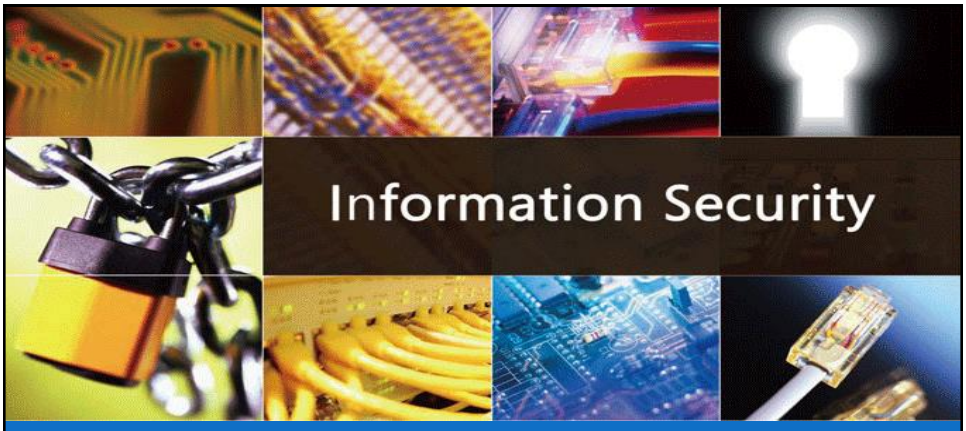


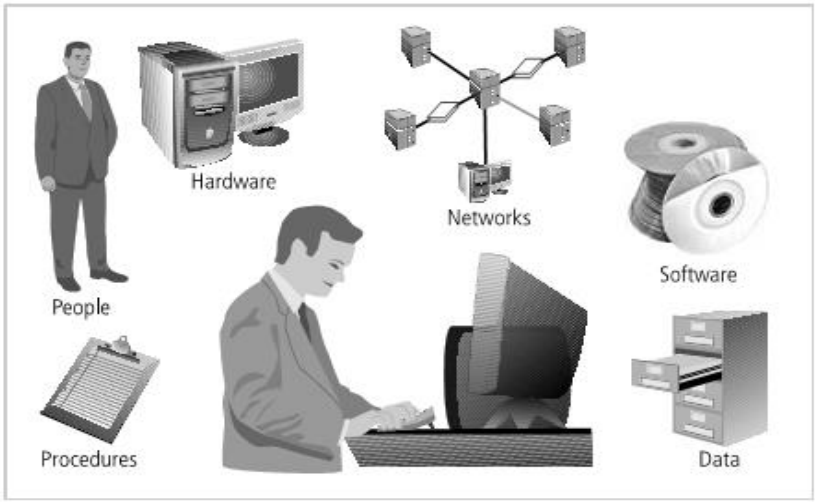

# Chapter 1: Computer Security Concepts

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

## Objective

- Describe the key security requirements of confidentiality, integrity, and availability.
- Discuss the types of security threats, vulnerability and attacks.
- Summarize the functional requirements for computer security.
- Explain the fundamental security design principles.
- Understand the principle aspects of a comprehensive security strategy.

