DATA SECURITY AND PRIVACY

Tophan Kumar Jena
Asst.Professor
Dept.: CSE

Books for this Course

- Text Books:
  - D.R.Stinson,Cryptography Theory and Practice, CRC Press
  - C.P.Pfleeger,S.L.Pfleeger and J.Margulies,Security in Computing
  - A. Banafa, Blockchain Technology and Application, 1st Edition ,2020
- Reference Book:
  - Cryptography and Network Security: Principles and Practice- William Stallings, PHI.
  - A.J.Menezes,P.C. Van Ooschot and S.A.Vanstone, Handbbok of Applied Cryptography, CRC Press
  - Cryptography and Network Security- B.A. Forouzan & D. Mukhopadhyay, McGraw Hill Special Indian Edition.

- Introduction to security
- Principles of Security
- Types of Attacks

Introduction to Security

- Security is prevention from harm:
  - **Personal security** is the protection of a person's livelihood.
  - **Information security** (InfoSec) is the protection of information from being accessed, used, misused, modified, or destroyed by the wrong people.
  - **Computer Security** (Cybersecurity) is information security in the world of digital assets (software, hardware, communication systems).
  - **Software Security** is the study and application of writing robust software that is secure.

- Network Security - measures to protect data during their transmission .
- Internet Security - measures to protect data during their transmission over a collection of interconnected networks .

Data Security

- Data security involves the use of various methods to make sure that data is correct, kept confidential and is safe.
- Data security includes:

  Ensuring integrity of data.

  Ensuring privacy of data.

  Prevent the loss or destruction of the data

Information Security

- Information security (InfoSec), is the practice of defending information from
  - unauthorized access,
  - disclosure,
  - disruption,
  - modification,
  - inspection,
  - recording,
  - destruction.

Who needs Information Security?

- Government,
- Military,
- Corporations,
- Financial institutions,
- Hospitals
- Private businesses
- They have a great deal of
  - confidential information about their employees, customers, products, research and financial status.

Security Services

- Confidentiality: Ensures that the information in a computer system a n d transmitted information are accessible only for reading by authorized parties. E.g. Printing, displaying and other forms of disclosure.
- Authentication: Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.

- Integrity: Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
- Non repudiation: Requires that neither the sender nor the receiver of a message be able to deny the transmission.

- Access control: Requires that access to information resources may be controlled by or the target system.
- Availability: Requires that computer system assets be available to authorized parties when needed.

What is CIA Triad ?

Application ?

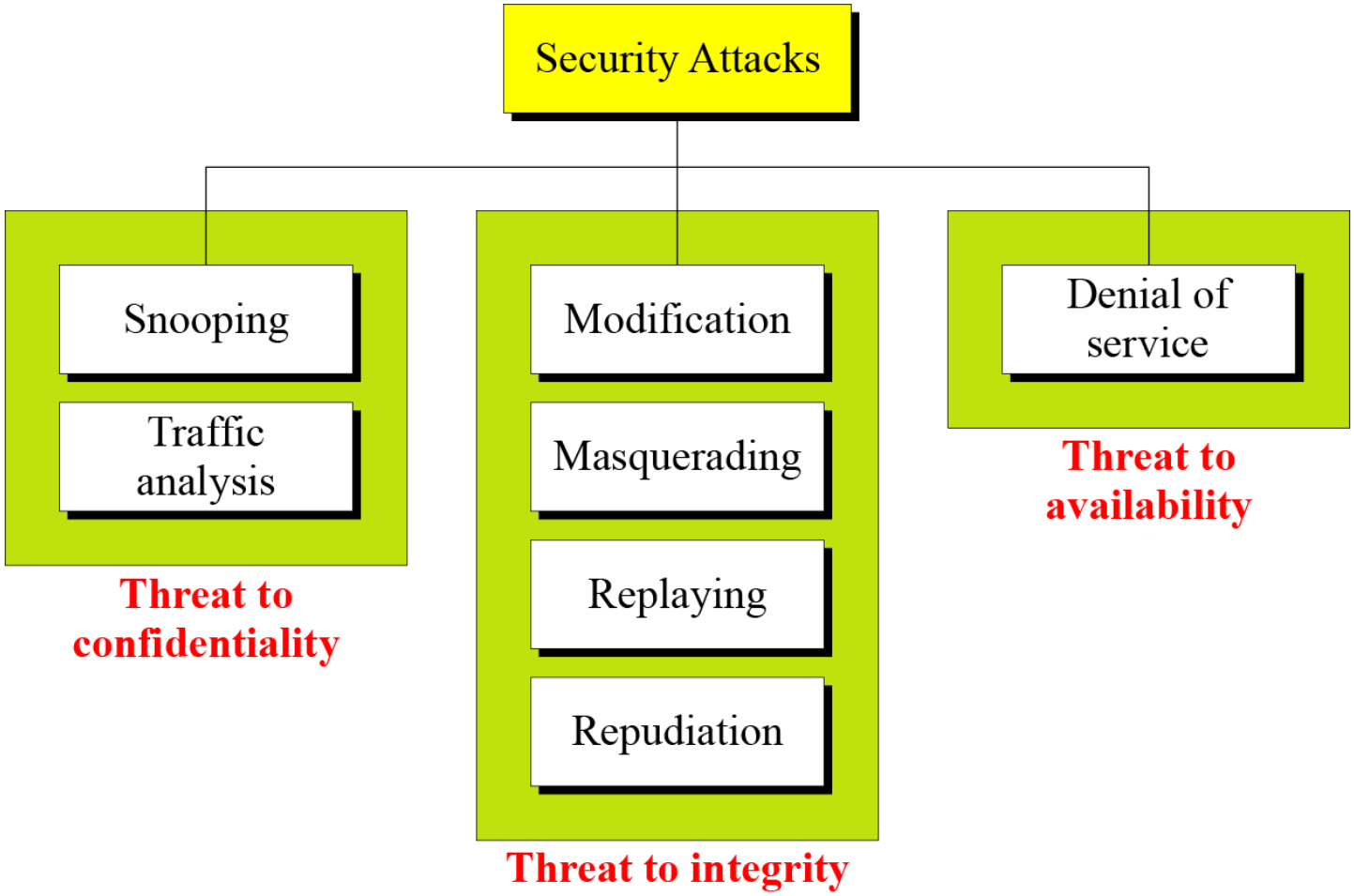
- Security in Transmission
- Electronic Signature/Digital Signature
- Identification/Password protection
- Security Protocol

