Information System Security
Threat, Vulnerabilities and attack

Cyber security threat

A cyber security threat is any potential action or event that could harm digital system , steal data or disrupt operation .

Threat Categorization

- **Deliberate Threat**
  - Traffic overload
  - Network Failure
  - Malicious Software
  - Illegal use of Software
  - Theft
  - Infiltration

Environment

- Earthquakes
- Floods
- Lightning
- Storm
- Tornadoes
- Deterioration

Accidental

- Service Failure
- Hardware Failure
- Human Error
- Design Failure
- Misroute Message
- Transmission Error

Threats to Info. Security

Threat Category	Examples
Acts of human error or failure	*Accidents, employee mistakes*
Intellectual property compromise	Piracy, copyright infringement
Deliberate espionage or trespass	Unauthorized access, data collection
Deliberate information extortion	Blackmail of info. disclosure
Deliberate sabotage or vandalism	Destruction of systems or info.
Deliberate theft	Illegally taking equipment or info.
Deliberate software attacks	*Viruses, worms, denial of service*
Forces of nature	Fires, floods, earthquakes
Deviations in service from providers	Power and Internet provider issues
Technological hardware failures	Equipment failure
Technological software failures	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Vulnerability

A **vulnerability** is a weakness in the security system

1. Physical Vulnerability
2. Natural Vulnerability
3. Hardware and Software Vulnerability
4. Media Vulnerability
5. Human vulnerability

Vulnerability

A **vulnerability** scanner software

1. NESSUS
2. BurpSuite
3. Qualys
4. Zenmap
5. Acunetix Vulnerability Scanner
6. Netsparker
7. Intruder

.....

Attacks (1)

- Act or action that exploits vulnerability (i.e., an identified weakness) in controlled system
- Accomplished by threat agent which damages or steals organization's information

Attacks (2)

- **Malicious code**: launching viruses, worms, Trojan horses, and active Web scripts aiming to steal or destroy info.
- **Backdoor**: accessing system or network using known or previously unknown mechanism
- **Password crack**: attempting to reverse calculate a password
- **Brute force**: trying every possible combination of options of a password
- **Dictionary**: selects specific accounts to attack and uses commonly used passwords (i.e., the dictionary) to guide guesses