# Components of an Information System

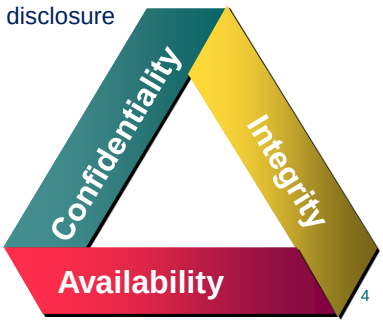




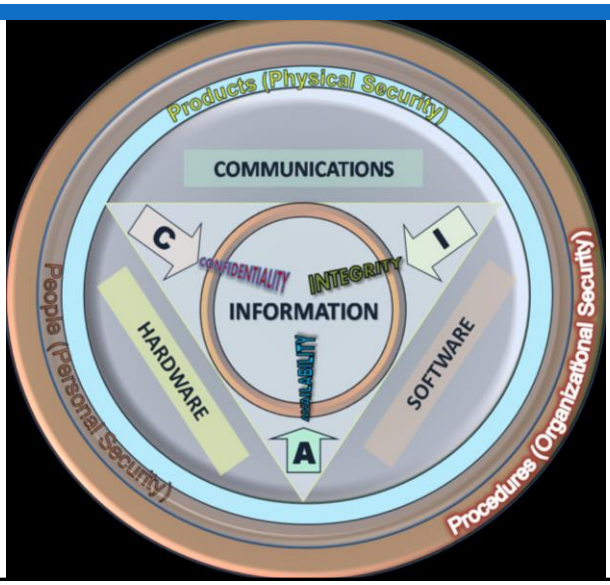

# Security concepts

- Computer Security: The protection an information system in order to attain the applicable objectives of preserving of information system resources: (CIA Triad)
  - Integrity: Prevents unauthorized modification of S&I
  - Availability: Prevents disruption of service and productivity.
  - Confidentiality: Prevents unauthorized disclosure of systems and information

(includes hardware, software, firmware, information/ data, and telecommunications)



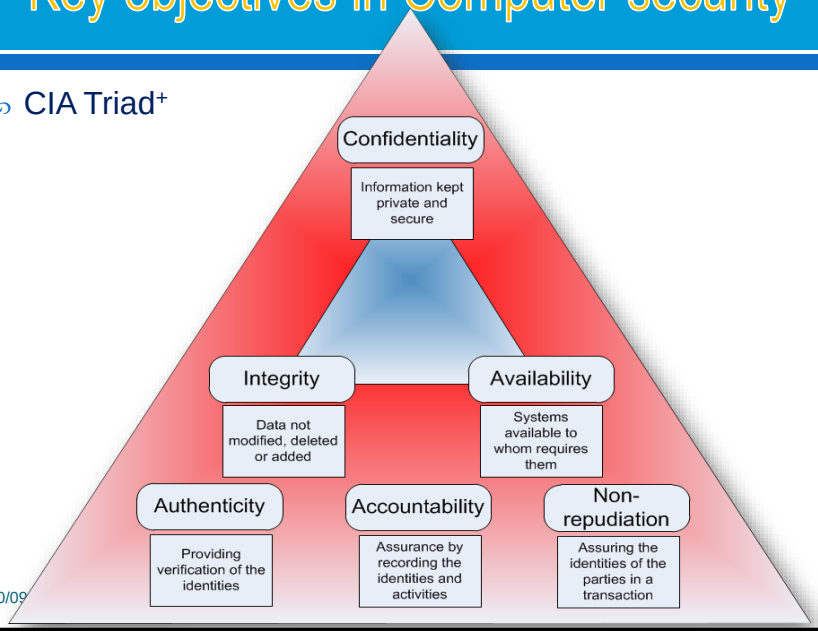
# CIA Triad And Components




5

# Key objectives in Computer security

- CIA Triad+






6

# Exercise 1

- Choose an information system
- Assume that a security model is needed for the protection of an information using CIA Triad+.
- Tips:
  - What are informations in your class
    - People, hardware, software, procedure, network, data,….
  - Need protect based on a security model CIA triad+
    - Integrity
    - Availability
    - Confidentiality
    - Authentication
    - Accountability
  - Check how every component in the class is protected



# Key Terms [Terminology]

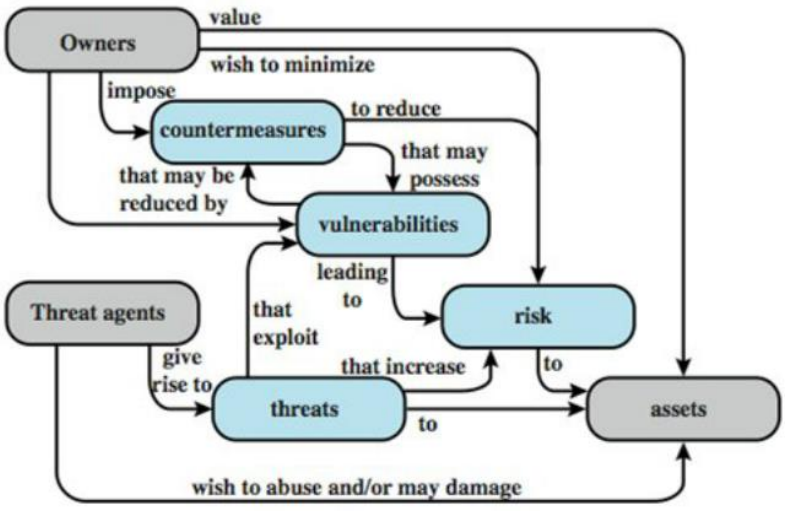
- Attack - an act that is an intentional or unintentional attempt to cause damage or compromise to the information and/or the systems that support it.
- Threats - a category of objects, persons, or other entities that represents a potential danger to an asset.
- Threat Agent -a specific instance or component 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

