# Chapter 1

# Introduction

Dr. Shin-Ming Cheng

# Roadmap

- Cryptographic algorithms
  - the study of techniques for ensuring the secrecy and/or authenticity of information
    - symmetric ciphers
    - asymmetric encryption
    - hash functions
- Mutual Trust
  - study of techniques and algorithms for providing mutual trust in two main areas
    - key management and distribution
      - establish trust in the encryption keys used between two communicating entities
    - user authentication
      - establish trust in the identity of a communicating partner

# Roadmap

- Network Security
  - covers the use of cryptographic algorithms in network protocols and network applications
- Computer Security
  - security of computers against intruders (e.g., hackers) and malicious software (e.g., viruses).
  - Typically, the computer to be secured is attached to a network and the bulk of the threats arise from the network.

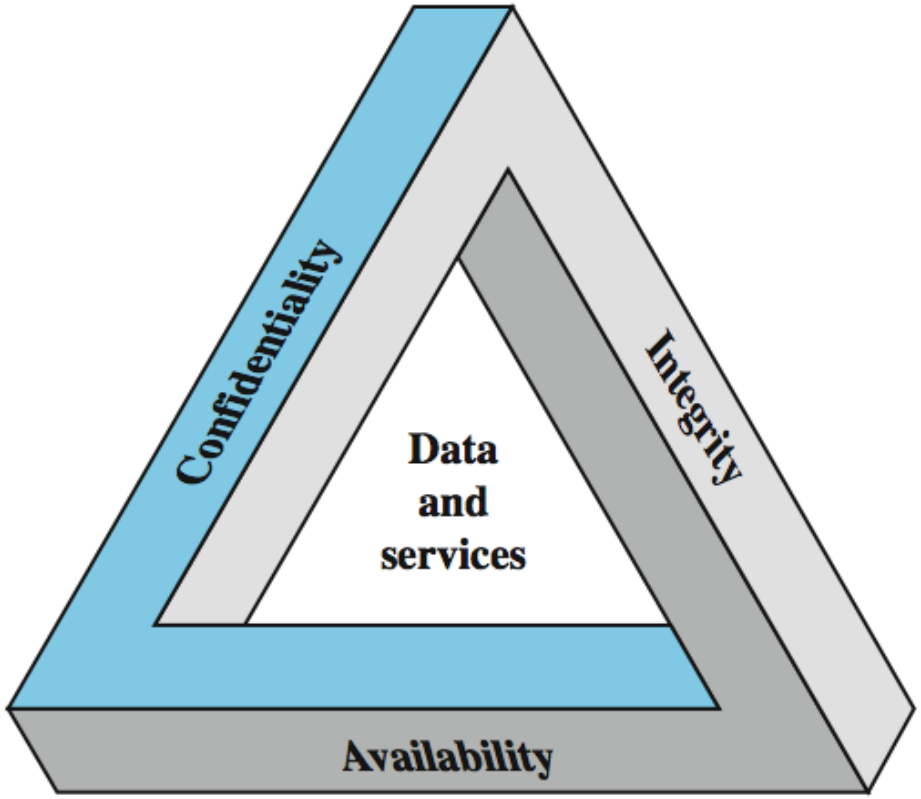
# Standards Organizations

- National Institute of Standards & Technology (NIST)
  - Federal Information Processing Standards (FIPS)
- Internet Society (ISOC)
  - Internet Engineering Task Force (IETF)
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)

# Computer Security

- the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources
  - Hardware
  - Software
  - Firmware
  - information/data,
  - telecommunications

# Key Security Concepts: CIA triad



# Key Security Concepts: CIA triad

- Confidentiality (covers both data confidentiality and privacy):
  - 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 (covers both data and system integrity)
  - Guarding against improper information modification or destruction, and includes ens
  - uring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

# Key Security Concepts: CIA triad

- Availability:
  - Ensuring timely and reliable access to and use of information.
  - A loss of availability is the disruption of access to or use of information or an information system.

