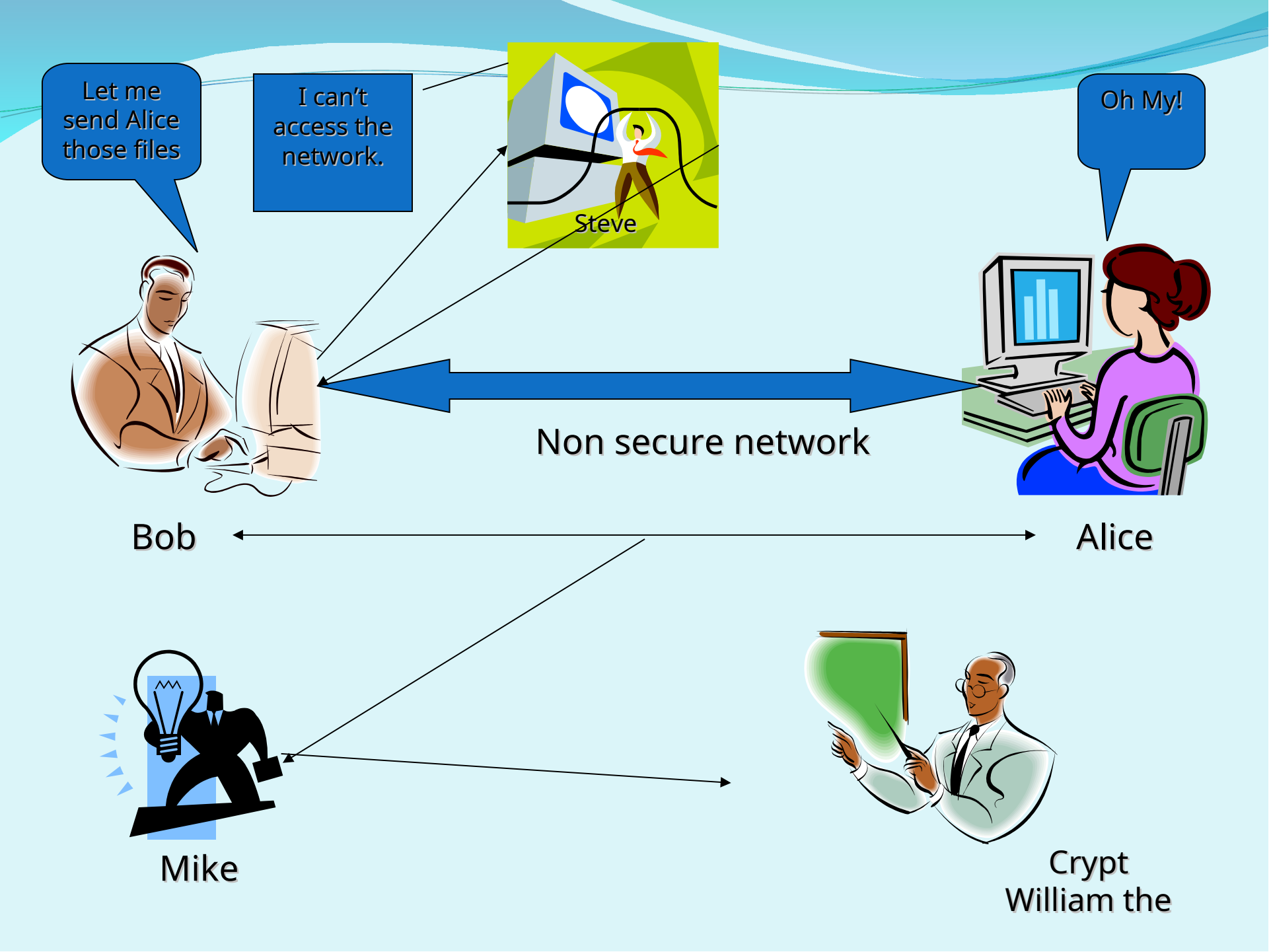
Chapter - 1

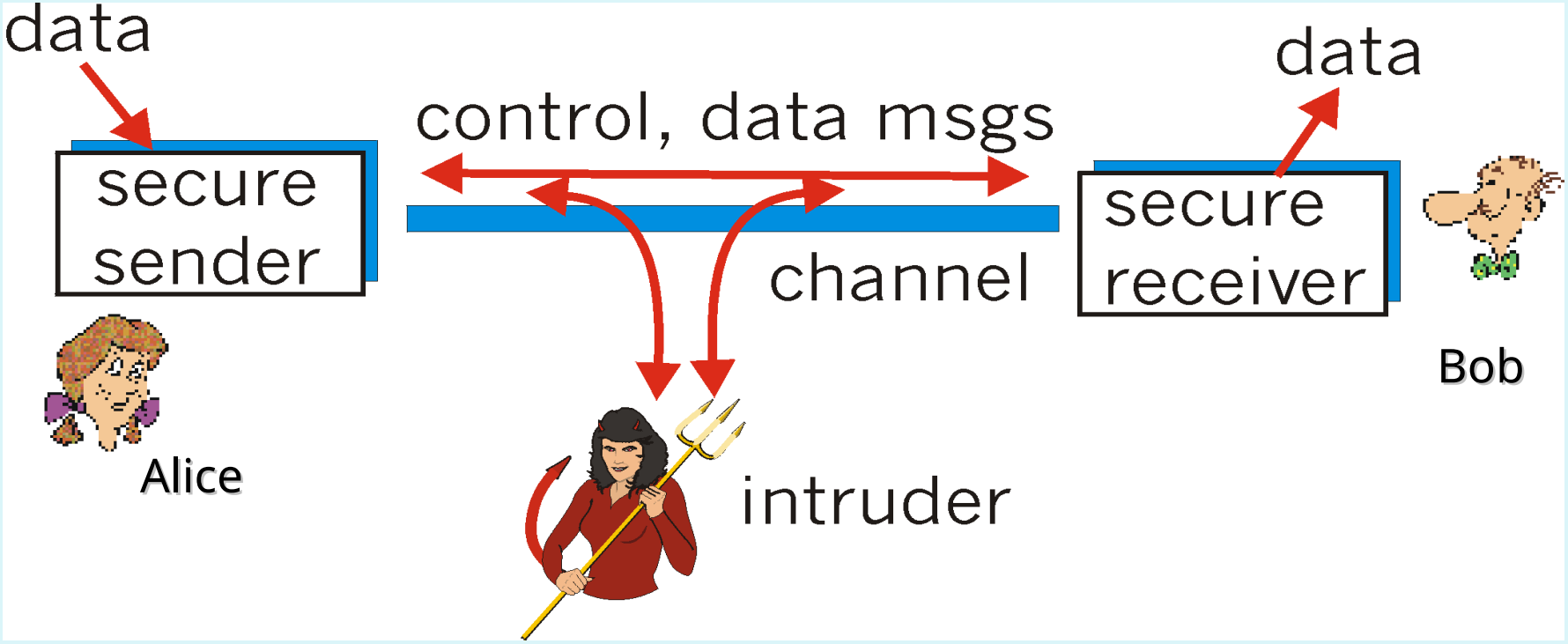
An Overview of Network Security

Outline

- Network Security concept
- Importance of Computer Security
- Security Attacks and level of practical attacks
- Attacker profiles
- Security Services and its importance
- Security Mechanisms
- Basic Model for Network Security


Let me send Alice those files
I can't access the network.
Steve
Oh My!
Non secure network
Bob
Alice
Mike
Crypt
William the

The Problem


data
secure sender
control, data msgs
channel
data
secure receiver
Alice
intruder
Bob

1.1 Network Security Concept

- If you know your enemies and know yourself, you will win hundred times in hundred battles. If you know yourself but not your enemies, you will suffer a defeat for every victory won. If you do not know yourself or your enemies, you will always lose.

