澳門理工大學
Universidade Politécnica de Macau
Macao Polytechnic University

COMP412: Computer Security

Introduction

Dr. Kim, Song-Kyoo (Amang)
Associate Professor,

Computing Program
MACAO POLYTECHNIC UNIVERSITY
Macau, SAR

Agenda

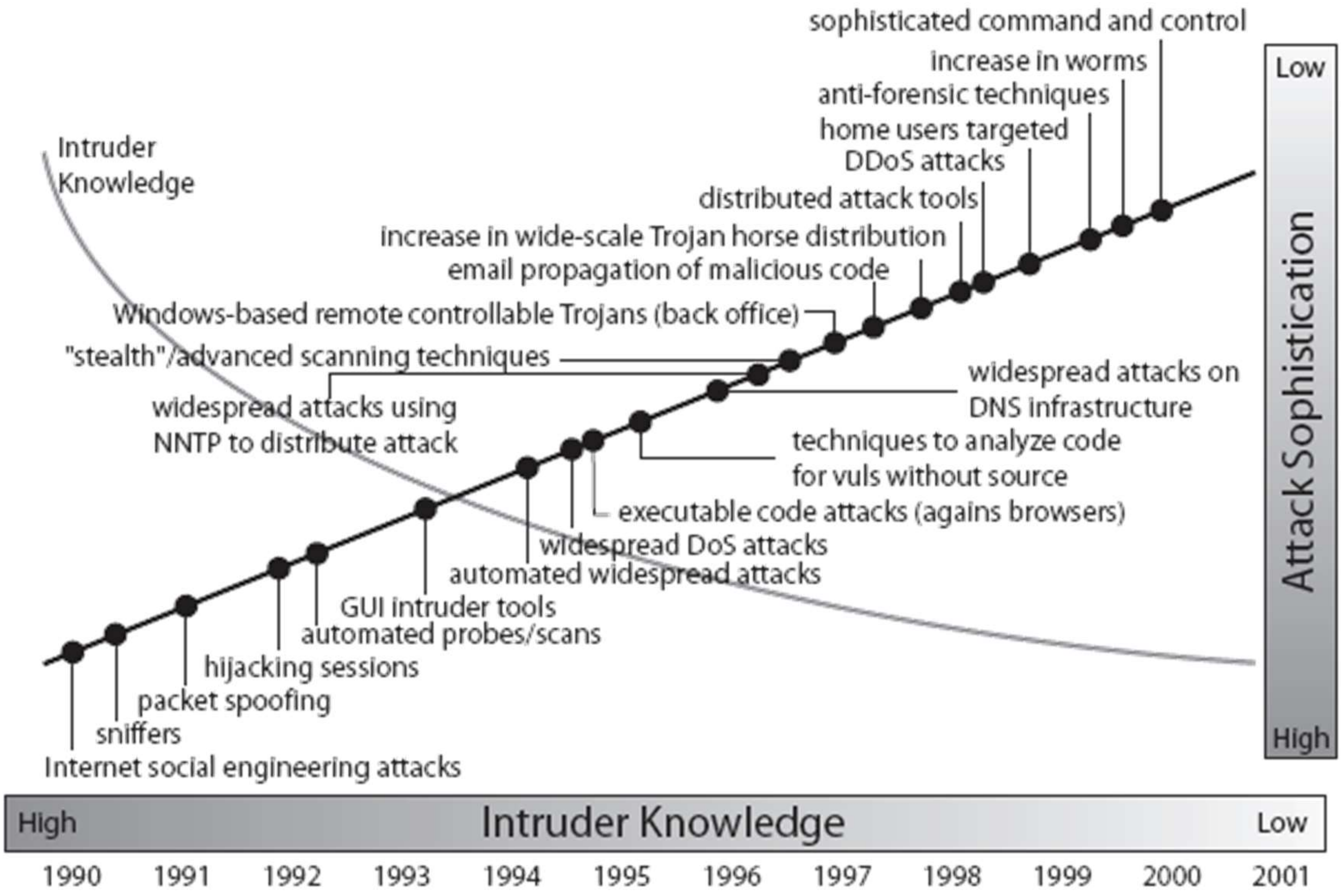
- Definition and Objectives
- The OSI Security Architecture
- Security Models
- Some Cryptography Terms
- Model of Network Security
- Symmetric Cipher Model
- Classical Ciphers

Computer Security

- Information is a strategic resources
  - Stored and processed within a computer
  - Transferred between computers