# Key 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.

# Levels of Impact

- can define 3 levels of impact from a security breach
  - Low
  - Moderate
  - High

# Examples of Security Requirements

- confidentiality – student grades
- integrity – patient information
- availability – authentication service

# Computer Security Challenges

- not simple
- must consider potential attacks
- procedures used counter-intuitive
- involve algorithms and secret info
- must decide where to deploy mechanisms
- battle of wits between attacker / admin
- not perceived on benefit until fails
- requires regular monitoring
- too often an after-thought
- regarded as impediment to using system

# OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
  - To assess effectively the security needs of an organization and to evaluate and choose various security products and policies
  - a systematic way of
    - Defining the requirements for security
    - Characterizing the approaches to satisfying those requirements
  - provides a useful, if abstract, overview of concepts we will study

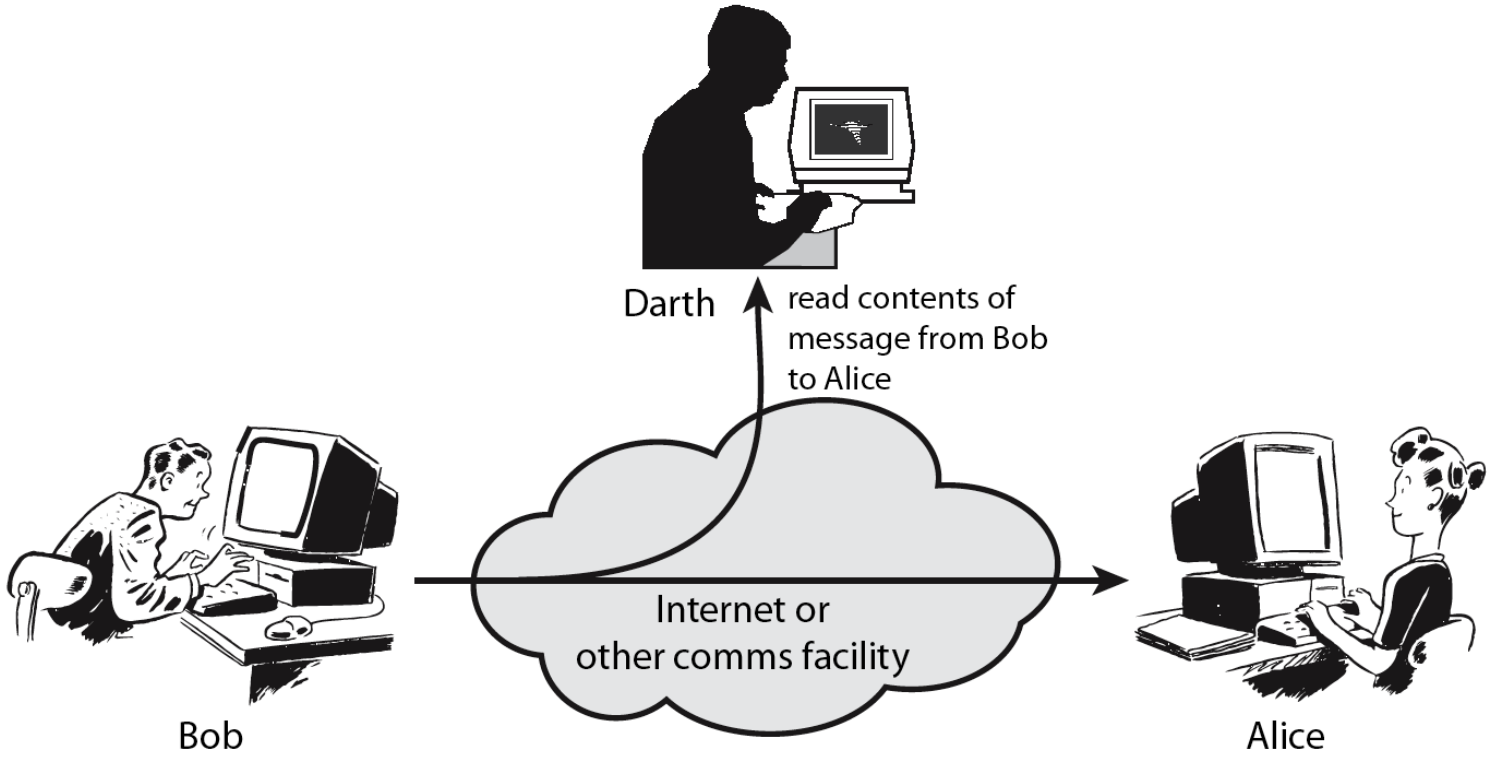
# OSI Security

- Security attack:
  - Any actions that compromises the security of information owned by an organization (or a person)
- Security mechanism:
  - a mechanism that is designed to detect, prevent, or recover from a security attack
- Security service
  - a service that enhances the security of the data processing systems and the information transfers of an organization. The services make use of one or more