# 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

9

# Security Concepts and Relationships




10/09/2022

# Exercise 2

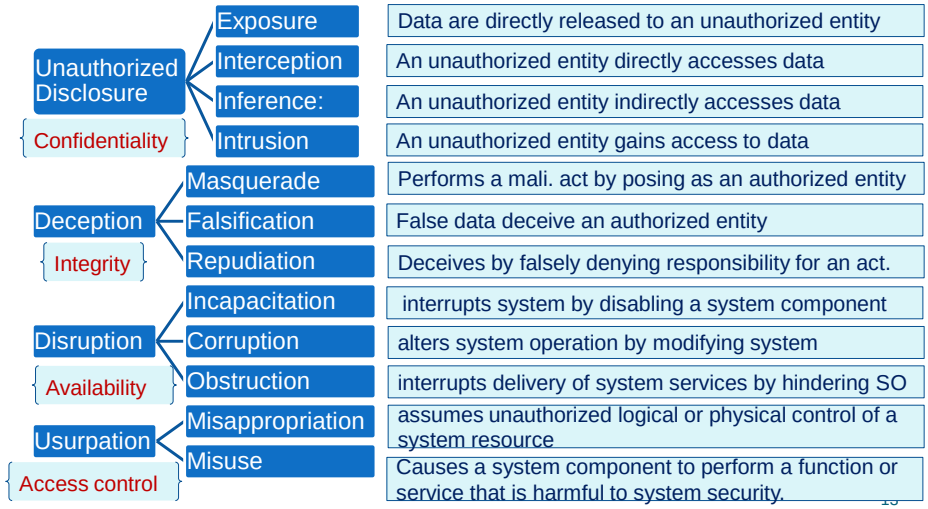
- Consider the information stored on **your personal computer**. For each of the terms listed, find an example and document it: threat, threat agent, vulnerability, exposure, risk, attack, and exploit.



# Categories of threats, vulnerabilities & attacks

- Threats
- Vulnerabilities
- Attacks

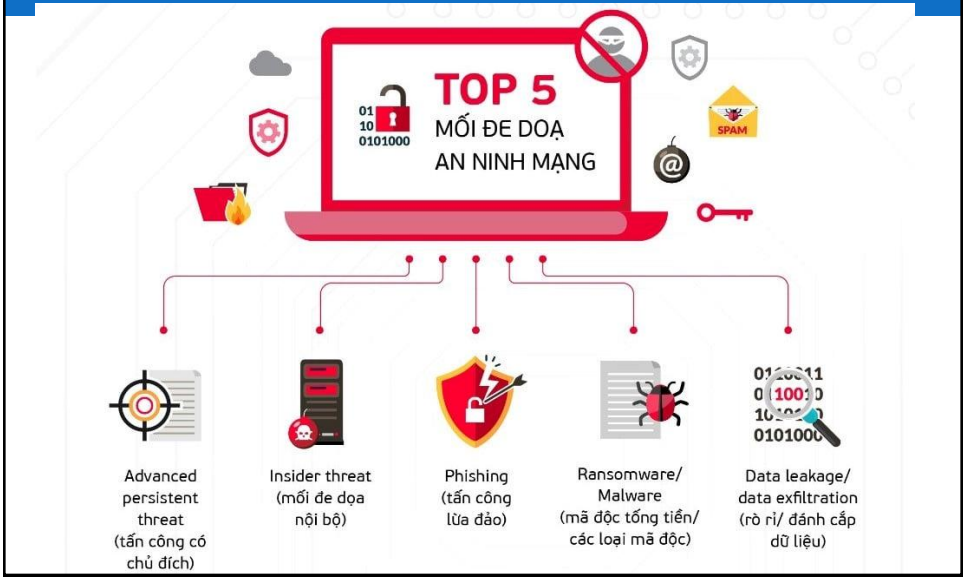
# Threat and the Types of Threat actions