- Situations that you need security
  - Capture sensitive information and read by unauthorized party
  - Intercept a message, alter the content and then forward it to receiver
  - Construct a malicious message and send to receiver
  - Delay a message delivered to the receiver
  - Deny what you have done

Security Trends



Source: CERT

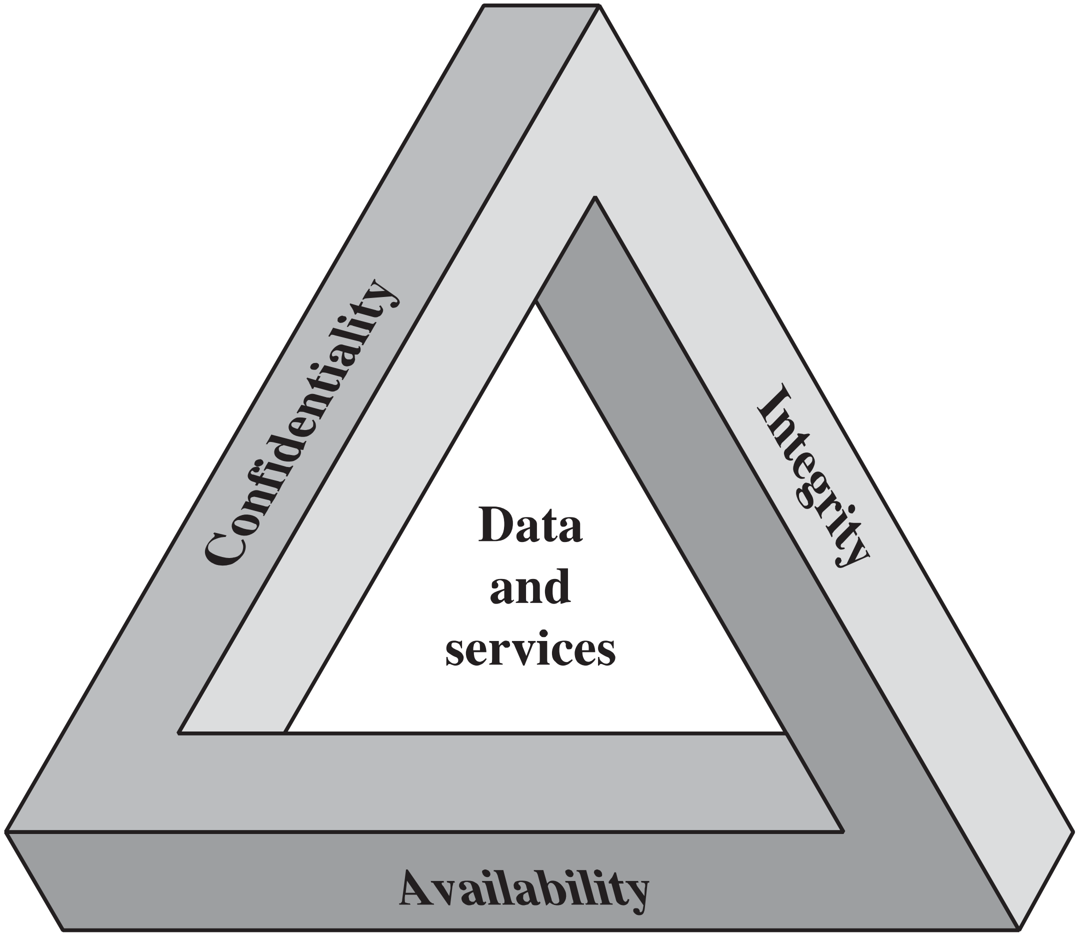
Definition of Computer Security (1/4)

- 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.
  - Confidentiality
  - Integrity
  - Availability

- It includes hardware, software, firmware, information/ data, and telecommunications.

Definition of Computer Security (2/4)

- Objectives of Computer Security (**CIA triad**)



Definition of Computer Security (3/4)

- Confidentiality
  - **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
  - **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.

Definition of Computer Security (4/4)

- **Integrity**
  - **Data integrity:** Assures that information and programs are changed only in a specified and authorized manner.
  - **System integrity:** Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
- **Availability**
  - Assures that systems work promptly and service is not denied to authorized users.