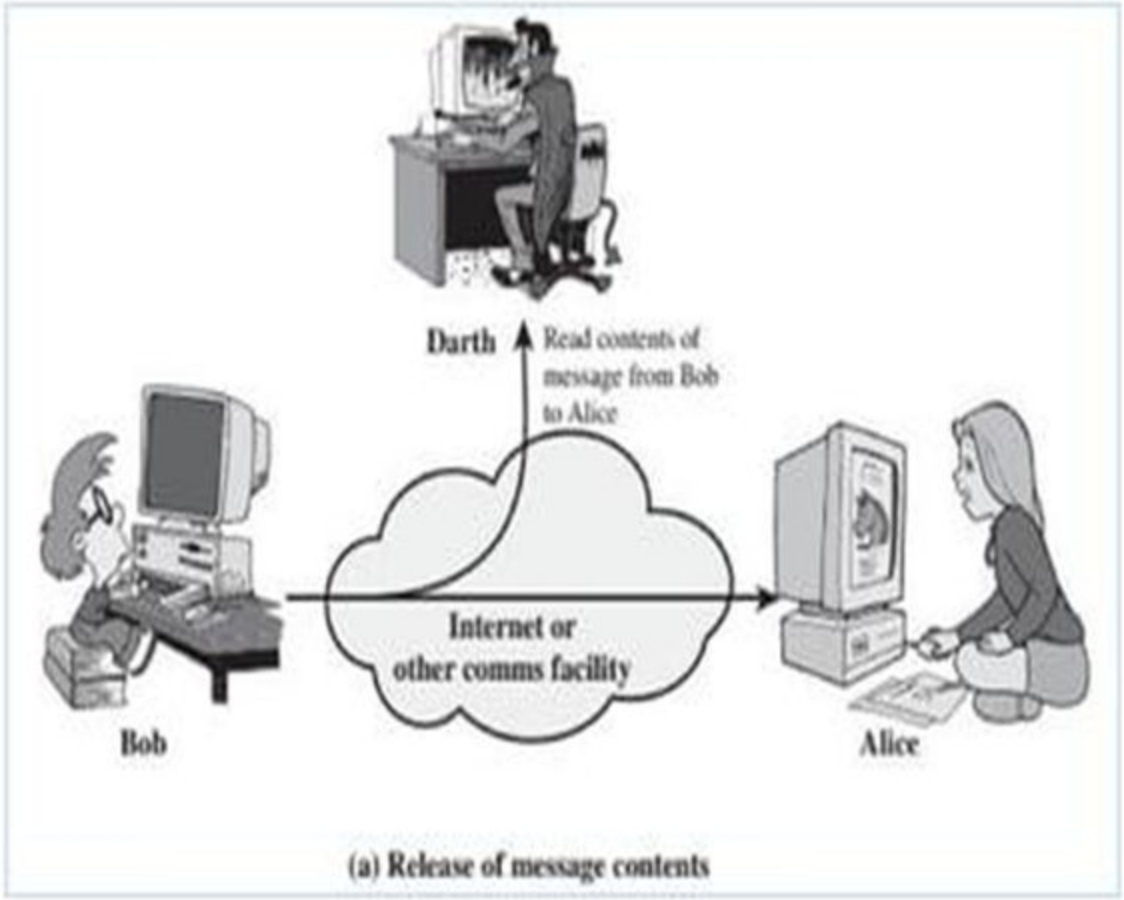
Security Attacks Categories

1. Passive Attacks
2. Active Attacks

A **passive attack** attempts to learn or make use of information from the system but does not affect system resources.

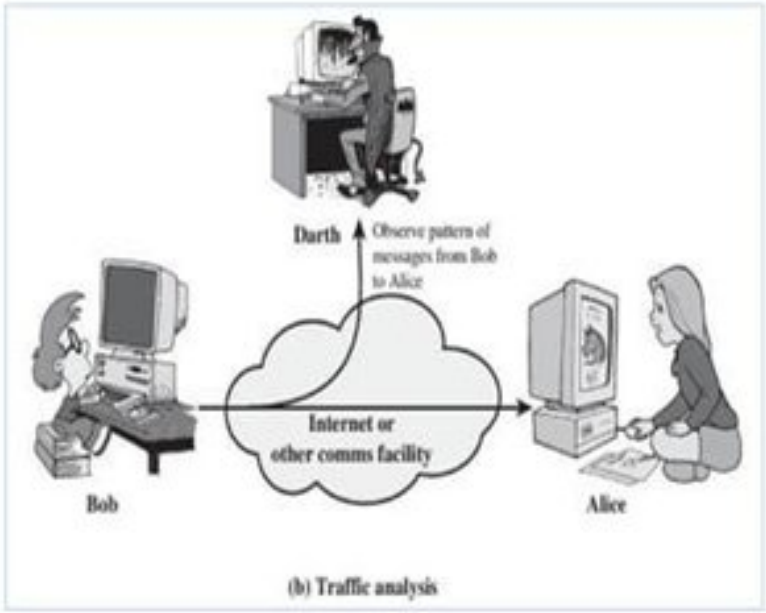
An **active attack** attempts to alter system resources or affect their operation.