# Some Definitions

- Threat
  - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
  - A threat is a possible danger that might exploit a vulnerability.
- Attack
  - An assault on system security that derives from an intelligent threat;
  - An intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

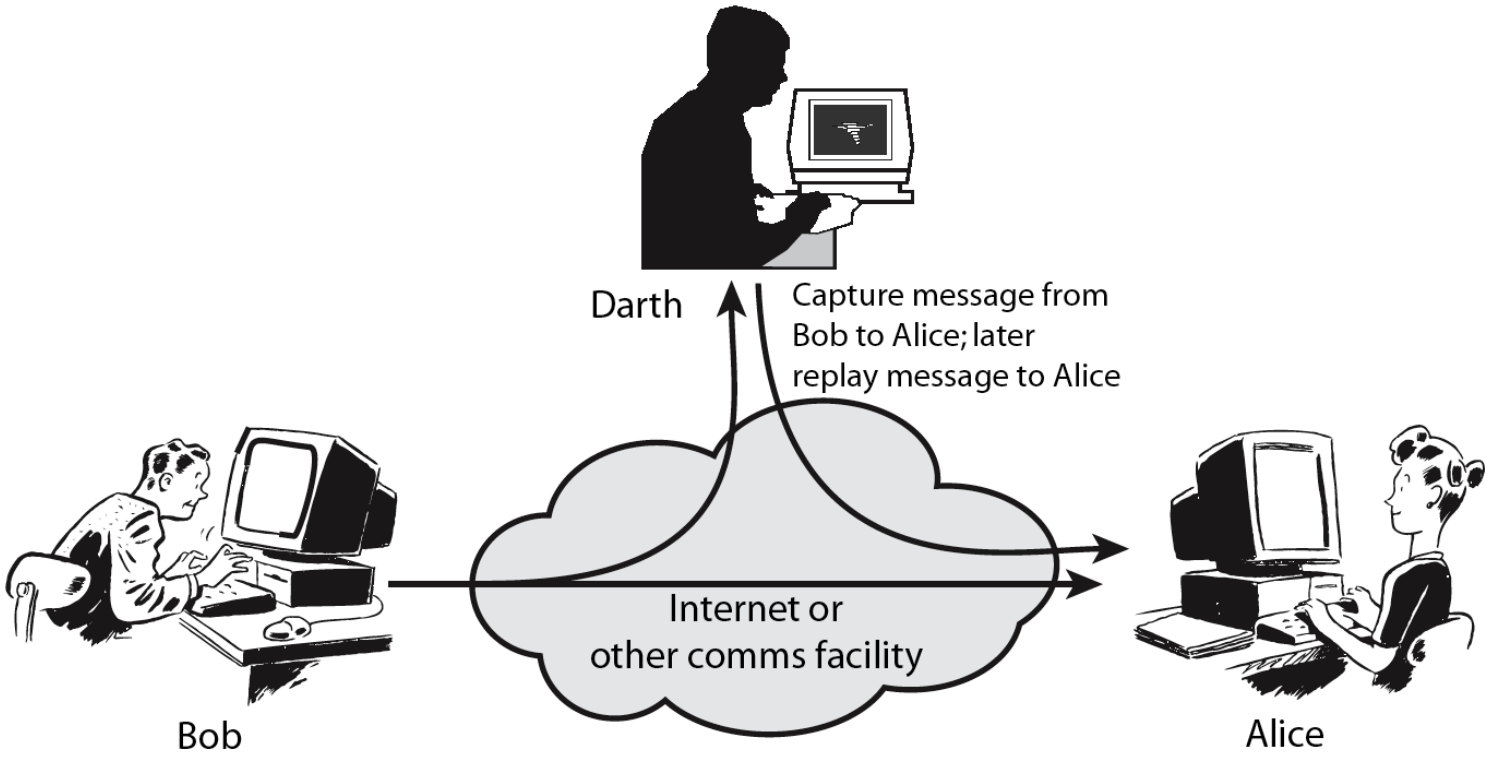
# Passive Attacks



# Passive Attacks

- Attempts to learn or make use of information from the system but does not affect system resources.
- In the nature of eavesdropping on, or monitoring of, transmissions.
  - release of message contents
  - traffic analysis
    - monitor traffic flow to determine location and identity of communicating hosts and could observe the frequency and length of messages being exchanged

# Active Attacks



# Active Attacks

- involve some modification of the data stream or the creation of a false stream
  - masquerade of one entity as some other
  - replay previous messages
  - modify/alter (part of) messages in transit to produce an unauthorized effect
  - denial of service
    - prevents or inhibits the normal use or management of communications facilities

# Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

# Security Services

- X.800
  - a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- RFC 2828
  - a processing or communication service provided by a system to give a specific kind of protection to system resources

# Security Services (X.800)

- Authentication
  - assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication
- Access Control
  - prevention of the unauthorized use of a resource
- Data Confidentiality
  - protection of data from unauthorized disclosure
- Data Integrity
  - assurance that data received is as sent by an authorized entity
- Non-Repudiation
  - protection against denial by one of the parties in a communication
- Availability
  - resource accessible/usable

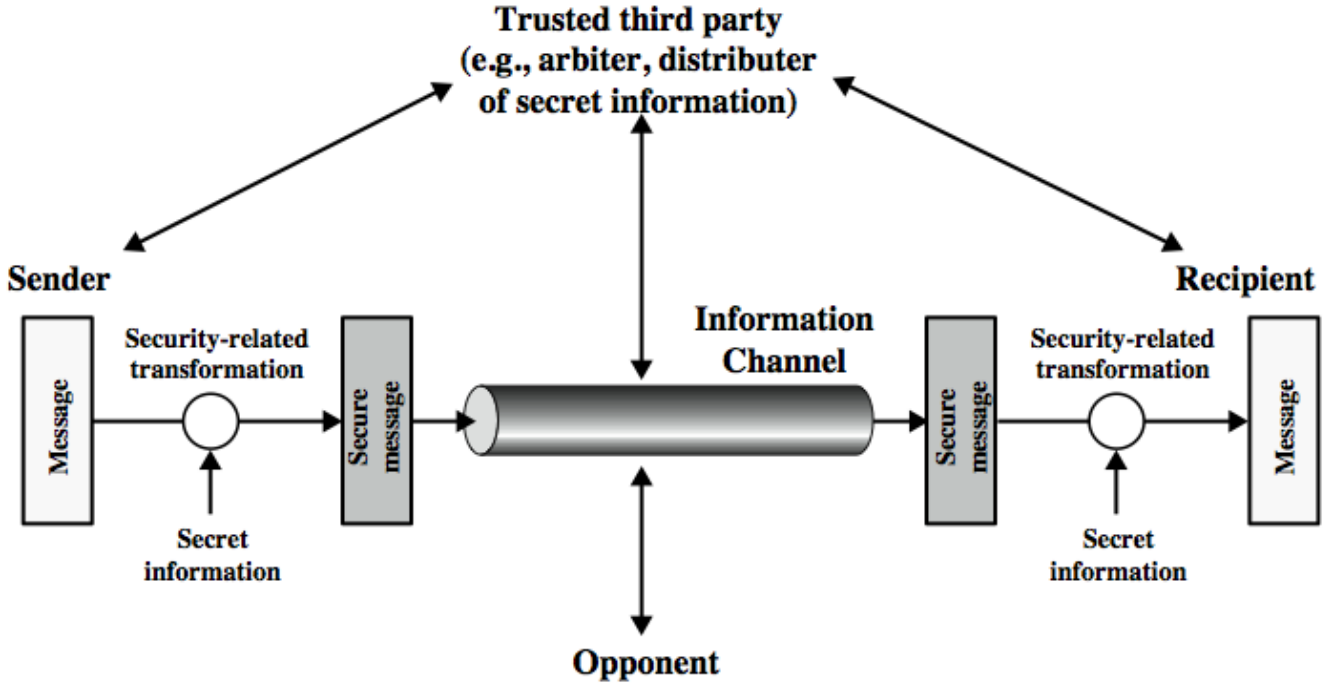
# Security Mechanism

- feature designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all services required
- however one particular element underlies many of the security mechanisms in use:
  - cryptographic techniques
- hence our focus on this topic

# Security Mechanisms (X.800)

- specific security mechanisms
  - protocol layer specific
  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- pervasive security mechanisms
  - trusted functionality, security labels, event detection, security audit trails, security recovery

# Encryption for Network Security

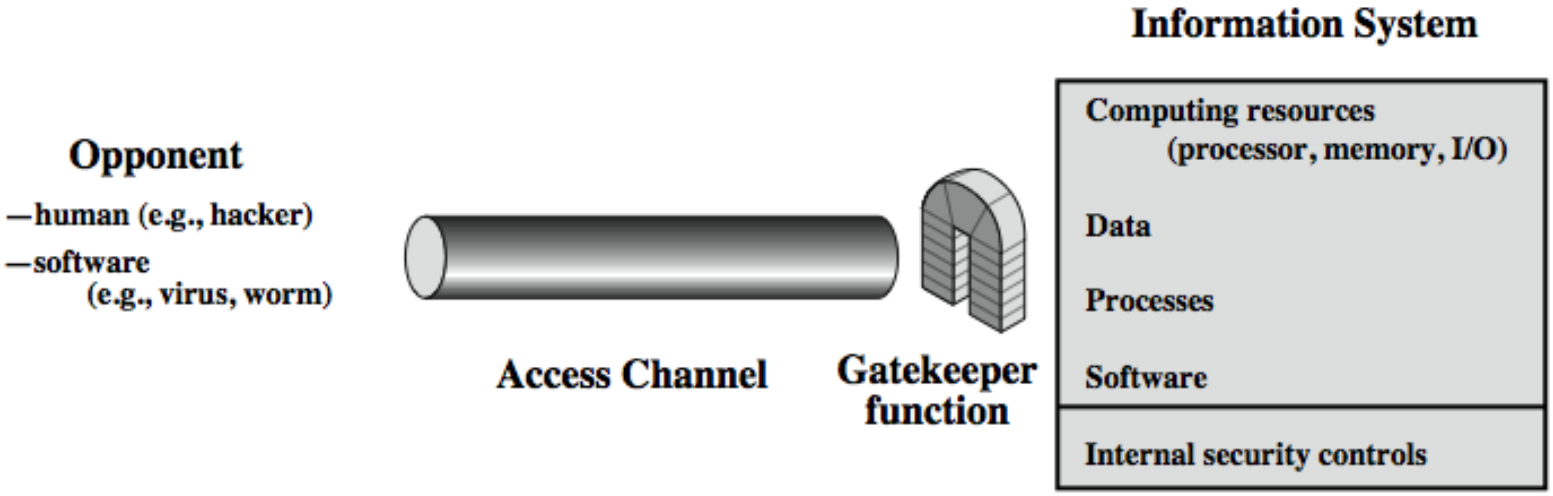



› They can use an appropriate security transform (encryption algorithm), with suitable keys, possibly negotiated using the presence of a trusted third party.

# Encryption for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

# Model for Network Access Security



# Model for Network Access Security

- gatekeeper function
  - password-based login procedures
    - designed to deny access to all but authorized users
  - screening logic
    - designed to detect and reject worms, viruses, and other similar attacks
- internal controls
  - monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders.

# Model for Network Access Security

› using this model requires us to:
  – select appropriate gatekeeper functions to identify users
  – implement security controls to ensure only authorised users access designated information or resources

# Summary

- topic roadmap & standards organizations
- security concepts:
  - confidentiality, integrity, availability
- X.800 security architecture
- security attacks, services, mechanisms
- models for network (access) security