Security Attacks

- The three goals of security-Confidentiality, Integrity, and Availability—can be threatened by security attacks.

1. Attacks on Confidentiality
2. Attacks on Integrity
3. Attacks on Availability

- All these attacks can be broadly classified as either Active or Passive attacks


Security Attacks
Snooping
Traffic analysis
Threat to confidentiality
Modification
Masquerading
Replaying
Repudiation
Threat to integrity
Denial of service
Threat to availability

Attacks on Confidentiality

- Snooping refers to unauthorized access to or interception of data.
- Traffic analysis refers to obtaining some specific type of information by monitoring online traffic.

Attacks on Integrity

- Modification means that the attacker intercepts the message and changes it.
- Masquerading or spoofing happens when the attacker impersonates somebody else.
- Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it
- Repudiation means that sender of the message might later deny that he has sent the message; the receiver of the message might later deny that he has received the message.

Attacks on Availability

- Denial of service (DoS) is a very powerful attack, which may slow down or totally interrupt the service of a system .
- An attacker in DoS typically floods the targeted machine (Server) with so many superfluous requests that, the machine remains busy in servicing them.
- As a result all legitimate requests from other systems are prevented from servicing.

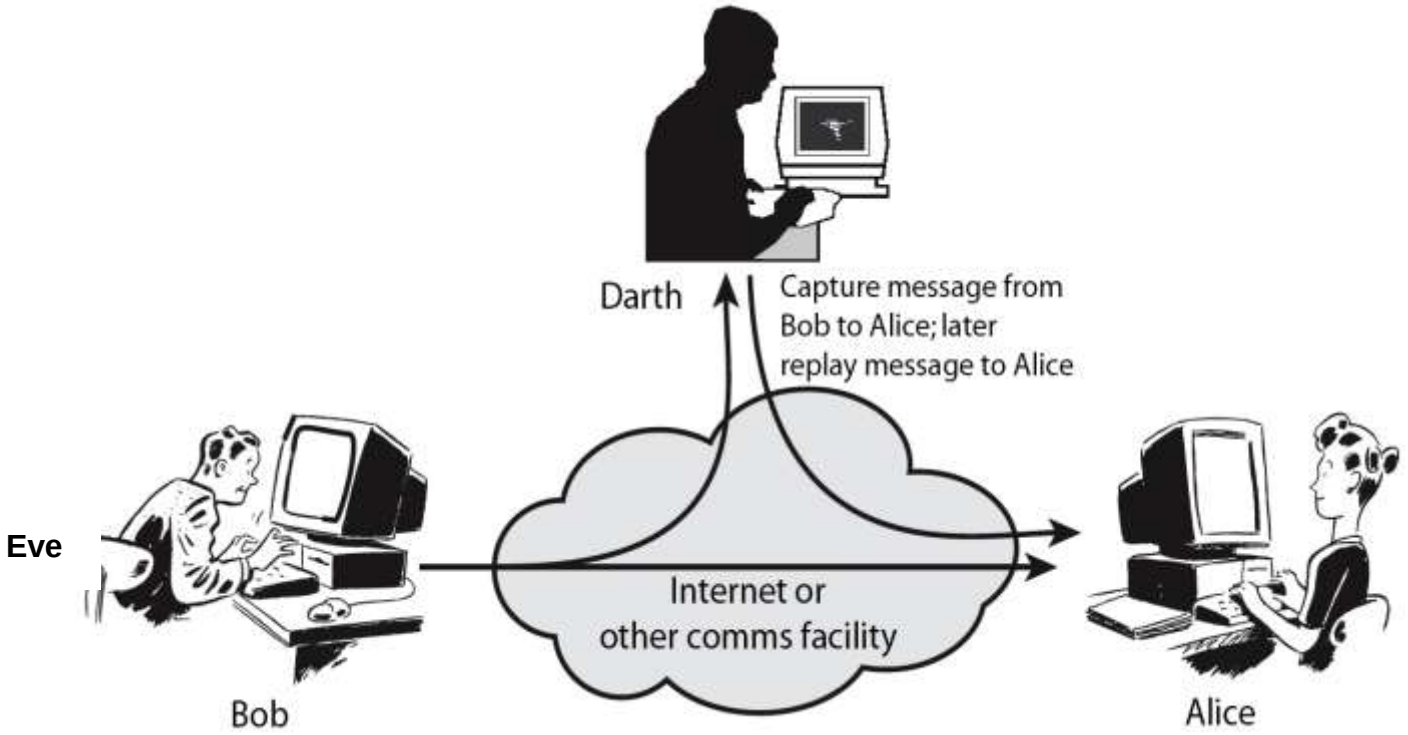
Active vs Passive Attacks

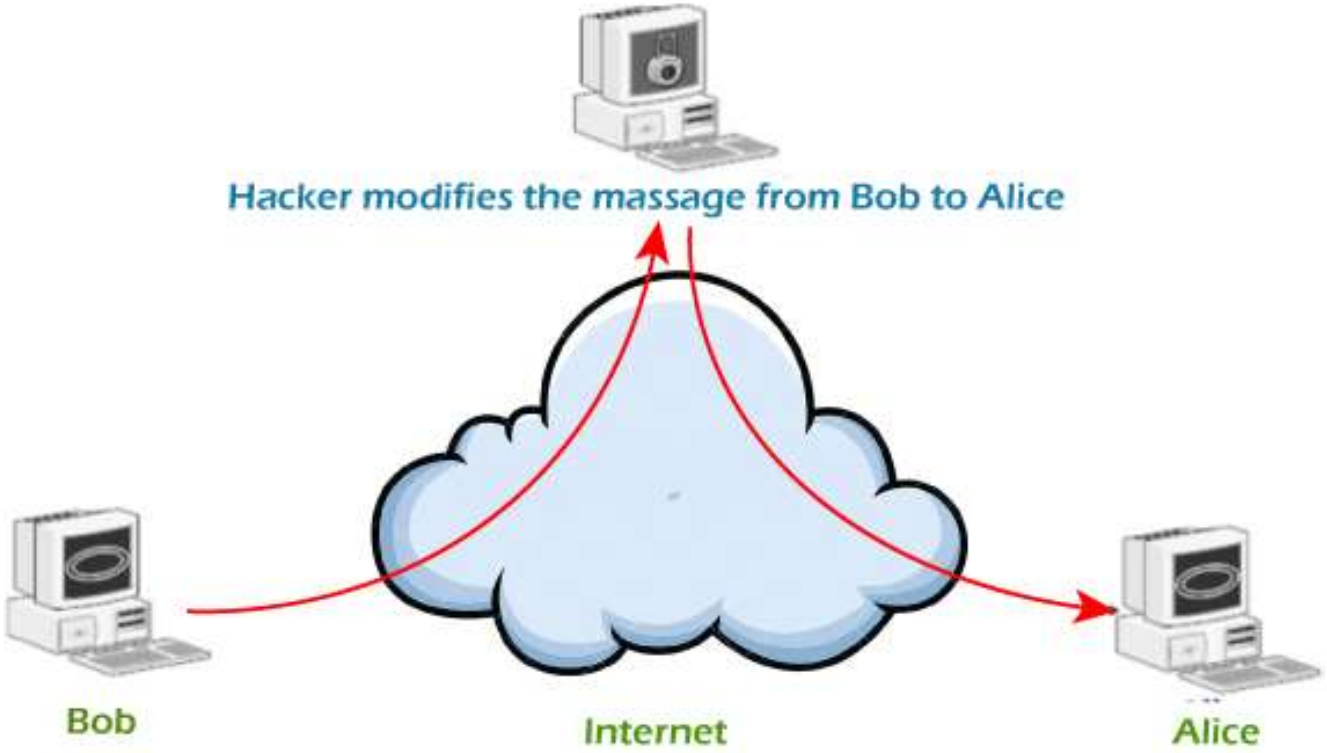
- Active attack may change the data or harm the system.