Additional Concepts (1/3)

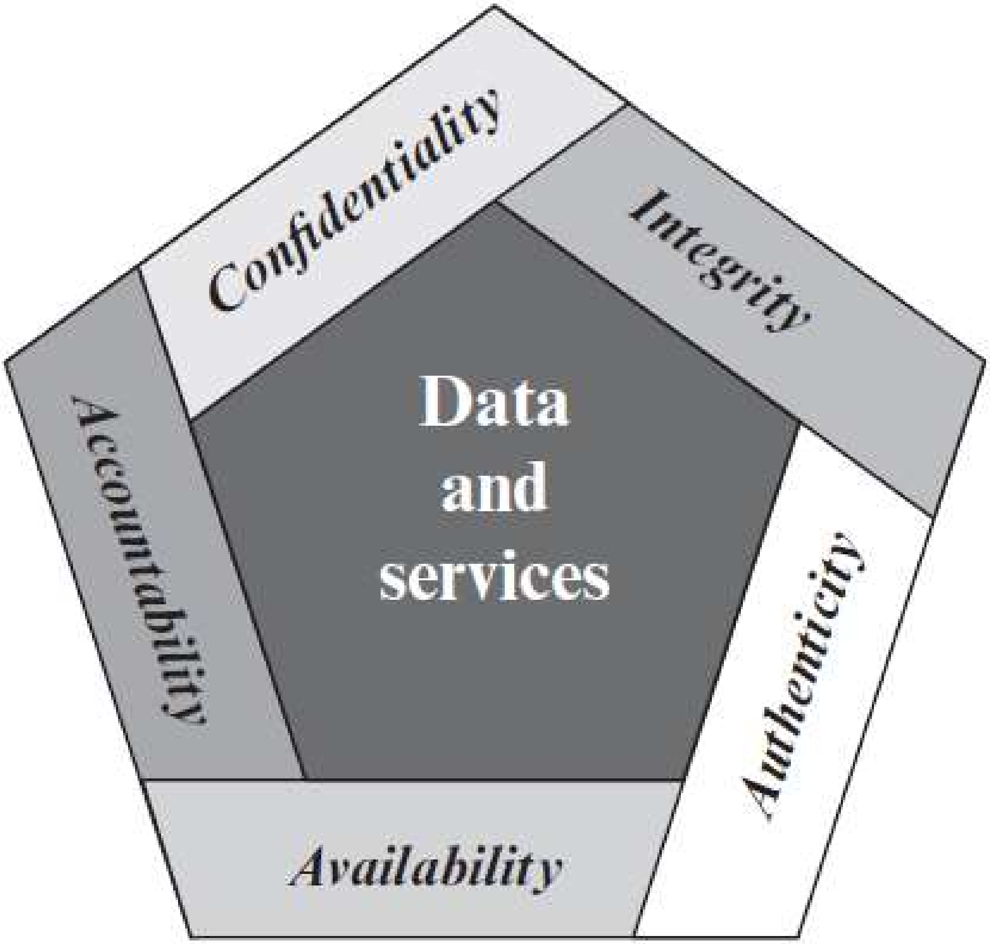
- **Authenticity**
  - The property of being genuine and being able to be verified and trusted;
  - Confidence in the validity of a transmission, a message, or message originator.
  - This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Additional Concepts (2/3)

- **Accountability**
  - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
  - Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party.
  - Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Additional Concepts (3/3)

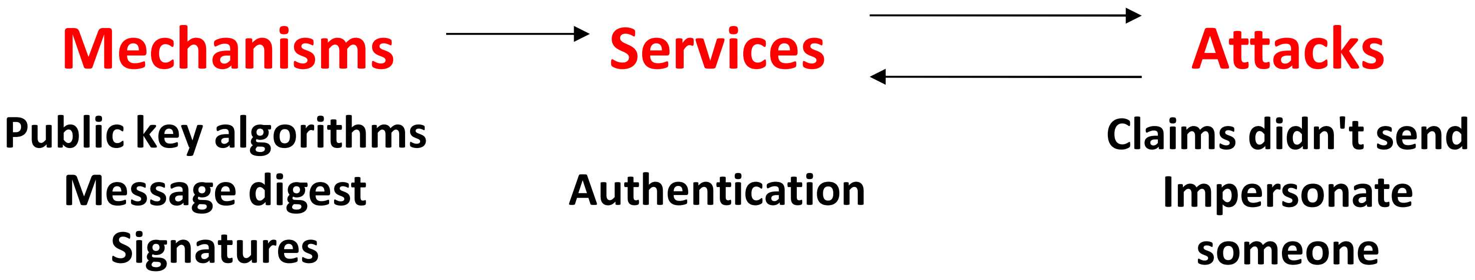
- Computer Security Requirements (**CIA+**)



OSI Security Architecture

- To assess the security needs and evaluate various security products, we need a systematic way of defining requirements for security and characterizing the approaches to meet security requirements.

