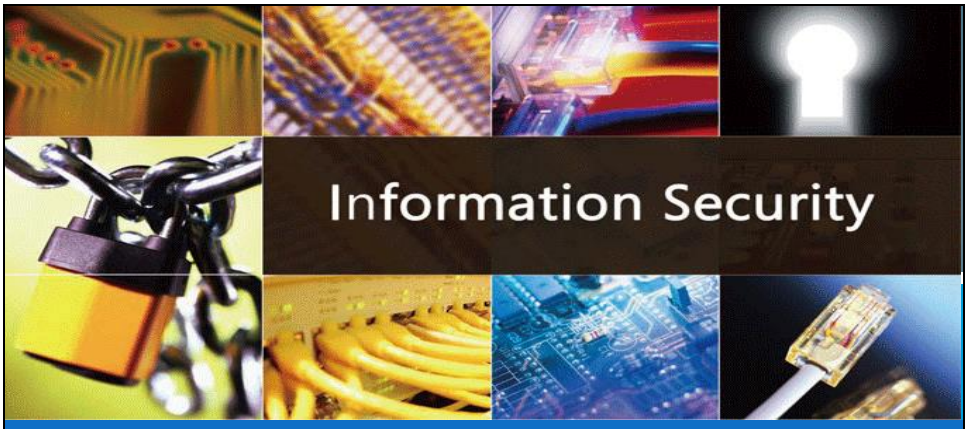


Computer Security Concepts

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

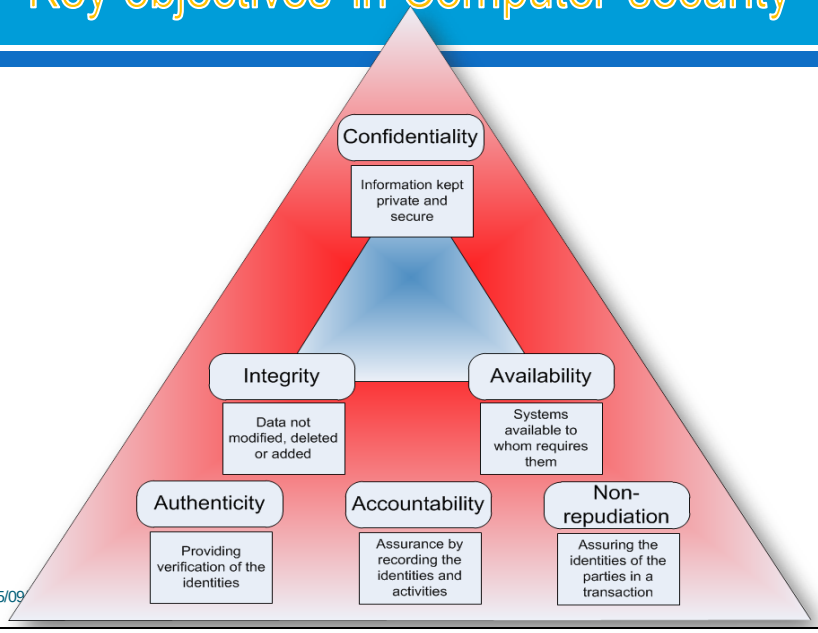
Objective

- Describe the key security requirements of confidentiality, integrity, and availability.
- Discuss the types of security threats and attacks that must be dealt with and give examples of the types of threats and attacks that apply to different categories of computer and network assets.
- Summarize the functional requirements for computer security.
- Explain the fundamental security design principles.
- Understand the principle aspects of a comprehensive security strategy.

Computer Security

- The protection afforded to an automated information system 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).

Key objectives in Computer security



Key Terms [Terminology]

- Attack - an act that is an intentional or unintentional attempt to cause damage or compromise to the information and/or the systems that support it.
- Threats - a category of objects, persons, or other entities that represents a potential danger to an asset.
- Threat Agent -a specific instance or component of a more general threat
- Vulnerability- weaknesses or faults in a system or protection mechanism that expose information to attack or damage
- Hacking - Good: to use computers or systems for enjoyment; Bad: to illegally gain access to a computer or system
- Risk - the probability that threat will exploit a vulnerability with a harmful result.
- Subject - an active entity that interacts with an information system and causes information to move through the system for a specific end purpose
- Object - a passive entity in the information system that receives or contains information