  Sun Tzu, "The Art of War“

- The art of war teaches us not on the likelihood of the enemy’s not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

  The art of War, Sun Tzu

Cont…

- Computer system security consists of measures to deter, prevent, detect, and correct security violations in information system.
- Information Systems are decomposed in three main portions, *hardware, software and communications*.
- Information Security requirements have changed in recent times
  - traditionally provided by physical (locking) and administrative mechanisms (Personal screening during hiring).
- Computer use requires automated tools to protect files and other stored information b/c of introduction of distributed systems and use of networks and communications facilities for carrying data between terminal user and computer.

Cont...

The Various Computer System Securities:-

- ***Data security:-***
  - Means of ensuring that data is kept safe from corruption and that access to it is suitably controlled.
- ***Computer Security:-***
  - *Deals with* protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users.
  - Generic name for the collection of tools designed to protect data and to thwart hackers.

Cont…

- Malware: malicious software which includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware.

- ***Network Security:***
  - *M*easures to protect data during their transmission.
  - Providing protection at the boundaries of an organization
  - Starts from authenticating any user, most likely a username and a password
- ***Internet Security:***
  - Measures to protect data during their transmission over collection of interconnected networks

Why Computer Security?

- To give people the freedom to enjoy computer and computer networks without fear of compromising their rights and interests.
  - Enabling people to carry out their jobs, education/research
  - Supporting critical business process
  - Protecting personal and sensitive information
- Computer security is therefore needs to guard computer system and networked systems as well as protect electronic data that is either stored on computers or transmitted over the networks.
- This means that everyone who uses a computer or mobile device needs to understand how to keep their computer, device and data secure.
  - Information Technology Security is **everyone's** responsibility!

Cont . . .

- ***Computer Security System:***
  - The protection afforded to an automated information system/data in order to attain the applicable objectives of preserving the *integrity, availability, and confidentiality* of information system resources (includes hardware, software, firmware, information/ data, and telecommunications).
- Therefore this course enables you
  - *To Learn* ***"good computing security practices."***
  - *To Incorporate these practices into your everyday routine. Encourage others to do so as well.*
  - *To Report anything unusual to your supervisor and ITS Support Center if you become aware of a suspected security incident*

Consequences

- The consequences of ignoring computer security includes the following
  - *Loss Of Confidential Data*
  - *Loss In Productivity*
  - *Identity Theft*
  - *Compromised Data Integrity*
  - *Unavailability Of Access To Data Or Computer Network*
  - *Lawsuits & Judicial Actions*
  - *Termination Of Employment*

1.2 Security Threats and Attacks

What is Computer security Threats?

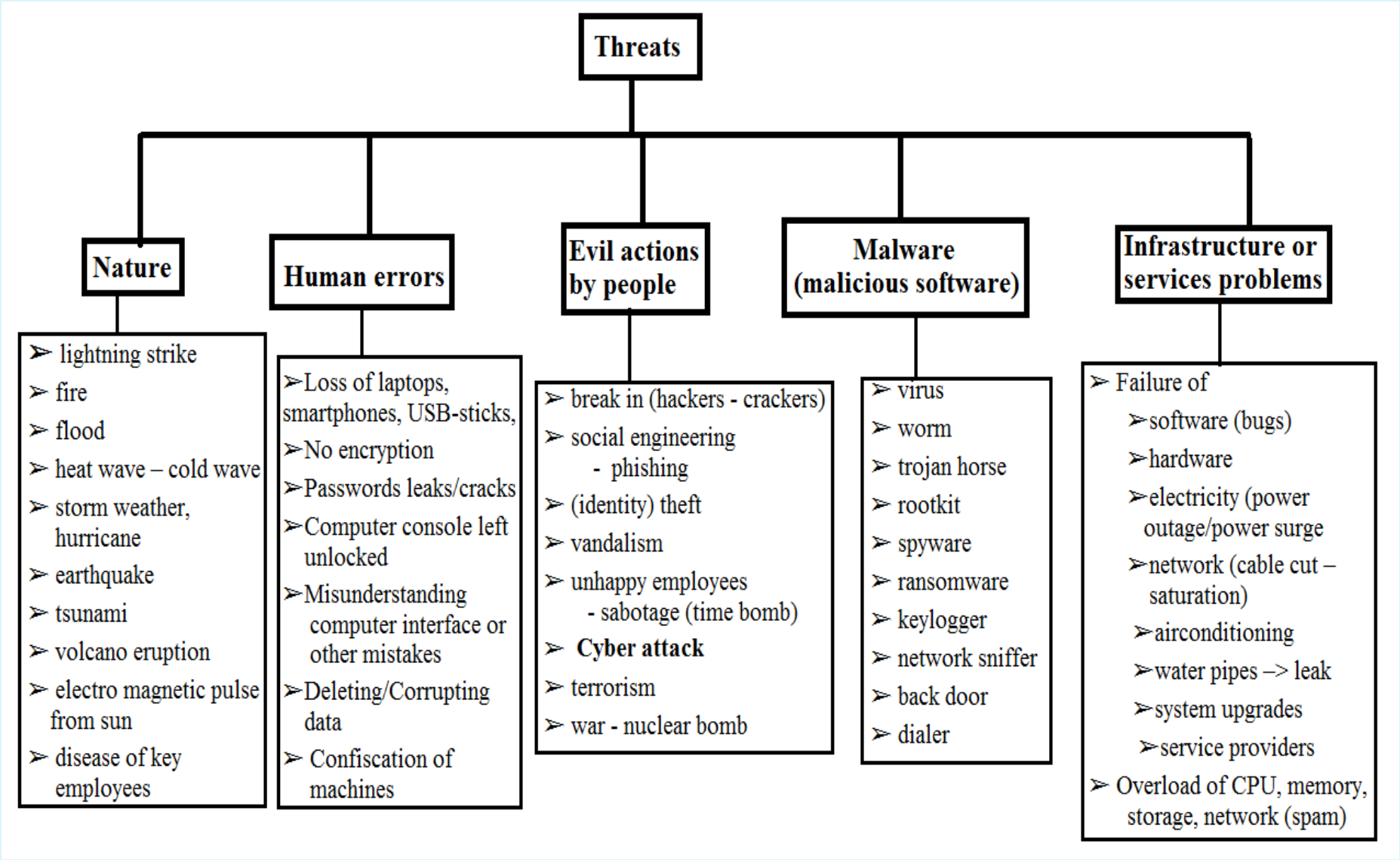
- A threat is a possible danger that might exploit a vulnerability to breach security and thus cause possible harm.
- A threat can be either
  - ***"intentional"*** (i.e., intelligent; e.g., an individual cracker or a criminal organization) or
  - ***"accidental"*** (e.g., the possibility of a computer malfunctioning, or the possibility of a natural disaster such as an earthquake, a fire, or a tornado) or
  - otherwise a circumstance, capability, action, or event