# 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. |

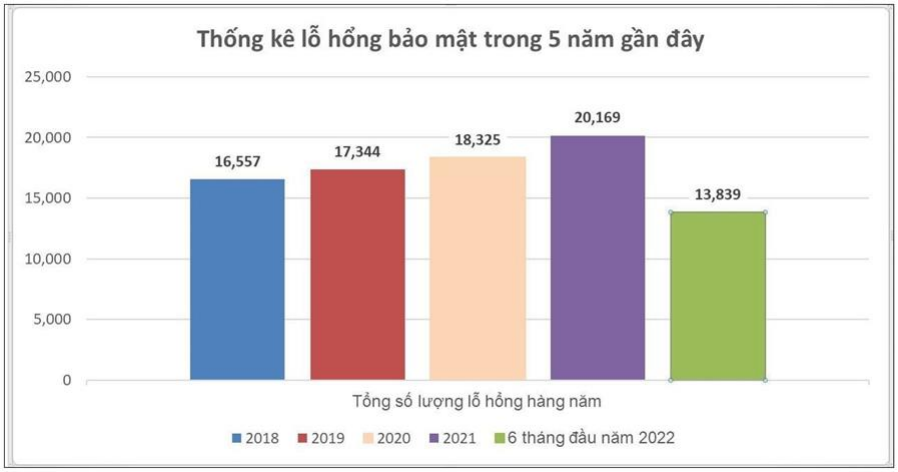
# Threats - news




# Security vulnerability

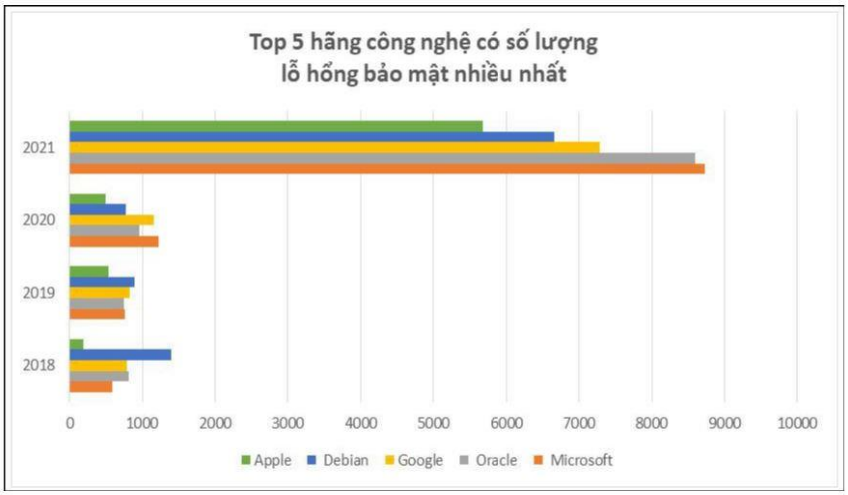
- security vulnerability: a hole or a weakness
  - can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application
- Sources:
  - weak defenses
  - Risky resource management
  - Insecure interaction between components
- Common types

# Vulnerability - news






# Vulnerability - news

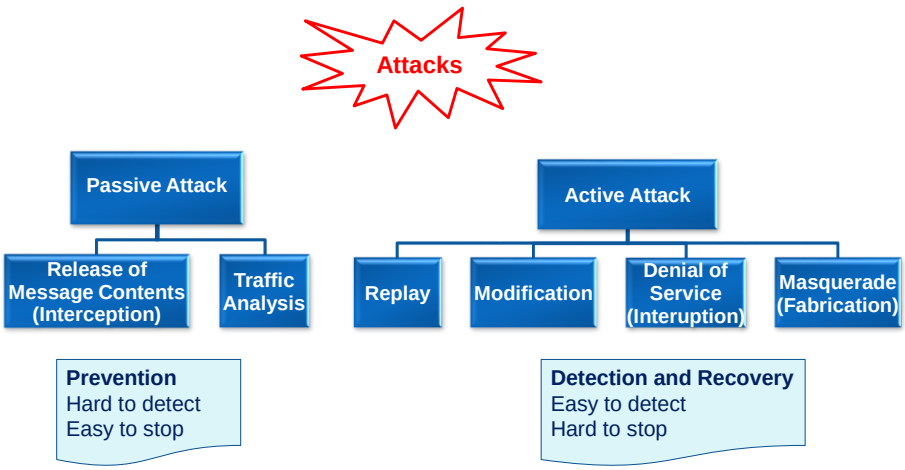


# Vulnerability Management

- Management

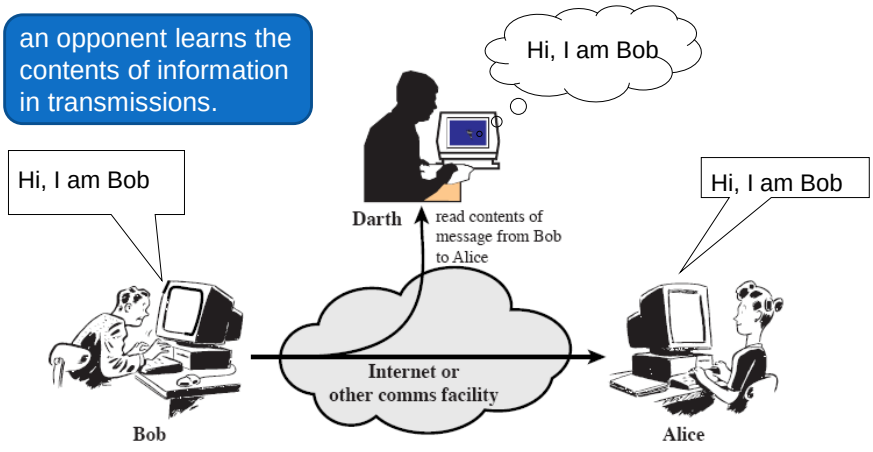



# Attacks



# Passive attacks: Release..

an opponent learns the contents of information in transmissions.



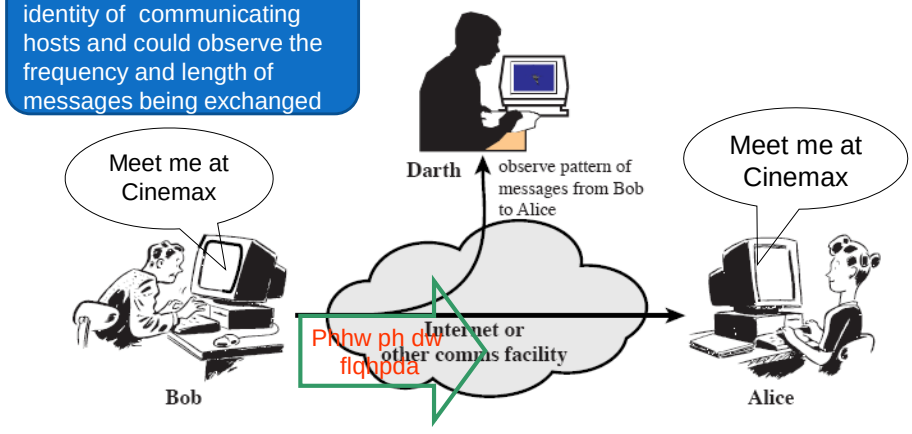

(a) Release of message contents

related goals?



# Passive attacks: traffic analysis

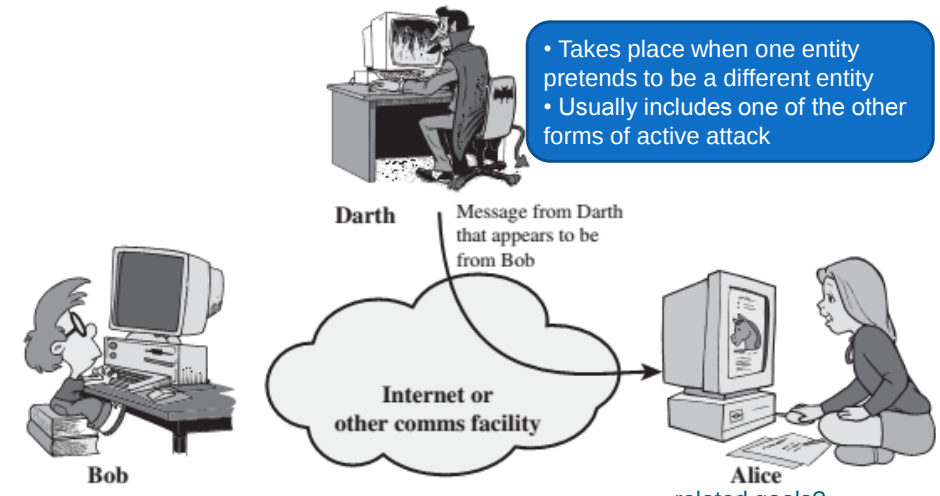
determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged




(b) Traffic analysis

related goals?

# Active attacks: Masquerade



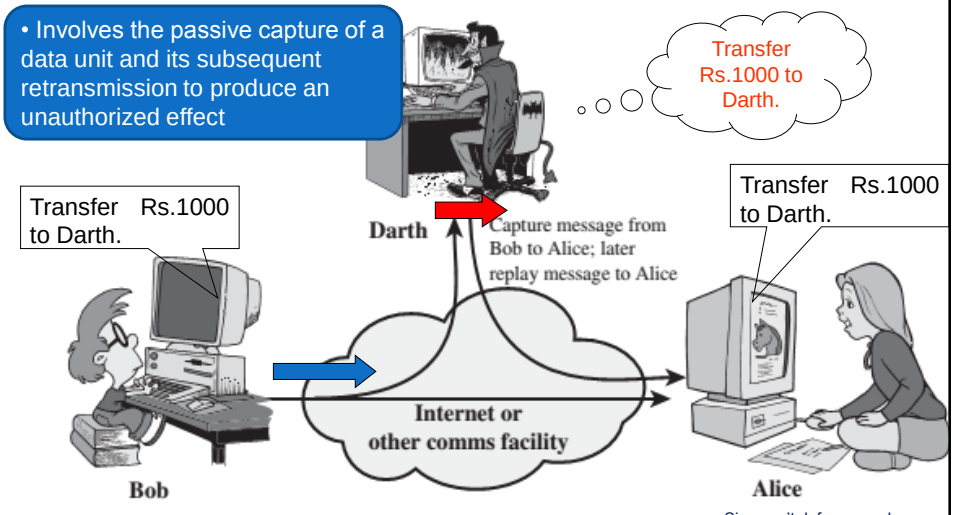

- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack

related goals?