Passsive Attack #1



(a) Release of message contents

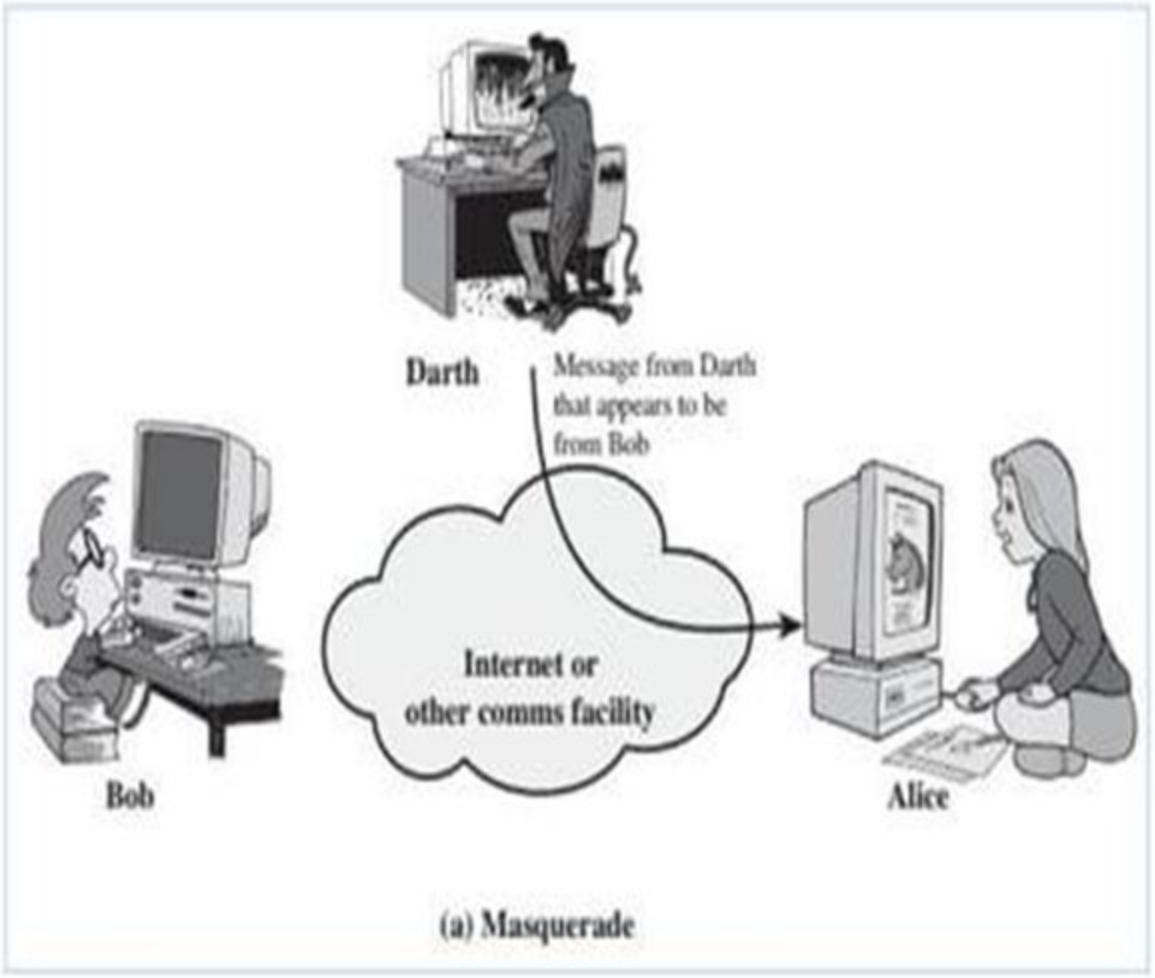
Passsive Attack #2



(b) Traffic analysis

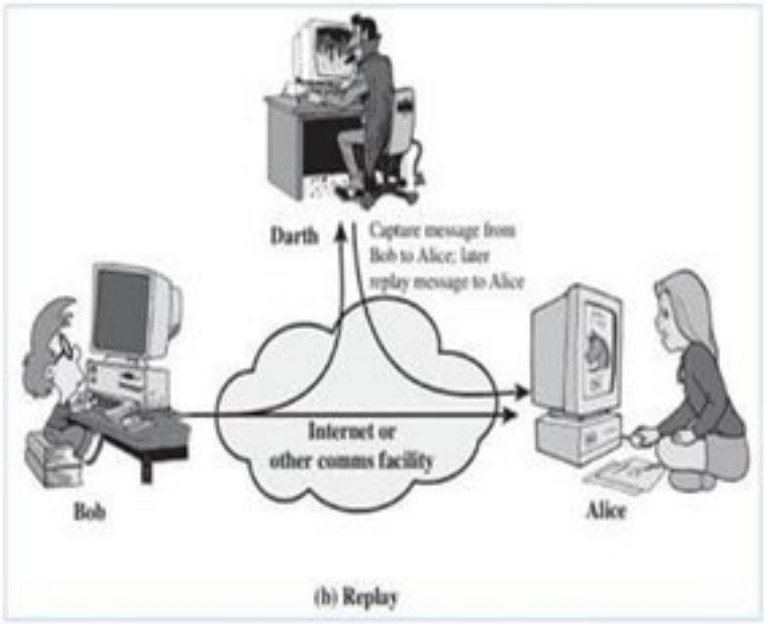
Passive attacks are very difficult to detect, because they do not involve any alteration of the data

Active Attack #1



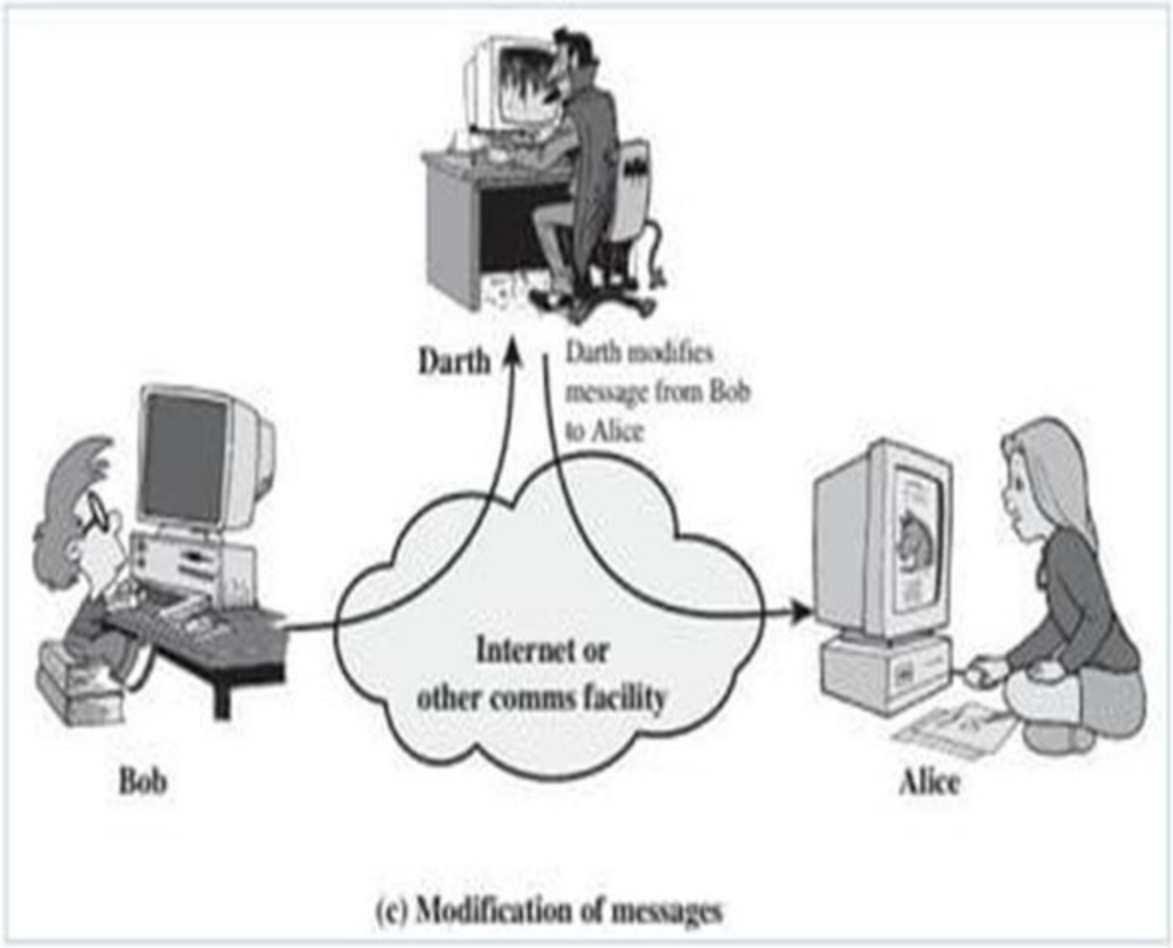
(a) Masquerade

Active Attack #2



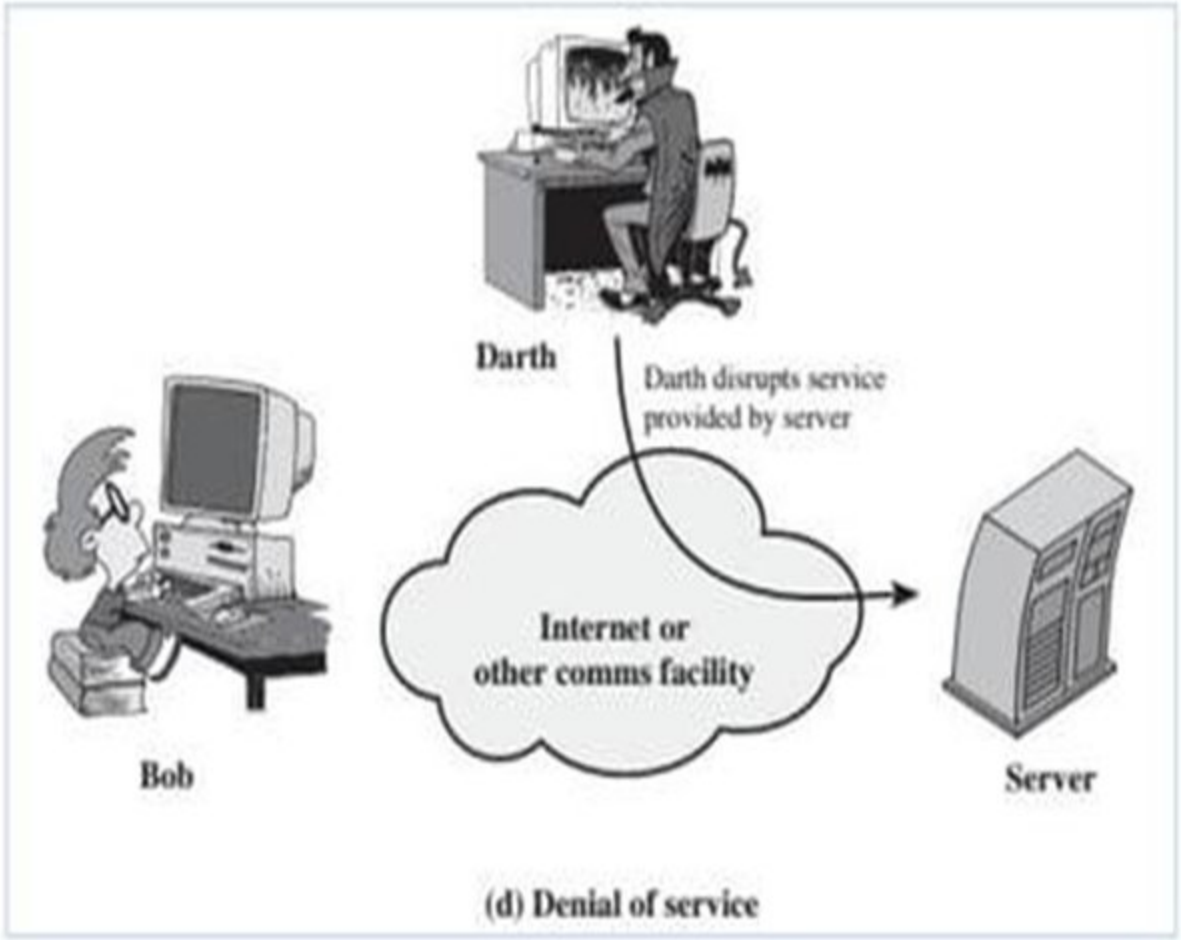
(b) Replay

Active Attack #3



(c) Modification of messages

Active Attack #4



(d) Denial of service

3 “Biggest” Common Attack

3 "Biggest" Common Attack

- ✓ The primary vulnerabilities for end-user computers are virus, worm, and Trojan Horse attacks:
- ✓ A virus is malicious software which attaches to another program to execute a specific unwanted function on a computer.
- ✓ A worm executes arbitrary code and installs copies of itself in the memory of the infected computer, which then infects other hosts.
- ✓ A Trojan Horse is an application written to look like something else. When a Trojan Horse is downloaded and opened, it attacks the end-user computer from within.