History of computer security threats

- **1986 The first virus for PCs -** The first virus for IBM PCs, Brain, was written by two brothers in Pakistan, when they noticed that people were copying their software. The virus put a copy of itself and a copyright message on any floppy disk copies their customers made.
- **1971 The first worm -** Bob Thomas, a developer working on ARPANET, a precursor to the Internet, wrote a program called Creeper that passed from computer to computer, displaying a message.
- **1988 The Internet Worm -** Robert Morris, a 23-year-old student, released a worm on the US DARPA Internet. It spread to thousands of computers and, due to an error, kept re-infecting computers many times, causing them to crash.
- **1999 Email viruses -** Melissa, a virus that forwards itself by email, spread worldwide. Bubbleboy, the first virus to infect a computer when email is viewed, appeared.
- **2000 Denial-of-service attacks -** “Distributed denial-of-service” attacks by hackers put Yahoo!, eBay, Amazon and other high profile websites offline for several hours. Love Bug became the most successful email virus yet.

Categories of Computer Security Threats

What can go wrong?



Common Security Attacks

- ***Security Attacks:-*** Any action that compromises the security of information/resource owned by an organization.
- Security attacks are classified as either *passive or active*

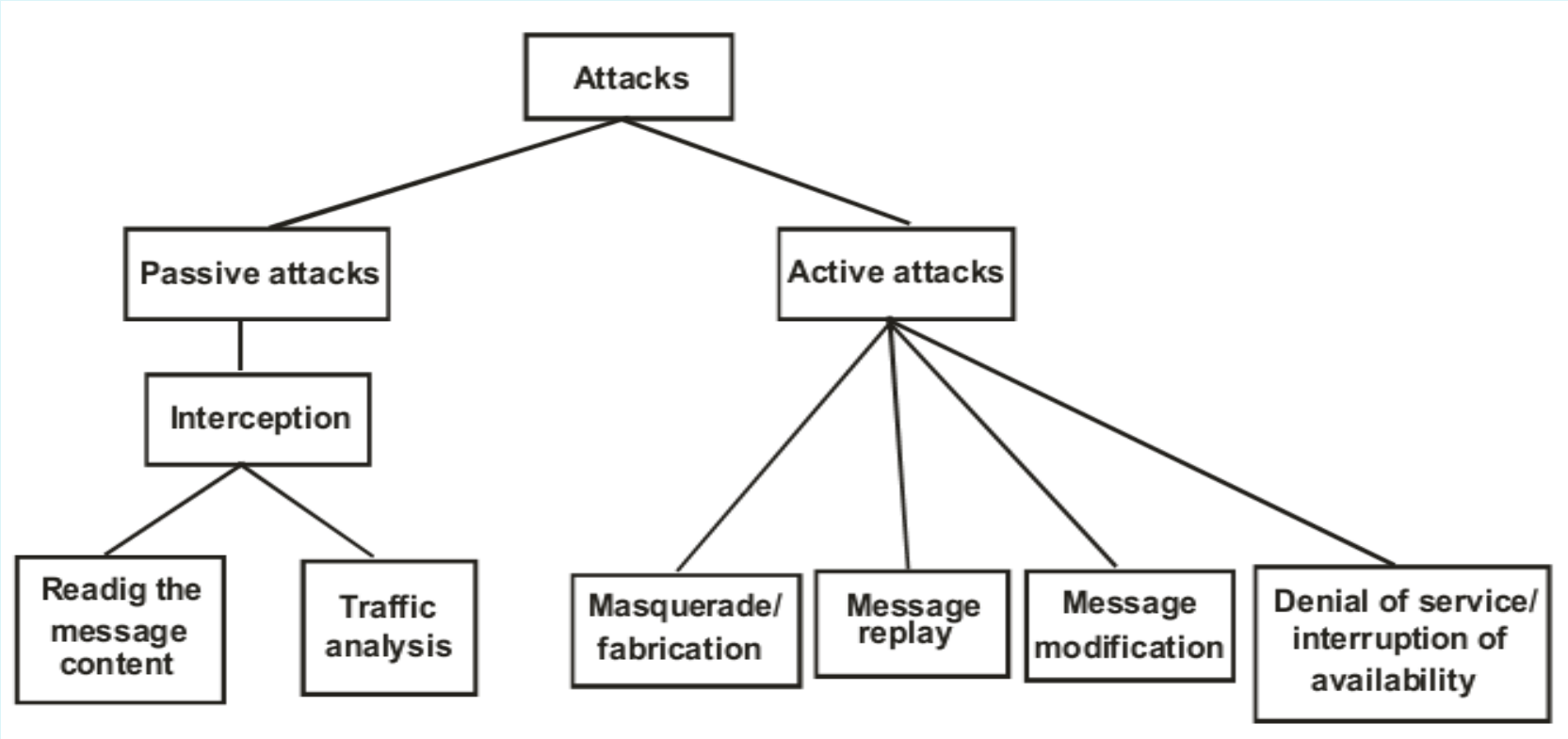


Fig 1.1 Types of Common Security Attacks

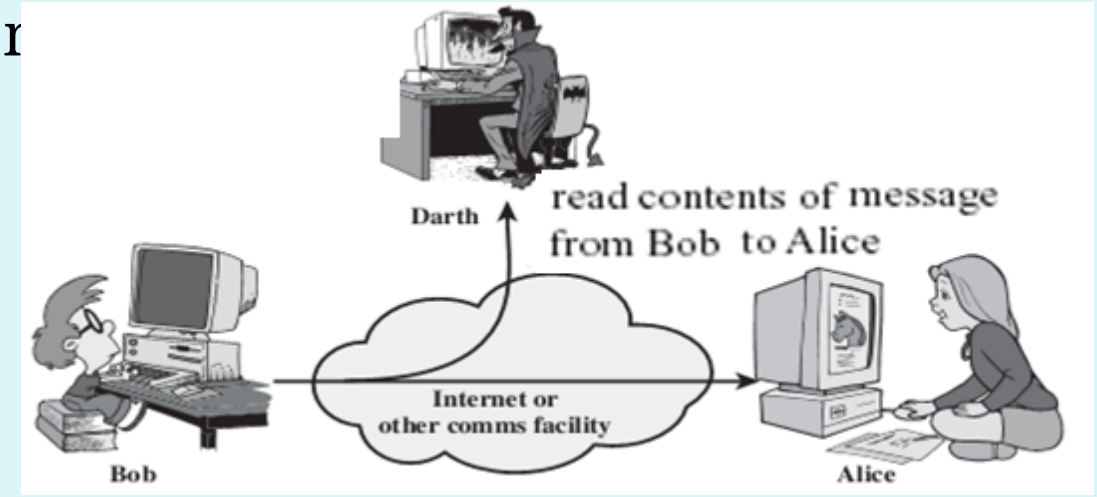
(I) Passive Attacks

- A type of attacks which do not change or modify the information flowing between the parties.
- attempts to learn or make use of information from the system but does not affect system resources.
- goal of learning as much *confidential information* as possible.
- very difficult to detect, b/c they don't involve any alteration of the data and message is sent and received in an apparently normal fashion.
- neither the sender nor receiver is aware that a third party has read msg.
- This type of attack include
  - *Eavesdropping - unauthorized reading of a message of file*
  - *Traffic analysis.*

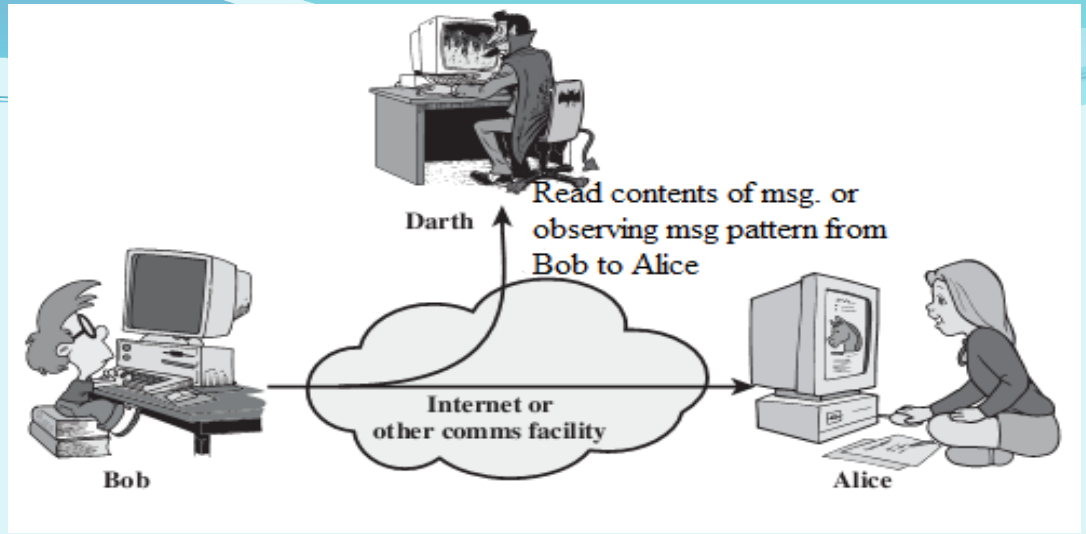
Cont…

- **Eavesdropping (**to listen secretly to what other people saying**):**
  - Also called release of message contents.
  - The unauthorized capture of transmitted data/confidential information (telephone conversation, an electronic mail message, and a transferred file) either by some form of *line tapping* or from the *compromising emanations broadcast* by the electrical signals in the line.
  - Radio, optical and r
    intercepted covertly

Example:
•Wiretapping to capture data in a network
•Illicit copying of files or programs



Cont...

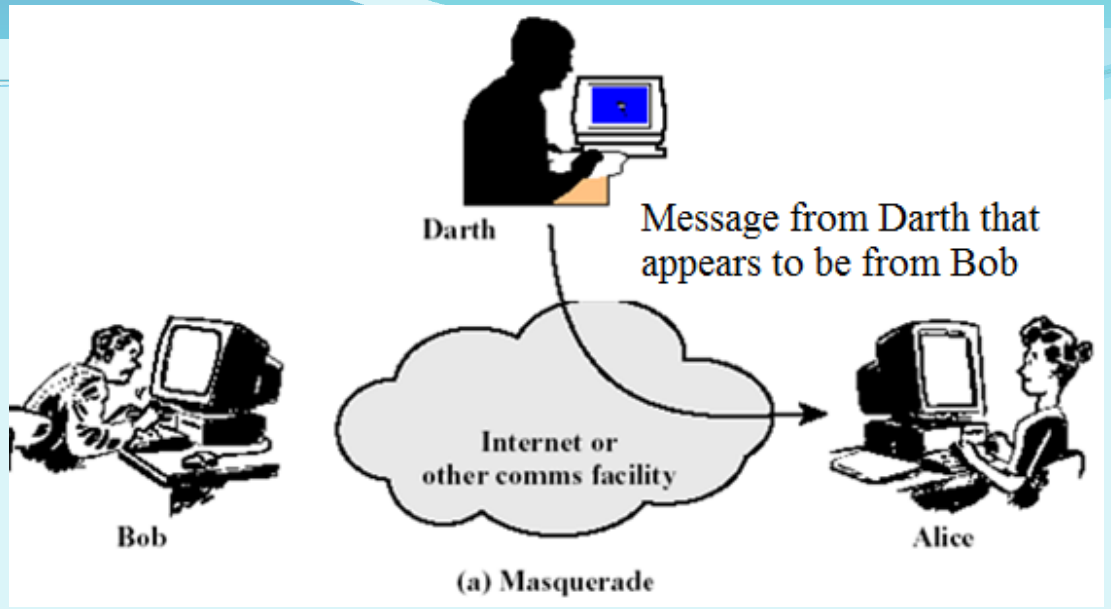


- **Traffic Analysis:**
  - The purpose of this attack is to determine who is talking to whom by analyzing IP packets/header.
  - Even if the payload of the IP packet is masked (encrypted), the attacker may still obtain useful information from analyzing IP headers.
  - be able to observe the pattern of these messages (number, size, frequency, time of message sent, length of messages being exchanged) and the opponent could determine the location and identity of communicating hosts.
  - This information might be useful in guessing the nature of the communication that was taking place.

(II) Active Attacks

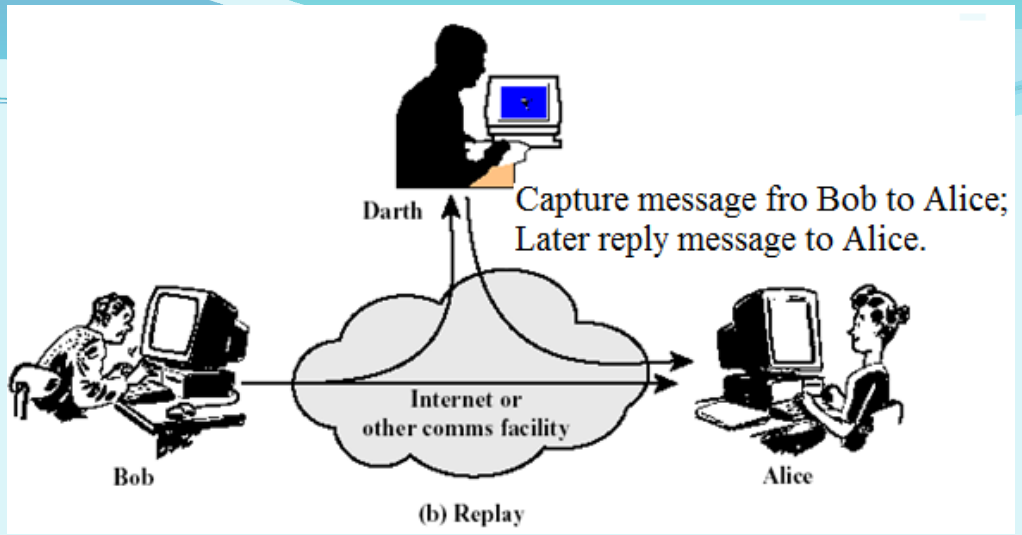
- **A** types of attacks which attempt to alter system resources or affect their operation this includes Masquerade, Message replay, Modification of messages or files, Denial of service.
- Are easier to detect since the information stream is altered and involves the other party.
- Harder to prevent since no absolute protection is available with the current buggy systems.
- Involves some modification of the data stream or creation of a false stream.
- Tries to fool the parties to believe they are talking to each other directly, while they really are talking to the attacker him-selves.

Cont...



- **Masquerade:**
  - This attack is possible by the user who will be pretending like a legitimate user and attack the system.
  - Example:- any employee is sending the message to the working staff members by taking the name of his manager. He can send the message for conducting meetings in a particular time with his employee, which is actually a forged message.
  - enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

Cont...

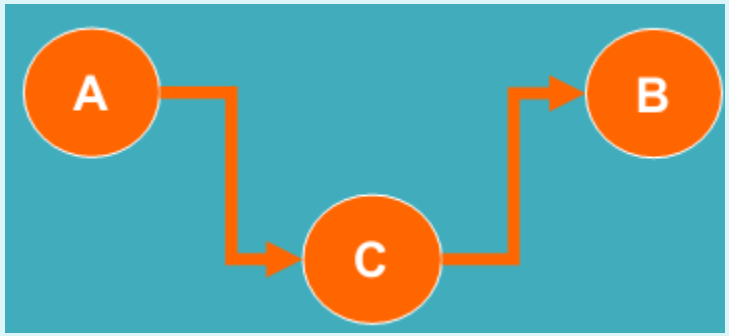


- **Message Reply**
  - Can take place by sending the same message twice.
  - Involves the passive capture of a data unit and its subsequent retransmission to produce an authorized effect.
  - Passive capture of data, alter and then retransmit.
  - Example:- User A sends a message stating that transfer B**irr**.10, 000 from Account A to Account B. This message is watched by an other user C and the same message is sent once again by user C on behalf of A. In that scenario, Birr.20, 000 will be debited from account A instead of Birr.10, 000, without his notification. This transaction will create an integrity problem.

Cont...

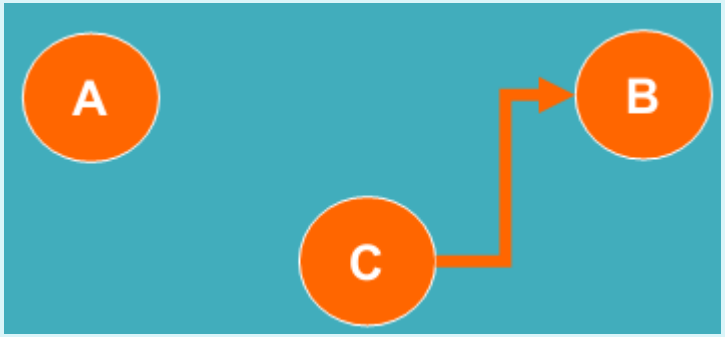
- **Modification of message**
  - An unauthorized party gains access to information and also modifies it.
  - This is an attack on integrity of information.
  - Some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect or contain different information.
  - Corrupting transmitted data or tampering with it before it reaches its destination
    - E.g., a message "Allow John to read confidential file accounts" is modified as "Allow Brown to read confidential file accounts."

- Changing values in a data file
- Altering a program so that it performs differently
- Modifying the content of



Cont...

- **Fabrication of message**
  - An unauthorized party injects fabricated information into the system.
    - That is, Faking data as if it were created by a legitimate and authentic party
  - This is an attack on authenticity.
  - Examples of this is
    - insertion of spurious messages,
    - addition of records to a file etc.



Cont…

- **Denial of service (DoS)**
  - an attempt to make a computer resource unavailable to its intended users and can be launched in many ways.
  - Such attacks often force the target computer to process a large number of useless things, hoping to consume all its critical resources.
  - Another form of service denial is the *disruption of an entire network, either by disabling the network or by overloading* it with messages so as to degrade performance
  - In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consume its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.
    - Cutting of a communication line
    - Destruction of hardware
    - Disabling file management system