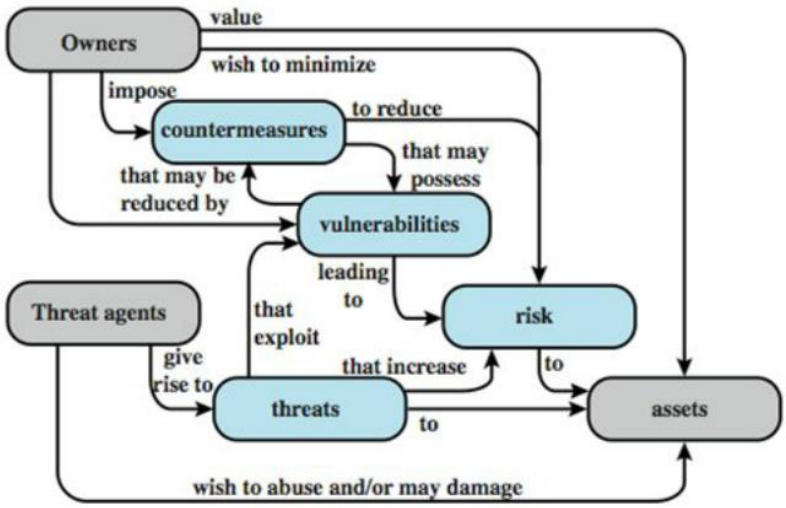
5

Key Terms [Terminology]

- Access - a subject or object's ability to use, manipulate, modify, or affect another subject or object
- Asset - the organizational resource that is being protected.
- Control, Safeguard or Countermeasure- security mechanisms, policies or procedures that can successfully counter attacks, reduce risk, resolve vulnerabilities, and otherwise improve the security within an organization
- Exploit – to take advantage of weaknesses or vulnerability in a system
- Exposure - a single instance of being open to damage.
- Security Blueprint - the plan for the implementation of new security measures in the organization
- Security Model - a collection of specific security rules that represents the implementation of a security policy
- Security Posture or Security Profile- a general label for the combination of all policy, procedures, technology, and programs that make up the total security effort currently in place

6

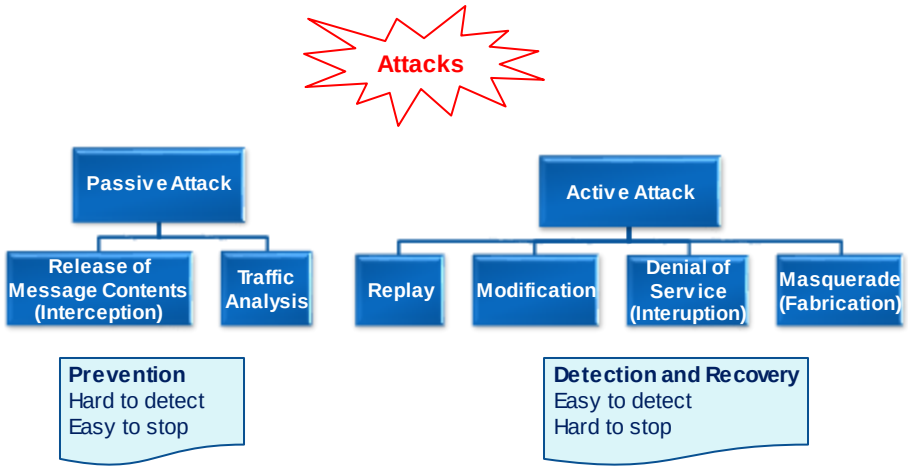
Security Concepts and Relationships



Categories of vulnerabilities & attacks

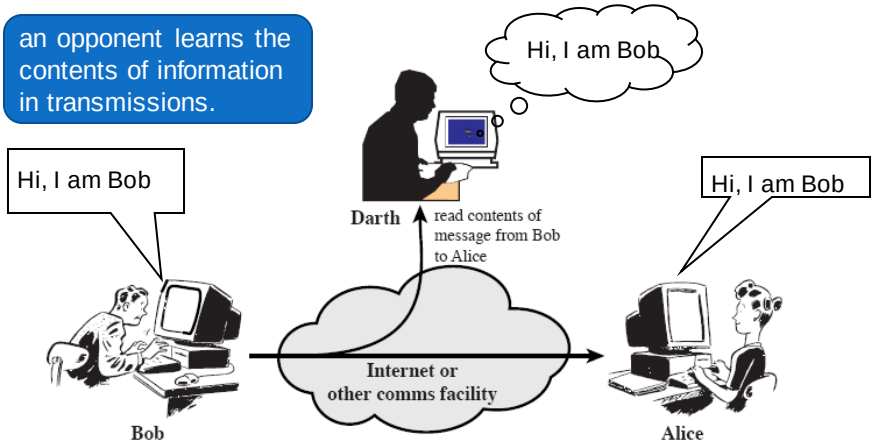
- Vulnerabilities
  - It can be **corrupted**, so that it does the wrong thing or gives wrong answers.
  - It can become **leaky**.
  - It can become **unavailable** or very slow.
- Attacks
  - **Active attack:** An attempt to alter system resources or affect their operation.
  - **Passive attack:** An attempt to learn or make use of information from the system that does not affect system resources.
  - **Inside attack:** Initiated by an entity inside the security perimeter, it is authorized to access system resources but uses them in a way not approved by those who granted the authorization.
  - **Outside attack:** Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system
- **Countermeasure**
  - Detect
  - Prevent
  - Recover

Attacks



Passive attacks: Release..

an opponent learns the contents of information in transmissions.