# Active attacks: Replay

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

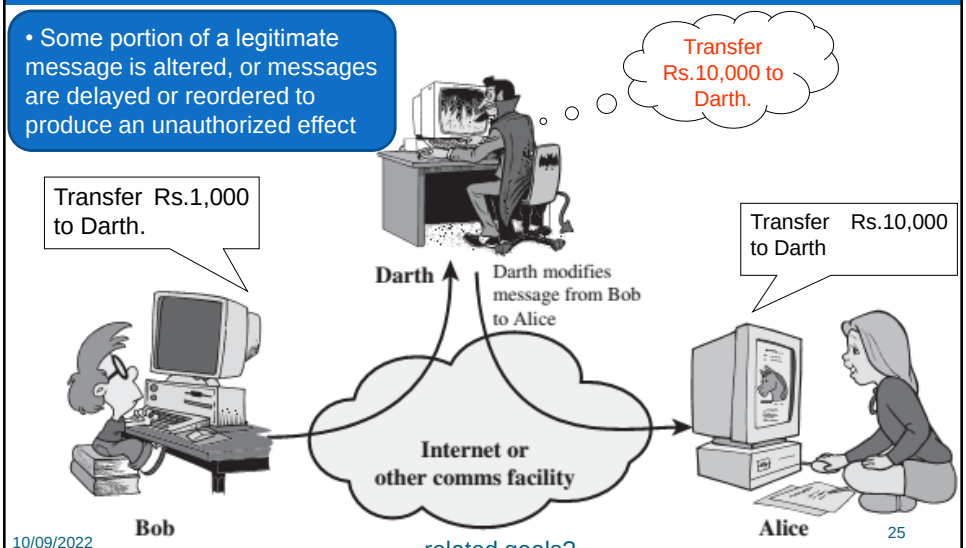



related goals?

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

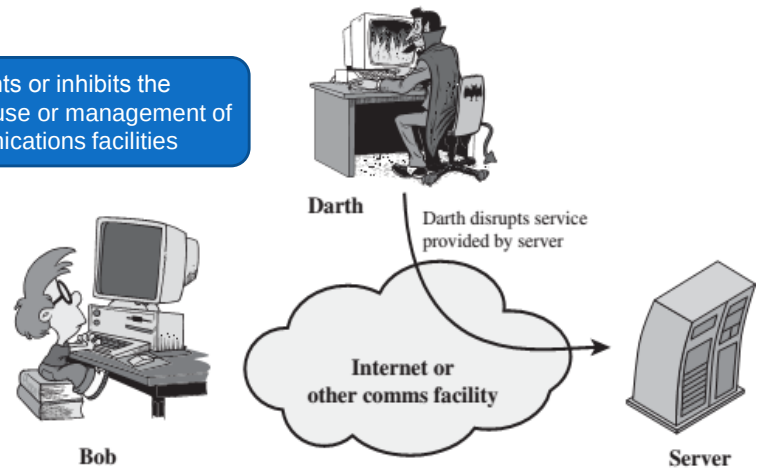



related goals?



# Active attacks: denial of service

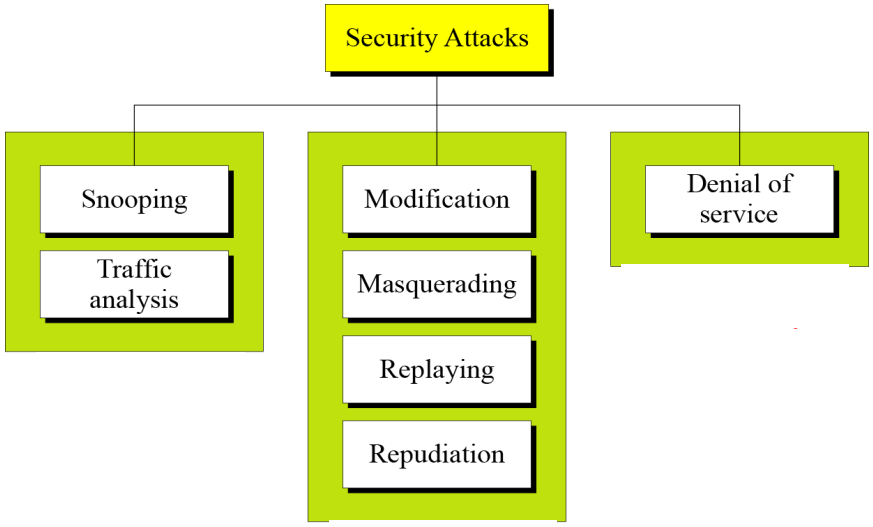
• Prevents or inhibits the normal use or management of communications facilities




related goals?

(d) Denial of service

# Taxonomy of attacks with relation to security goals




# attack surface

- The attack surface is the number of all possible points, or attack vectors, where an unauthorized user can access a system and extract data.
- The smaller the attack surface, the easier it is to protect.
- Organizations must
  - constantly monitor their attack surface to identify and
  - block potential threats as quickly as possible.
  - try and minimize the attack surface area to reduce the risk of cyberattacks succeeding.