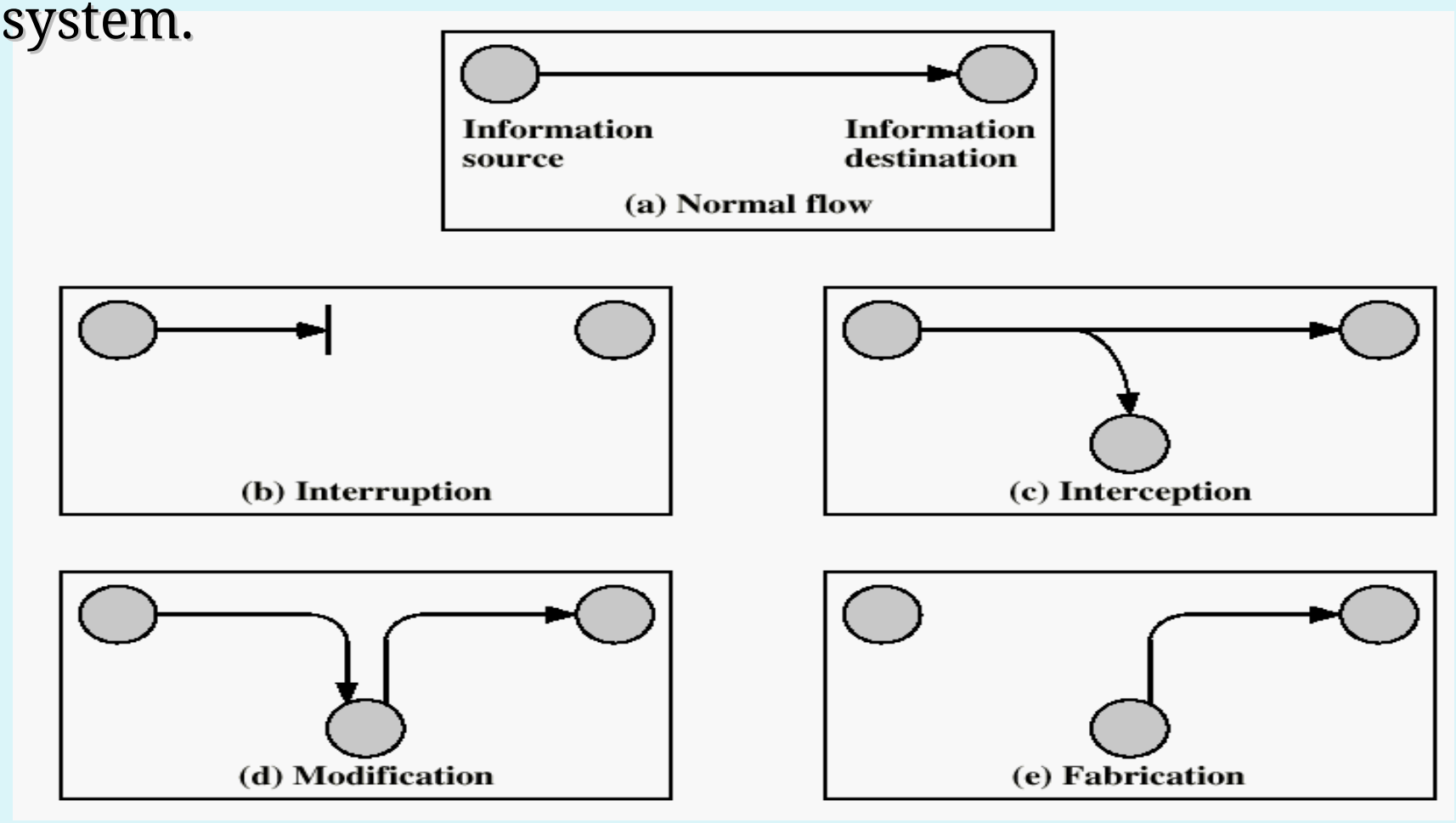
Cont...

An asset of the system becomes lost, unavailable, or unusable

- **How DoS attacks implemented**
  - Installing malicious software
  - Spam Mail
- **Various other forms of DoS attack is given below**
  - Buffer Overflow Attacks
  - SYN Attack and Smurf Attack
  - Teardrop Attack
- It is not easy to detect a DoS attack because there is nothing apparent to suggest that a user is launching a DOS attack, and is actually not a legal user of the system.
- In a DoS attack it is up to the server to detect that certain packets are from an attacker, and not from a legitimate user to take an appropriate action.

Cont...

- In general **security Attacks is** an assault on system security- an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.



Other security attacks

- Cryptanalysis
- Password Pilfering
- Identity Spoofing
  - (man-in-the-middle attacks, message replays, network spoofing, and software exploitation attacks)
- Repudiation
- Intrusion
- Malicious Software

1.3 Levels of practical side attacks

- ***Application Level Attacks***
  - happen at an application level in the sends that the attacker attempts to access, modify or prevent access to information of a particular application, or the application itself.
  - Example:- trying to obtain someone's credit card info on the Internet, or' changing contents of a msg. to change the amount in a transaction, etc.
- ***Network Level Attacks***
  - Aims at reducing capabilities of network by a number of possible means,
  - Generally make an attempt to either slow down, or completely bring to halt, a computer network.
  - automatically can lead to application level attacks, because once someone is able to gain access to a network, he/she is able to access/modify at least some sensitive information.

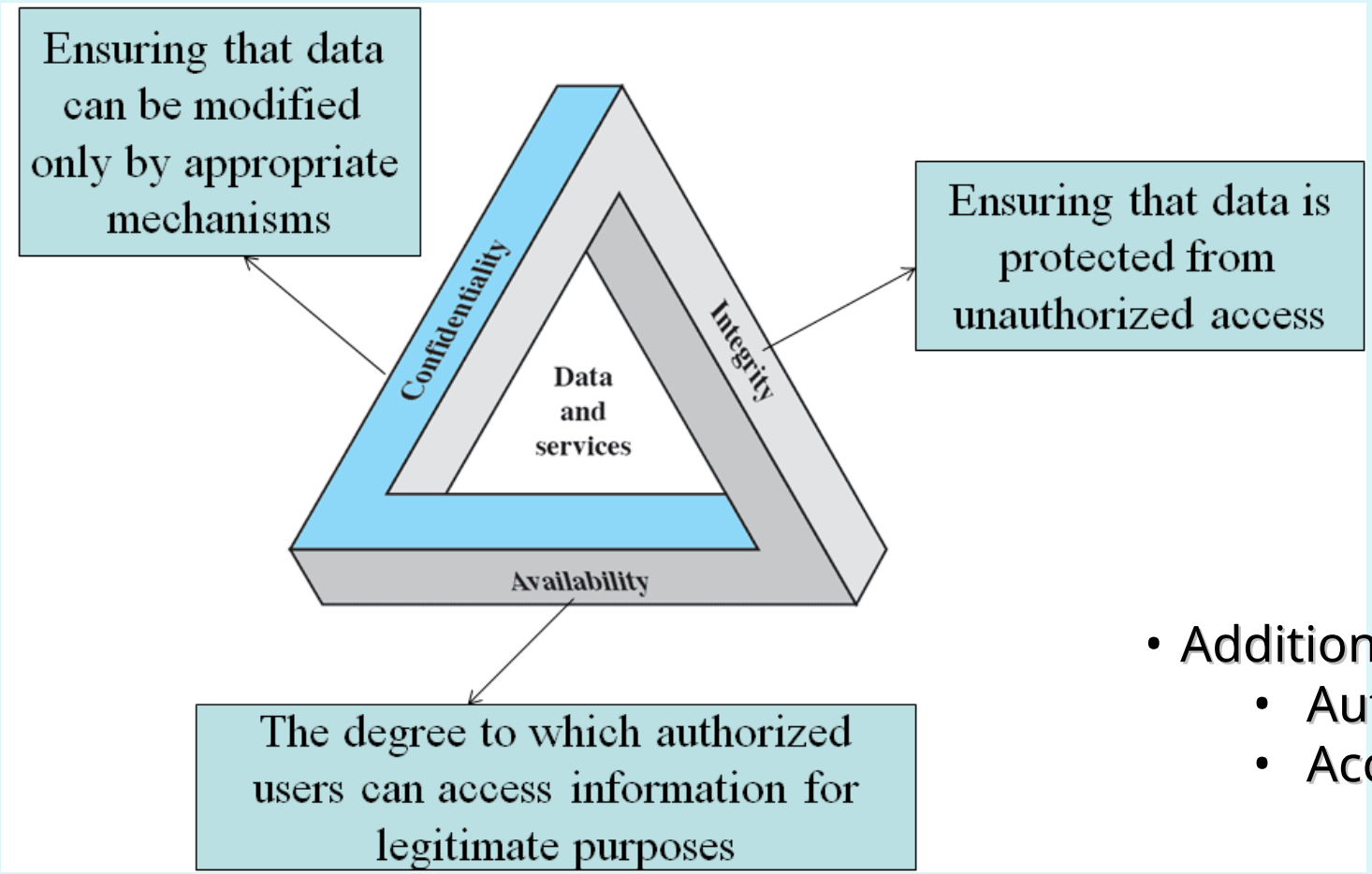
Cont...