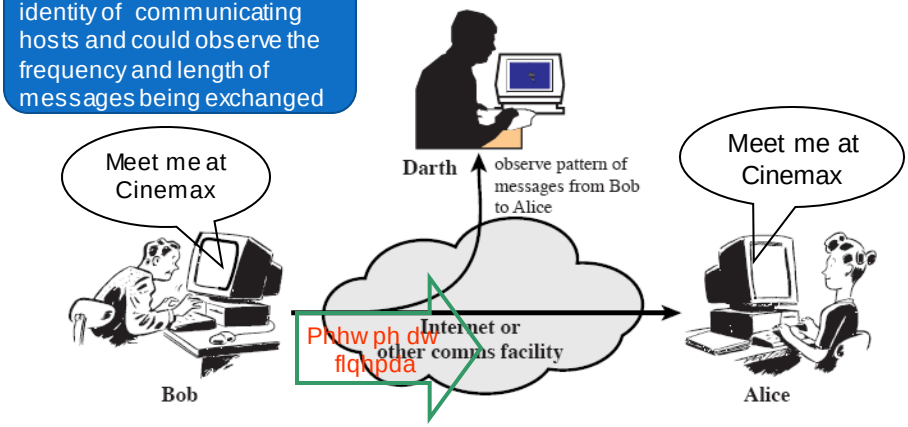


(a) Release of message contents

related goals?

Passive attacks: traffic analysis

determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged

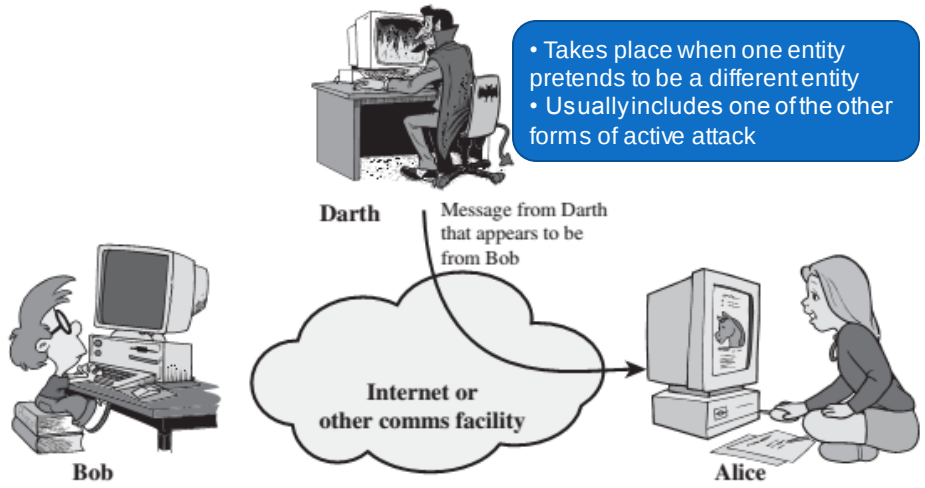


(b) Traffic analysis

related goals?

Active attacks: Masquerade

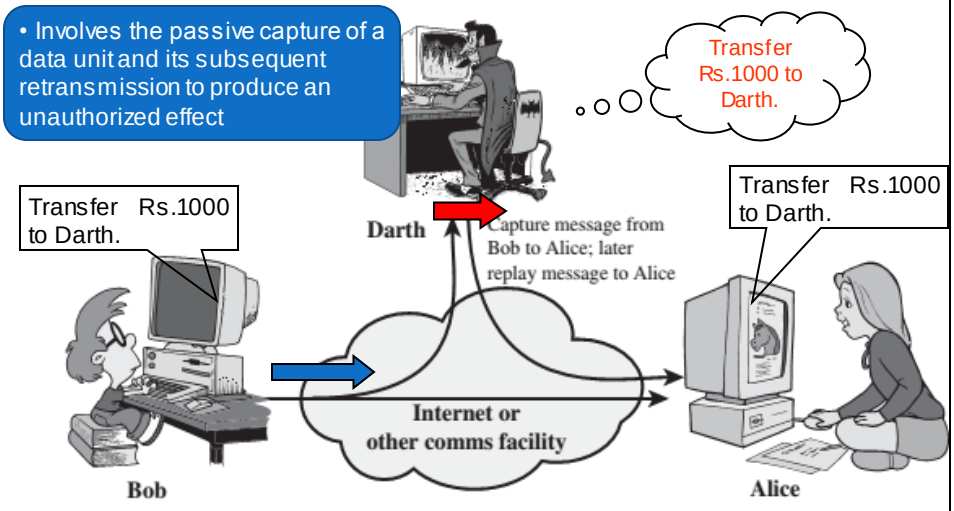
- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack



related goals?

Active attacks: Replay

• Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

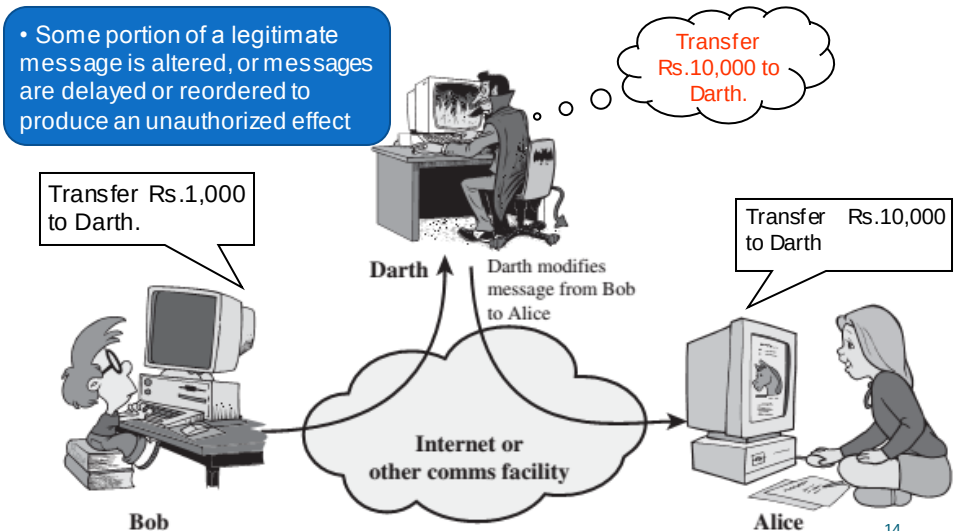


related goals?

Sign can't defense replay
A Think B send next sms

Active attacks: Modification of messages

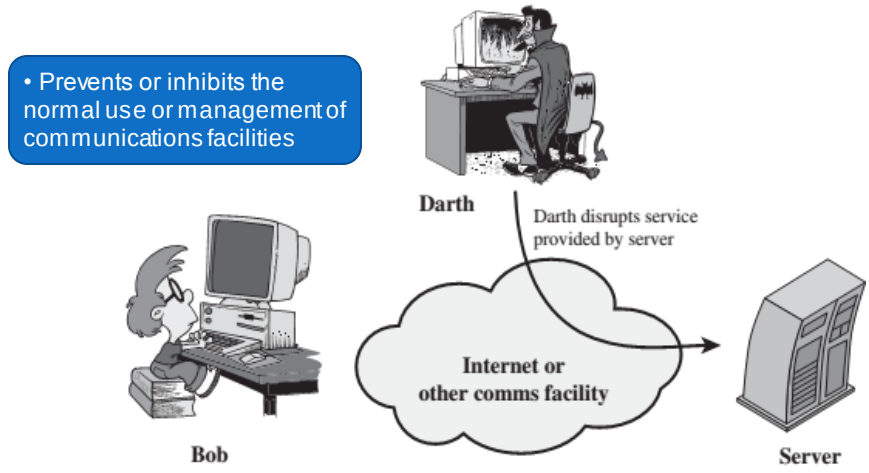
• Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect



related goals?

