Introduction to Security and Cryptography

Introduction

- Digital Information are now everywhere
- Some information are assets and have high value
- Requires information security mechanisms to secure them.
- The NIST standard FIPS 199 lists the following as security objectives(goals) for information and information systems.
  - Confidentiality
  - Integrity
  - Availability

Security Goals

- **Confidentiality**
  - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
  - A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity**
  - Guarding against improper information modification or destruction, with ensuring information nonrepudiation and authenticity.
  - A loss of integrity is the unauthorized modification or destruction of information.
- **Availability**
  - Ensuring timely and reliable access to and use of information.
  - A loss of availability is the disruption of access to information or an information system.

Additional Security Concepts

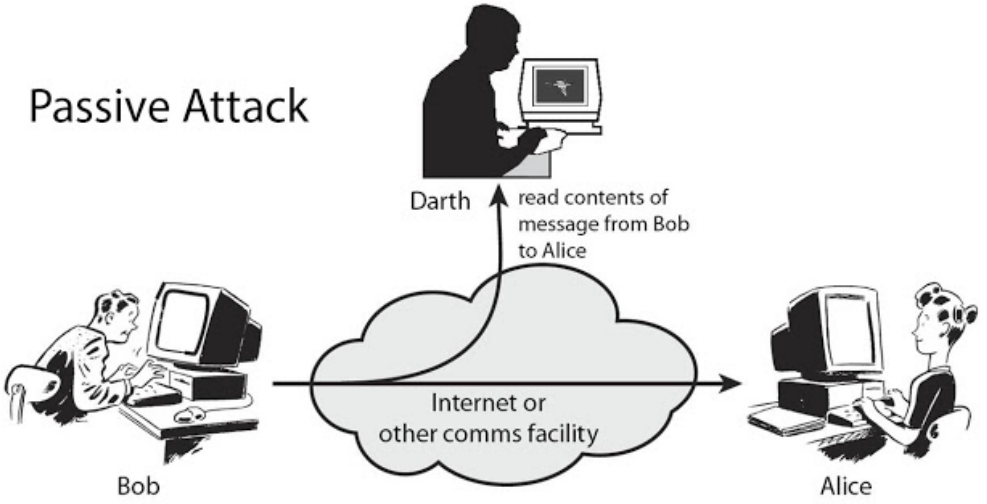
- **Authenticity**
  - The property of being genuine and being able to be verified and trusted
  - Confidence in the validity of a transmission, a message, or message originator
- **Accountability**
  - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - Supports nonrepudiation, deterrence, and after-action recovery and legal action.
  - Activity records are logged to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

X.800, The Security Architecture for OSI

- **Security attack**: An action that compromises the security of information owned by an organization.
- **Security mechanism**: A process (or a device) 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.
  - Intended to counter security attacks
  - Make use of one or more security mechanisms to provide the service.

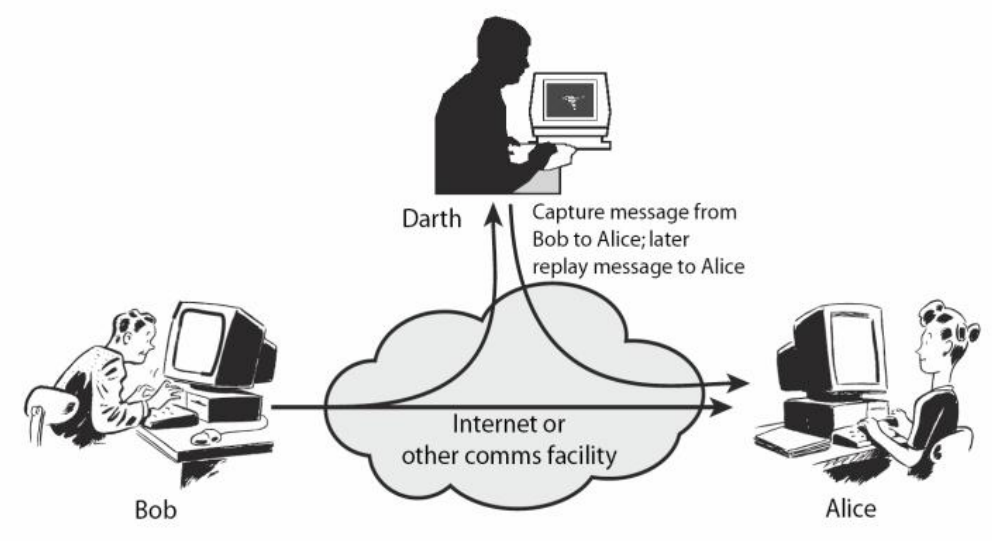
Security Attacks

- **Passive Attacks**
  - in the nature of eavesdropping on, or monitoring
  - obtain information that is being transmitted
  - Two types
    - release of message contents (snooping)
    - traffic analysis.



Security Attacks(2)

- **Active Attacks**
  - involve some modification of the data stream
  - The creation of a false stream
  - Four types
    - Masquerade
    - Replay
    - Modification
    - Denial of service



Active Replay attack

Security Attacks(3)

- Attacks on confidentiality
  - Snooping, Traffic analysis.
- Attacks on Integrity
  - Modification, Masquerading, Replay, Repudiation
- Attack on Availability
  - Denial of Service

Security Services by ITU-T

- Data Confidentiality
  - Confidentiality is the protection of transmitted data from passive attacks.
- Data Integrity
  - Protection of data from modification, insertion, deletion, and replaying by an adversary.
- Authentication
  - Ensuring authentic communication
    - Peer entity authentication
    - Data origin authentication

Security Services by ITU-T (2)

- Access Control
  - Ability to limit and control the access to host systems and applications via communications links
- Nonrepudiation
  - Prevents either sender or receiver from denying a transmitted message
- Availability
  - a system or a resource being accessible and usable upon demand by an authorized entity, according to specifications

Security Mechanisms

- **Encipherment**
  - The use of mathematical algorithms to transform data into a form that is not readily intelligible.
- **Digital Signature**
  - Data appended to, or a cryptographic transformation of, a data unit that allows a recipient to prove the source and integrity of the data unit and protect against forgery.
- **Access Control**
  - Enforce access rights to resources via pin, password, biometrics,etc..
- **Data Integrity**
  - Used to assure the integrity of a data unit or stream of data units.

Security Mechanisms(2)

- **Authentication Exchange**
  - To ensure the identity of an entity by means of information exchange.
- **Traffic Padding**
  - The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- **Routing Control**
  - Enables selection of particular physically secure routes for certain data and allows routing changes
- **Notarization**
  - The use of a trusted third party to assure certain properties of a data exchange.

Pervasive Security Mechanisms

- Trusted Functionality
- Security Label
- Event Detection
- Security Audit Trail
- Security Recovery

Security Mechanism - Services

SERVICE \ MECHANISM	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Cryptography (Secret writing)

- Study and practice of techniques to store and communicate information in a form (cipher) such that only authorized entities can read and process it.
- Cryptographic Attacks
  - Attacks on cryptographic techniques
- Types of Cryptographic attacks
  - Cryptanalytic Attacks : Combination of statistical and algebraic techniques with the aim to retrieve secret key of ciphers.
  - Non-cryptanalytic Attacks : Does not explore the mathematical aspects of the cryptographic techniques

Stegenography

- Means “covered writing” in greek
- Concealing the message itself by covering with something else.
- Mostly message is hidden inside another data.