- ***Cookies Attack***
  - A typical application is likely to involve a number of interactions between the client and the server, there must be some mechanism for the client to identify itself to the server each time it sends a HTIP request to the server.
  - For this, cookies are used.
  - A cookie is just one or more pieces of information stored as text strings in a text file on the disk of the client computer i.e. Web browser.
  - These attacks take two main forms: packet sniffing and packet spoofing
- ***Packet sniffing/IP Sniffing***
  - An attacker need not hijack a conversation, but instead, can simply observe i.e. sniff packets as they pass by
- ***Packet spoofing/IP Spoofing***.
  - Attacker sends packets with an incorrect source address. When this happens, receiver containing false source address would inadvertently send replies back.

Attacker profiles

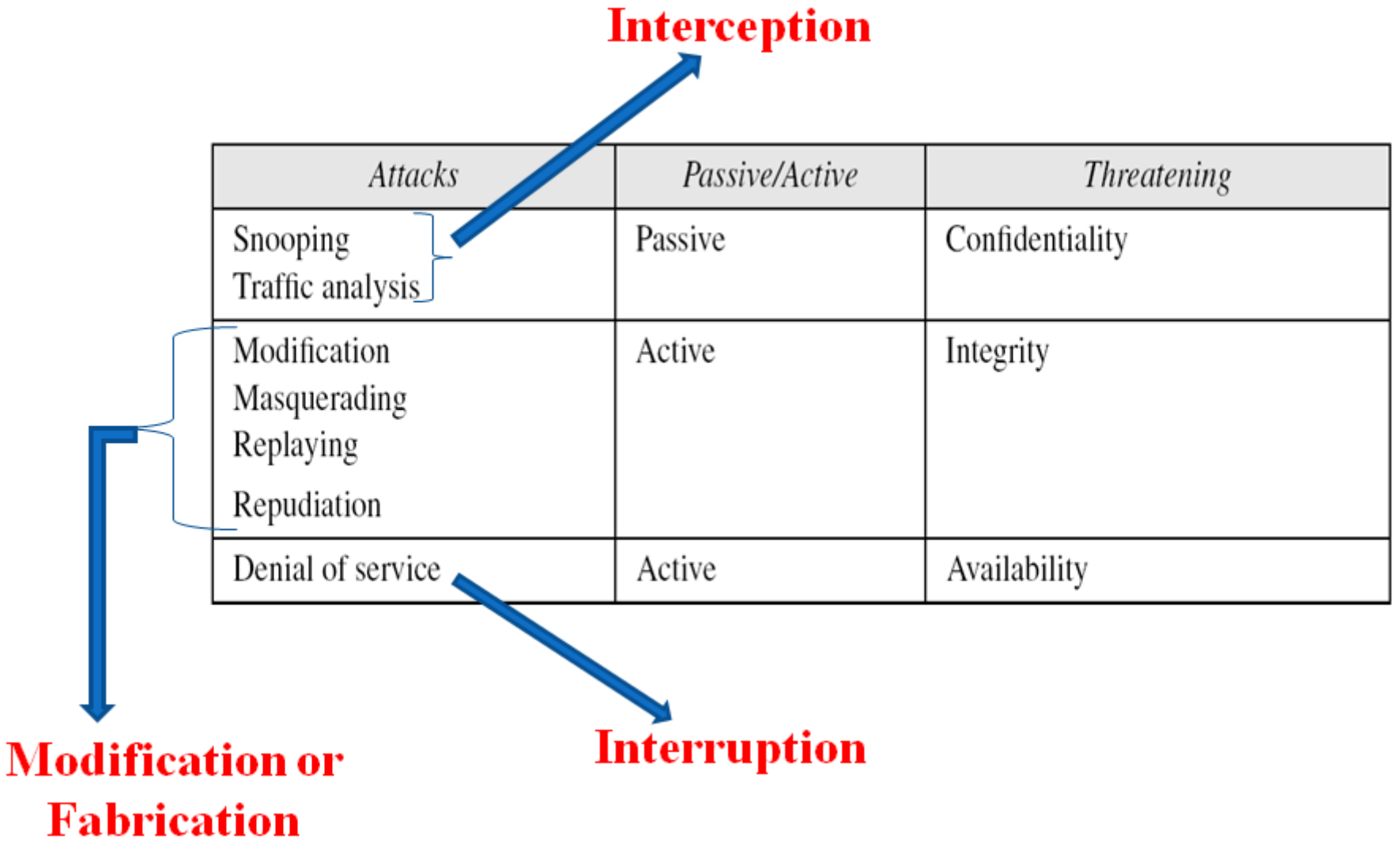
- Attackers are often characterized as
  - Hackers
    - Black-HatHackers
    - White-HatHackers
    - Grey-Hat Hackers
  - Script kiddies
  - Cyber spies
  - Vicious employees
  - Cyber terrorists
  - Hypothetical Attackers

1.4 Security Goals



- Additional Concepts
  - Authenticity
  - Accountability

Figure : CIA Triad of Information Security


Interception
Attacks
Passive/Active
Threatening
Snooping
Traffic analysis
Passive
Confidentiality
Modification
Masquerading
Replaying
Repudiation
Active
Integrity
Denial of service
Active
Availability
Modification or Fabrication
Interruption

Assets Vs. Security Goals

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

1.6 Security Service/principles

- A security service is the collection of mechanisms, procedures and other controls that are implemented to help in reducing the risk associated with threat.
  - *For example, the identification and authentication service helps reduce the risk of the unauthorized user threat.*
- Some services provide protection from threats, while other services provide for detection of the threat occurrence.
  - *An example of this would be a logging or monitoring service.*
- In general it is a processing or communication service that is provided by a system to give a specific kind of protection to system resources.
- Enhances the security of the data processing systems and the information transfers of an organization.

Cont...