- Passive attack is not to change the data or harm the system, but to obtain the information. So it harms the sender and receiver of the message

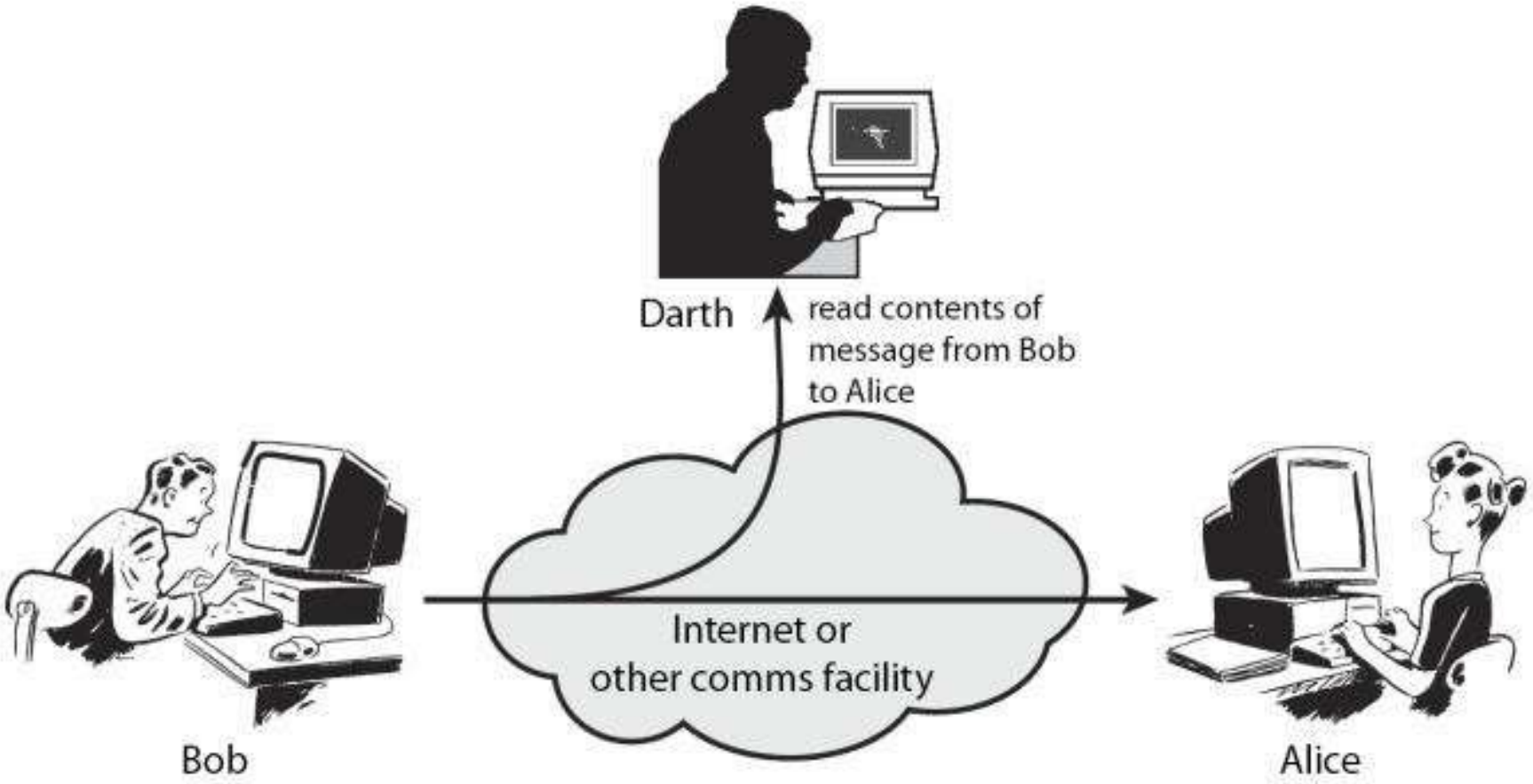
Active vs Passive

- Active Attack





Active Attacks (Modifications of messages)


Darth
read contents of
message from Bob
to Alice
Internet or
other comms facility
Bob
Alice

Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability