B. Tech. III (CSE) Semester – VI INFORMATION SECURITY AND CRYPTOGRAPHY CS302

INTRODUCTION

The OSI Security Architecture

- To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.
- Security Architecture for OSI, defines such a systematic approach.4 The OSI security architecture is useful to managers as a way of organizing the task of providing security.

The OSI security architecture focuses on security attacks, mechanisms, and services. These can be defined briefly as

■ Security attack: Any action that compromises the security of information owned by an organization.

■ Security mechanism: A process that is designed to detect, prevent, or recover from a security attack.

■ Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

Security 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.

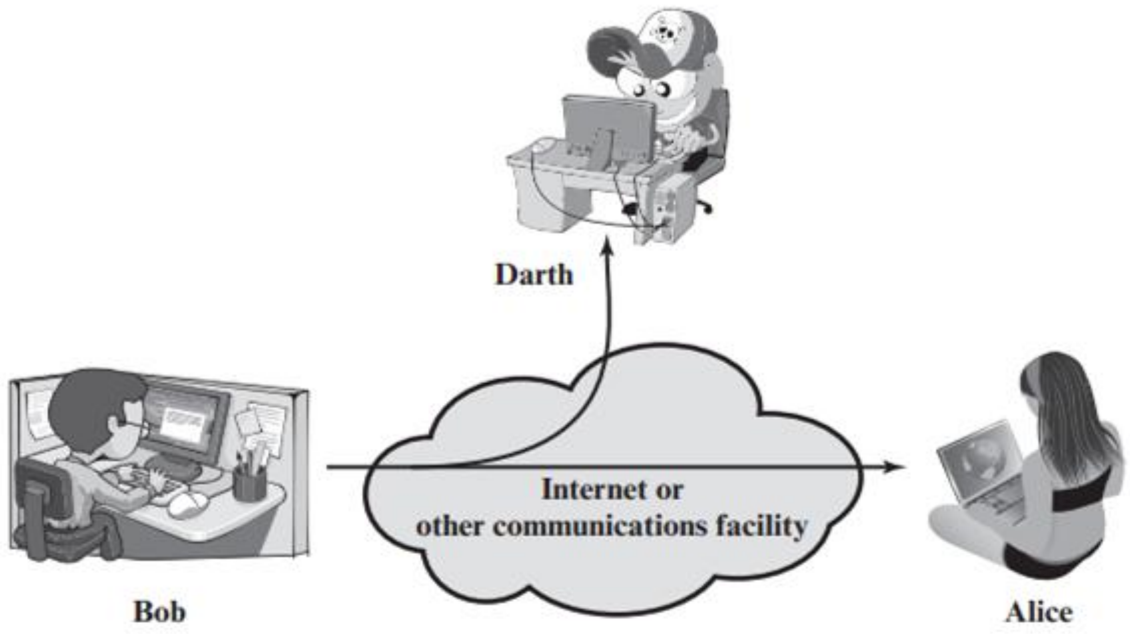
Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

Passive Attack

The **release of message contents** is easily understood. A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions

A second type of passive attack, **traffic analysis:** Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The common technique for masking contents is encryption.

Passive Attack



(a) Passive attacks

Active Attacks

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.

A **masquerade** takes place when one entity pretends to be a different entity.

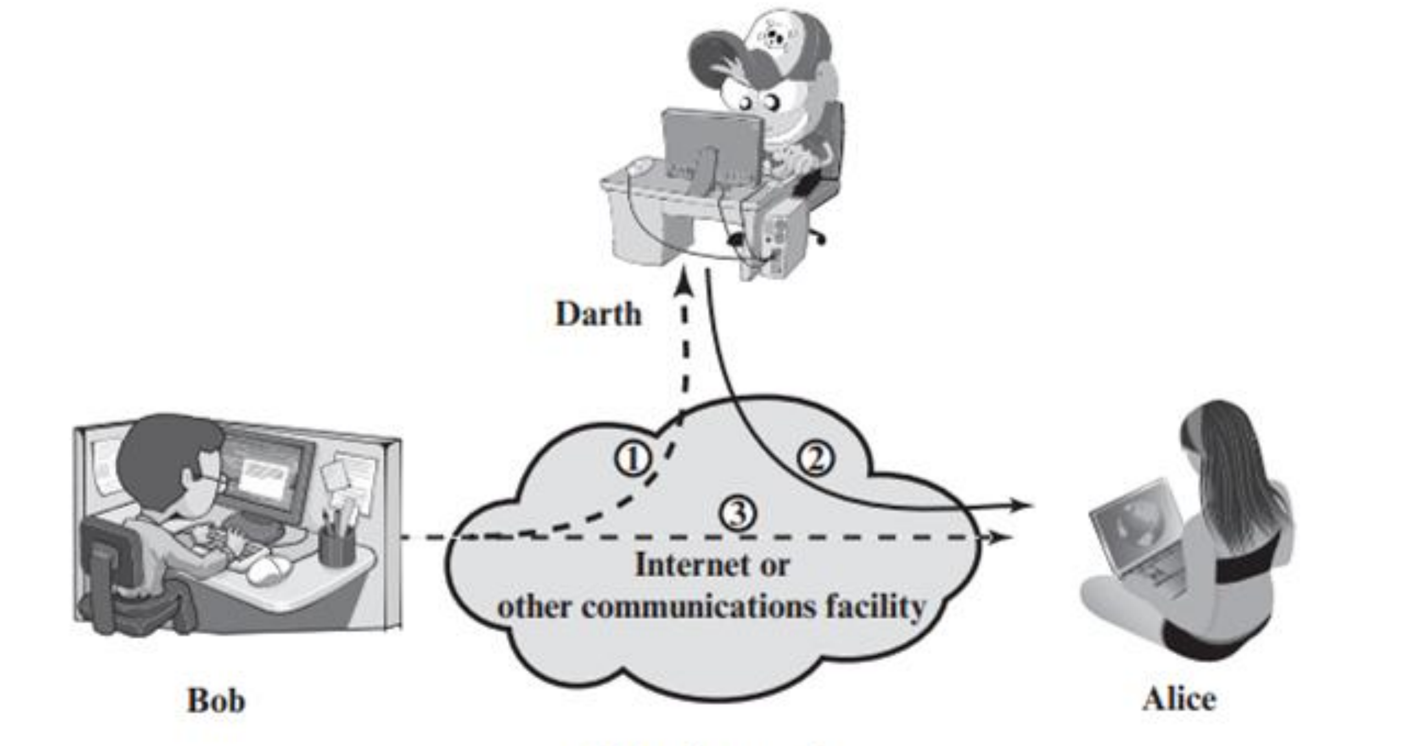
Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Active Attacks