- A single security services may need to be *implemented by multiple and different security mechanisms*.
- The common types of security services are shown on figure below:

(1) Data Confidentiality *(privacy of message)*

- Protection of data/information from disclosure to unauthorized entities such as organizations, people, machines and processes.
- Specially concerned with the protection of transmitted data from passive attacks and traffic flow from analysis.
- *Information includes data contents, size, existence, communication characteristics, etc.*
- *Threats can be in the area of network (dangerous b/c online business transaction) or in the area of application (can be created by insider user with full access to able and avoidable)*

confidentiality related issues

1. IP Spoofing
2. Packet sniffing
3. Alteration of message
4. Modification of message
5. Man-in-middle attacks
6. Brute force attack
7. Password cracking

Cont…

Protection Mechanisms

- Data Encryption
  - Symmetric (Secret-Key)
  - Asymmetric (Public-Key)

Service Types

- Data Confidentiality / Disclosure Protection
  - Connection Oriented - *protection of all data on connection(TCP)*
  - Connectionless - *protection all data in a single data block*
  - Selective Field - *protection of a single message or even specific fields within a message.*
- Traffic Flow Confidentiality
  - Origin Destination Association
  - Message Size and Transmission Patterns

(2) Data Integrity (has not been altered)

- Ensures that the messages are received with no duplication, insertion, modification, reordering or replays.
- Protection of data against creation, alteration, deletion, duplication, re-ordering by unauthorized entities (organizations, people, machines, processes).
- Assurance that data received is as sent by an authorized entity
- Integrity violation is always caused by active attacks.

Service Types

- Message Integrity
  - Associated with connectionless comm.
- Message Stream Integrity
  - Associated with connection oriented comm.

Protection Mechanisms

- Message Digests (Hashing)
- Sequence Numbers
- Nonce ID (Random Number)

Cont...

- ***Connection-oriented Integrity:***
  - ✓ Deals with a stream of messages or assure message delivery without alteration and Recovery of destructed or altered data
  - ✓ Addresses both message stream modification and denial of service

1. Connection Integrity with Recovery

✓ *Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.*

2. Connection Integrity without Recovery

✓ *Provides only detection and reporting without recovery and recovery done by other service or human intervention.*

3. Selective-Field Connection Integrity

✓ *Provides for the integrity of selected fields within the user data of a data block transferred over a connection*

Cont...

- ***Connectionless Integrity:***
  - ✓ Deals with individual messages and provides protection against message modification only.
  - ✓ This is because it only deals with individual packets.

1.Connectionless Integrity

- ✓ *Provides for the integrity of a single connectionless data block and may take the form of detection of data modification.*

2.Selective-Field Connectionless Integrity

- ✓ *Provides for the integrity of selected fields within a single connectionless data block.*

(3) Authentication

- Is the assurance that the communicating entity is the one that it claims to be (specially the source of the msg i.e. origin verification).
- Communicating entities are provided with assurance & information of relevant identities of communicating partners (people, machines, processes).
- Personnel Authentication requires special attention.

- In connection of a terminal to a host, two aspect is involved
  - *1st During connection initiation – two entities are authentic*
  - *2nd Services assure that the connection is not interfered by 3rd party*

Cont...

Authentication related issues

1. Stealing password
2. Fake login screen
3. Information leakage Etc.

I. Peer Entity Authentication:

- *used in association with a logical connection to provide confidence in identity of the entities.*
- *involves implementation of same protocol*

II. Data Origin Authentication:

- *In a connectionless transfer, it provides assurance that the source of received data is as claimed.*
- *Does not involve data protection against attacks*

Protection Mechanism

- Data encryption
- *Password (Manual or One-Time Password)*
- *Key Sharing (Manual, Symmetric Key or Asymmetric Key)*
- *Challenge–Response (Nonce Based or Zero Knowledge Proof)*

(4) Access Control *(Read, Write, Read/Write, Owner)*

- This service controls
  - *Who can have access to a resource,*
  - *Under what conditions access can occur and*
  - *What those accessing the resources are allowed to do.*
- *Protection of information resources or services from access or use by unauthorized entities (organizations, people, machines, processes).*
  - *Privileges – rights to access or use resources or services*
  - *Principles – entities own access control privileges*
  - *Subjects – entities exercise access control privileges*
  - *Objects / Targets – resources or services accessed/used by subjects*
  - *Delegation – transfer of access control privileges among principals*
  - *Authorization – transfer of access control privileges from principals to subjects*

Cont…

Protection Mechanisms

- Access Control Lists (ACLs)
  - Object Based Specification
    Ex.: UNIX File System
- Capabilities
  - Subject Based Specification
  - Issue Tickets/Certificates

Service Types

- Subject Based Typing
  - *Identity Based*
  - *Role Based*
- Enforcement Based Typing
  - *Mandatory Access Control — Management Directed*
  - *Discretionary Access Control — Resource Owner Directed*

(5) Non-Repudiation

- Prevents either sender or receiver from denying a service
- Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Service Types

- *Non-Repudiation of Origin*
- *Non-Repudiation of Reception*

Protection Mechanisms

- *Notarization*
- *Time Stamp*
- *Digital Signature*

(6) Availability

- Defined as keeping the right information or resources available to the right person at the right time (i.e. system resource being accessible and usable upon demand by an authorized system entity)
- Will stop the person from accessing various resources by flooding the network.
- A variety of attacks can result in the loss of or reduction in availability. *Mainly DoS attack.*
- Some attacks are amenable to automated countermeasures, such as authentication and encryption, whereas others require some sort of physical action
- Identified as issue only when the following conditions are existing.

1. **The resources are completely available up to the users expectation.**
2. **The content is present in a usable format.**
3. **The access rights are used in a proper way.**

(7) Audit

- Recording & analyses of participation, roles and actions in information communication by relevant entities.

Service Types

- Off-line Analysis (Computer Forensic)
- On-line Analysis (Real-time Intrusion Detection)

Protection Mechanisms

- Intrusion Monitors / Sensors
  - Common Intrusion Detection Framework (CIDF)
  - Common Information Model (CIM)

Summary o Security Services

- Confidentiality ------- (privacy)
- Authentication -------- (who created or sent the data)
- Integrity -------- (has not been altered)
- Non-repudiation --------- (the order is final)
- Access control --------- (prevent misuse of resources)
- Availability ---------- (permanence, non-erasure)
    - *Denial of Service Attacks*
    - *Virus that deletes files*

(II) Pervasive Security Mechanisms

- Mechanisms that are not specific to any particular OSI security service or protocol layer

- **Trusted Functionality -** *That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).*
- **Security Label -** *The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource*
- **Security Audit Trail -** *Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.*
- **Event Detection:-** *Detection of security-relevant events*.
- **Security Recovery:-** *Deals with requests from mechanisms, such as event handling and management functions, and takes recovery action*

THE END

???

Computer Security Challenges

Computer Security is both fascinating and complex:

- not simple
- must consider potential attacks
- procedures used counter-intuitive
- involve algorithms and secret information
- must decide where to deploy mechanisms
- battle of wits between attacker/administrator
- not perceived to be a benefit until fails
- requires regular monitoring
- too often an after-thought
- regarded as impediment to efficient and user friendly use of system