Active attacks: denial of service

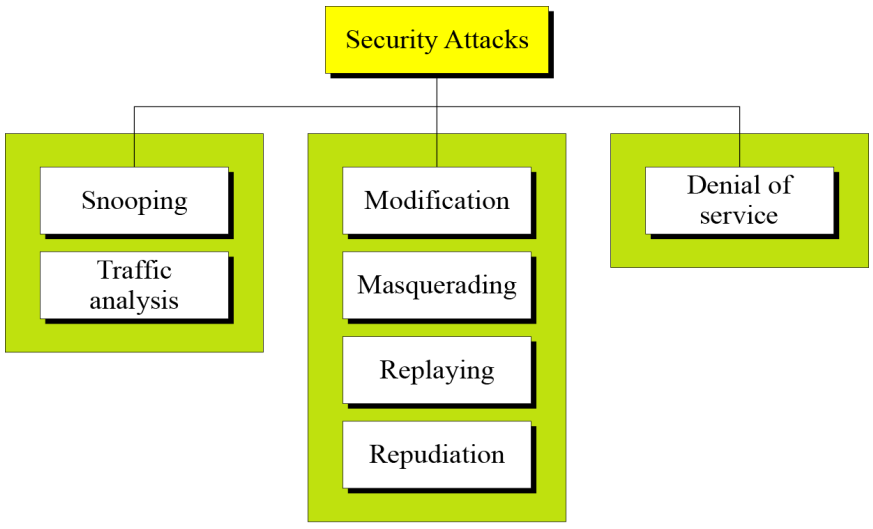
- Prevents or inhibits the normal use or management of communications facilities



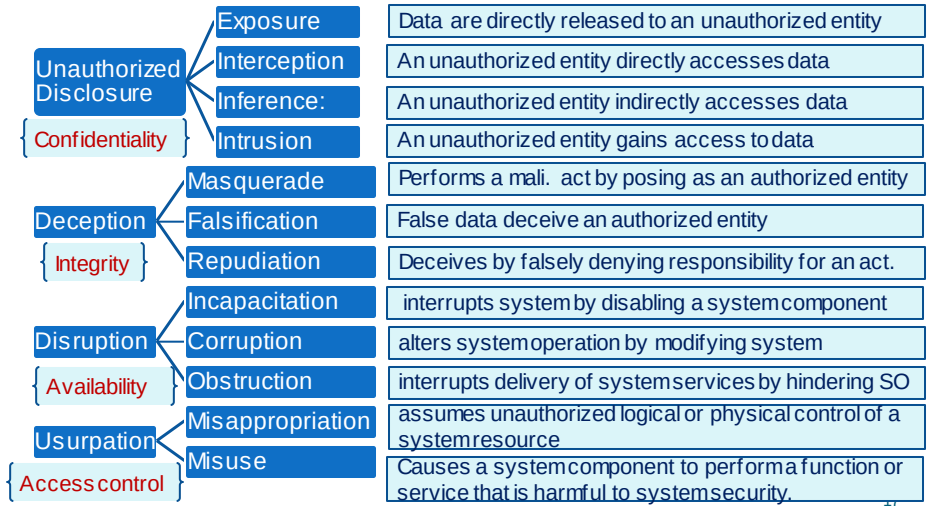
(d) Denial of service

related goals?

Taxonomy of attacks with relation to security goals



Threat and the Types of Threat actions



Threats and Assets

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
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 and Networks	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.

What should the Good Guys Do?

- **Prevention**
- **Detection**
- **Response**
- **Recovery and remediation**

Policy **(what)** vs. mechanism **(how)**

Security Requirements

the countermeasures are used to reduce vulnerabilities and deal with threats to system assets:

- **Access Control: (**authorized users)
- **Awareness and Training:** all people in organization
- **Audit and Accountability:** all information system
- **Certification, Accreditation, and Security Assessments:** (the controls)
- **Configuration Management:** (hardware, software, firmware, and documentation)
- **Contingency Planning:** ensure the availability of critical information resources.
- **Identification and Authentication: (**users, processes, or devices)
- **Incident Response**
- **Maintenance**
- **Media, Physical, Environmental, System and Communications Protection**
- **Planning**
- **Personnel Security**
- **Risk Assessment**
- **Systems and Services Acquisition**
- **System and Information Integrity**

Fundamental security design principles

- Reduce vulnerabilities by following **basic design principles for secure systems**:
  - Economy of mechanism
  - Fail-safe defaults
  - Complete mediation
  - Open design
  - Separation of privilege
  - Least privilege
  - Least common mechanism
  - Psychological acceptability
  - Isolation
  - Encapsulation
  - Modularity
  - Layering
  - Least surprise

Computer security strategy

- **Specification/policy:** What is the security scheme supposed to do?
- **Implementation/mechanisms:** How does it do it?
  - Prevention
  - Detection
  - Response
  - Recovery
- **Correctness/assurance:** Does it really work?
  - **Assurance:** a degree of confidence
  - **Evaluation:** the process of examining a computer product or system with respect to certain criteria

Summary

- The key security requirements
- Key objectives in Computer security
- The types of Vulnerabilities, threats and attacks
- Functional requirements for computer security
- Fundamental security design principles
- Computer security strategy.

Q & A