Modification of messages simply means that some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.

The **denial of service** prevents or inhibits the normal use or management of communications facilities. 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.

Active Attacks



(b) Active attacks

Security Services

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

a processing or communication service that is provided by a system to give a specific kind of protection to system resources; security services implement security policies and are implemented by security mechanisms.

Data confidentiality is designed to protect data from disclosure attack. The service as defined by X.800 is very broad and encompasses confidentiality of the whole message or part of a message and also protection against traffic analysis.

Data integrity is designed to protect data from modification, insertion, deletion, and replaying by an adversary. It may protect the whole message or part of the message.

This service provides the **authentication** of the party at the other end of the line. In connection-oriented communication, it provides authentication of the sender or receiver during the connection establishment. In connectionless communication, it authenticates the source of the data.

Security Services

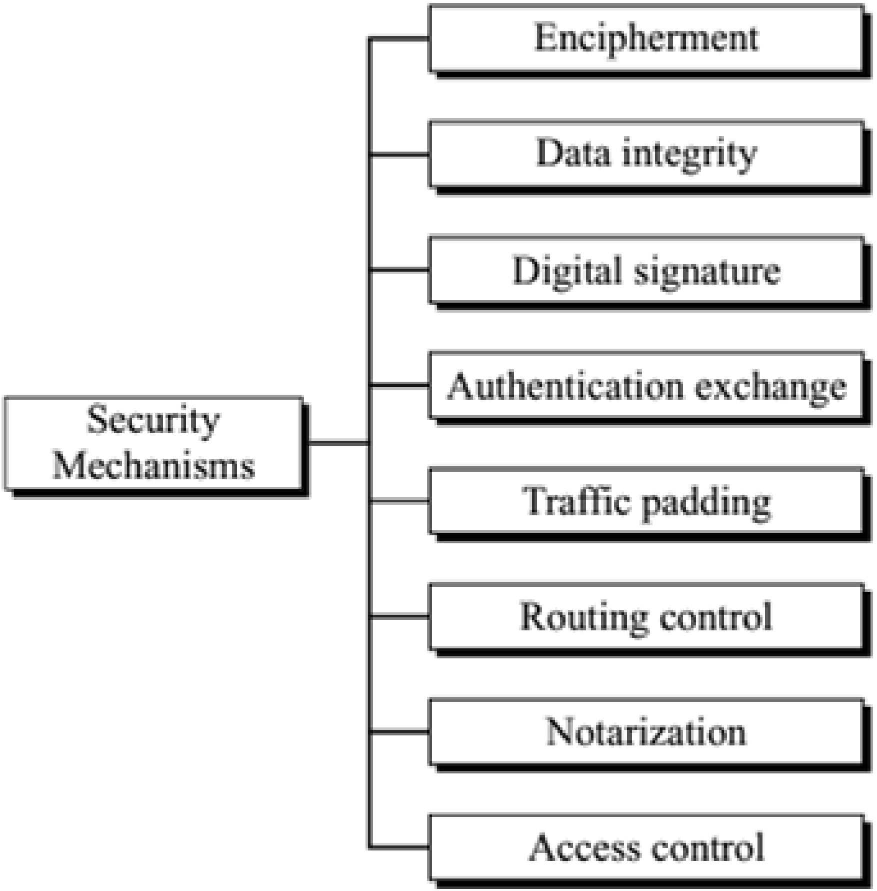
Nonrepudiation service protects against repudiation by either the sender or the receiver of the data. In non repudiation with proof of the origin, the receiver of the data can later prove the identity of the sender if denied.

Access control provides protection against unauthorized access to data. The term access in this definition is very broad and can involve reading, writing, modifying, executing programs, and so on.

Security Mechanism

The mechanisms are divided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service.

Encipherment, hiding or covering data, can provide confidentiality. It can also be used to complement other mechanisms to provide other services. Today two techniques cryptography and steganography are used for enciphering.


Security Mechanisms
Encipherment
Data integrity
Digital signature
Authentication exchange
Traffic padding
Routing control
Notarization
Access control

The **data integrity** mechanism appends to the data a short checkvalue that has been created by a specific process from the data itself. The receiver receives the data and the checkvalue.

A **digital signature** is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.

In **authentication exchange,** two entities exchange some messages to prove their identity to each other. For example, one entity can prove that she knows a secret that only she is supposed to know.

Traffic padding means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

Routing control means selecting and continuously changing different available routes between the sender and the receiver to prevent the opponent from eavesdropping on a particular route.

Access control uses methods to prove that a user has access right to the data or resources owned by a system. Examples of proofs are passwords and PINs.

Notarization means selecting a third trusted party to control the communication between two entities. This can be done, for example, to prevent repudiation. The receiver can involve a trusted party to store the sender request in order to prevent the sender from later denying that she has made such a request.