# attack vector

- An attack vector is the method a cyber criminal uses to gain unauthorized access or breach a user's accounts or an organization's systems.
- **Common Attack Vectors**
  - Phishing: Phishing messages typically contain a malicious link or attachment that leads to the attacker stealing users' passwords or data.
  - Malware: ex ransomware, Trojans, and viruses. The risk of malware is multiplied as the attack surface expands.
  - Compromised passwords: people using weak or reused passwords on their online accounts.
  - Encryption issues: deploying poor or weak encryption can be intercepted to read the original message.
  - Unpatched software: This gives them an open door into organizations' networks and resources.



# Attack Surface Reduction

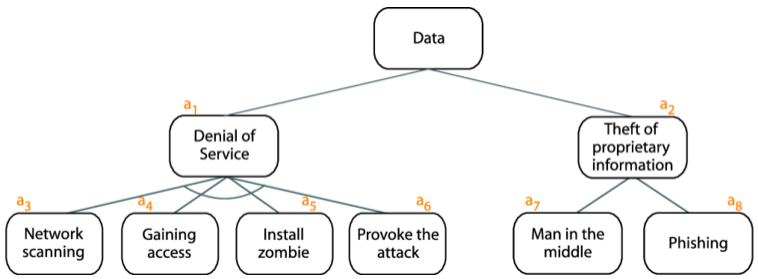
- Implement Zero-trust Policies
  - ensures only the right people have the right level of access to the right resources at the right time.
- Eliminate Complexity
  - Unnecessary complexity can result in poor management and policy mistakes that enable cyber criminals to gain unauthorized access to corporate data
- Scan for Vulnerabilities
  - identify vulnerabilities and show how endpoints can be exploited.
- Segment Network
  - allows organizations to minimize the size of their attack surface by adding barriers that block attackers. Ex firewalls
- Train Employees
  - Employees are the first line of defense against cyberattacks. They need understand best practices, spot the telltale signs of an attack through phishing emails and social engineering.

# Attack tree

- **Attack trees**
  - are conceptual diagrams showing how an asset, or target, might be attacked
  - have been used to describe threats on computer systems and possible attacks to realize those threats
- Four ways you can use attack trees as part of application security testing
  - Discover vulnerabilities to multistep attacks in computer networks and application design.
  - Represent costs for each path along the tree.
  - Improve the effectiveness of your testing strategy.
  - Evaluate the cost and effectiveness of potential defenses.



# Attack tree, ex



# What should the Good Guys Do?

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

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



# 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

# 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

# 10 Nguyên tắc thiết kế bảo mật

- 1. Minimise attack surface area - Giảm thiểu vector tấn công vào hệ thống
- 2. Establish secure defaults - Thiết lập cơ chế mặc định an toàn
- 3. The principle of Least privilege - Nguyên tắc đặc quyền tối thiểu
- 4. The principle of Defence in depth - Nguyên tắc bảo mật theo chiều sâu, nhiều lớp
- 5. Fail securely - Nguyên tắc xử lý thất bại một cách an toàn
- 6. Don't trust services - Không tin tưởng tuyệt đối vào dịch vụ
- 7. Separation of duties - Tách biệt về nhiệm vụ
- 8. Avoid security by obscurity - Tránh bảo mật bằng việc che giấu
- 9. Keep security simple - Giữ bảo mật một cách đơn giản
- 10. Fix security issues correctly - Vá lỗ hổng bảo mật một cách đúng đắn



# 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

- Assume that a security model is needed for the protection of an information using CIA Triad$^{+}$.
- Consider the information stored on **your personal computer**. For each of the terms listed, find an example and document it: threat, threat agent, vulnerability, exposure, risk, attack, and exploit.
- Using the Web, identify the chief information officers, chief information security officers in **VietNam**.
- Using the Web, find out more about **Kevin Mitnick**. What did he do? Who caught him? Write a short summary of his activities and explain why he is infamous.
- **10 Best Hackers The World** Has Ever Known