- Three aspects of information security will be considered.



Mechanisms → **Services** ⇄ **Attacks**

Public key algorithms
Message digest
Signatures

Authentication

Claims didn't send
Impersonate someone

Computer Security (1/3)

- Security Attacks
  - Any action that compromises the security of information owned by an organization
  - Information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems.
  - There are wide range of attacks and we focuses on generic types of attacks - password cracking, etc.
  - Note: threat & attack are almost same.

Computer Security (2/3)

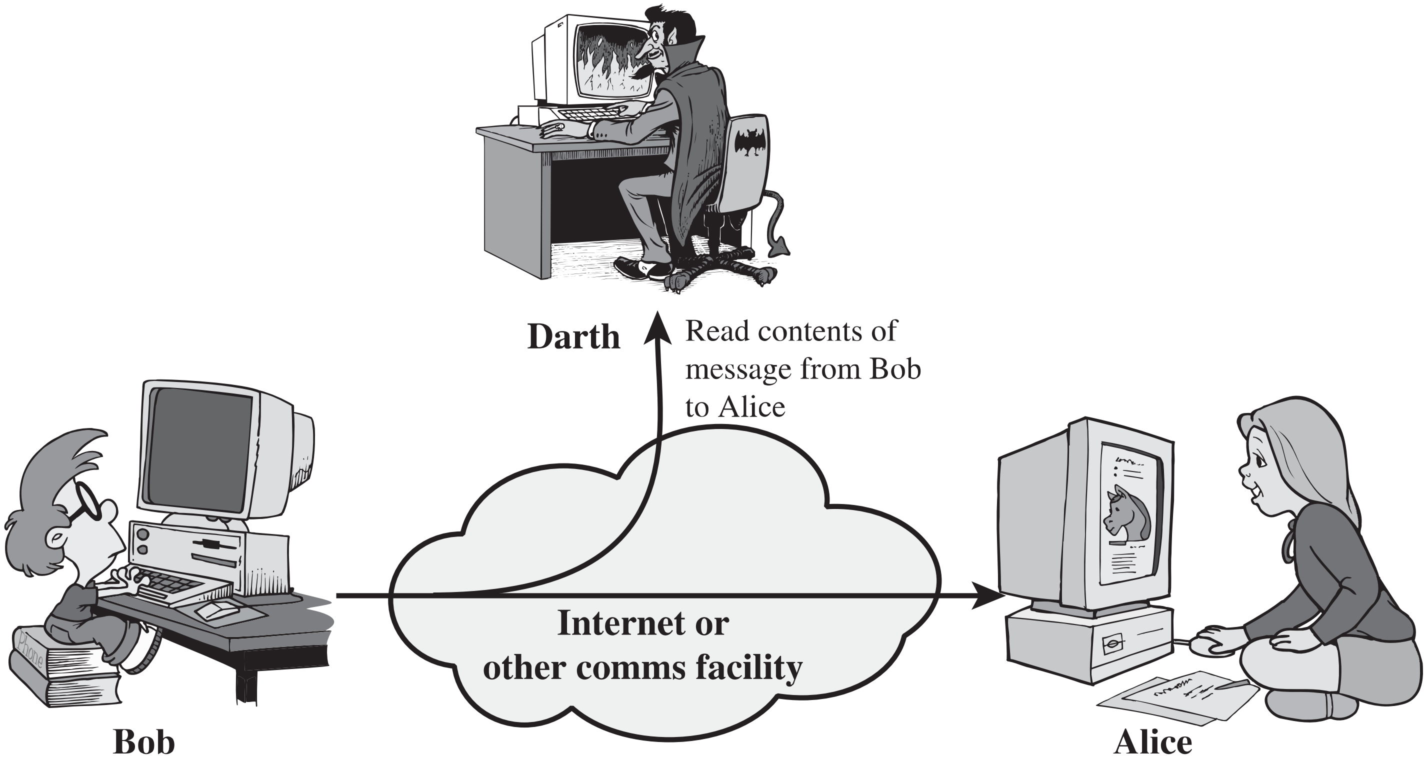
- Threat
  - A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
  - A threat is a possible danger that might exploit a vulnerability.
- Attack
  - An assault on system security that derives from an 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

Computer Security (3/3)

- Passive attacks
  - Release of message contents
  - Traffic analysis
- Active attacks
  - Masquerade
  - Replay
  - Modification of messages
  - Denial of services

Passive Attack (1/2)

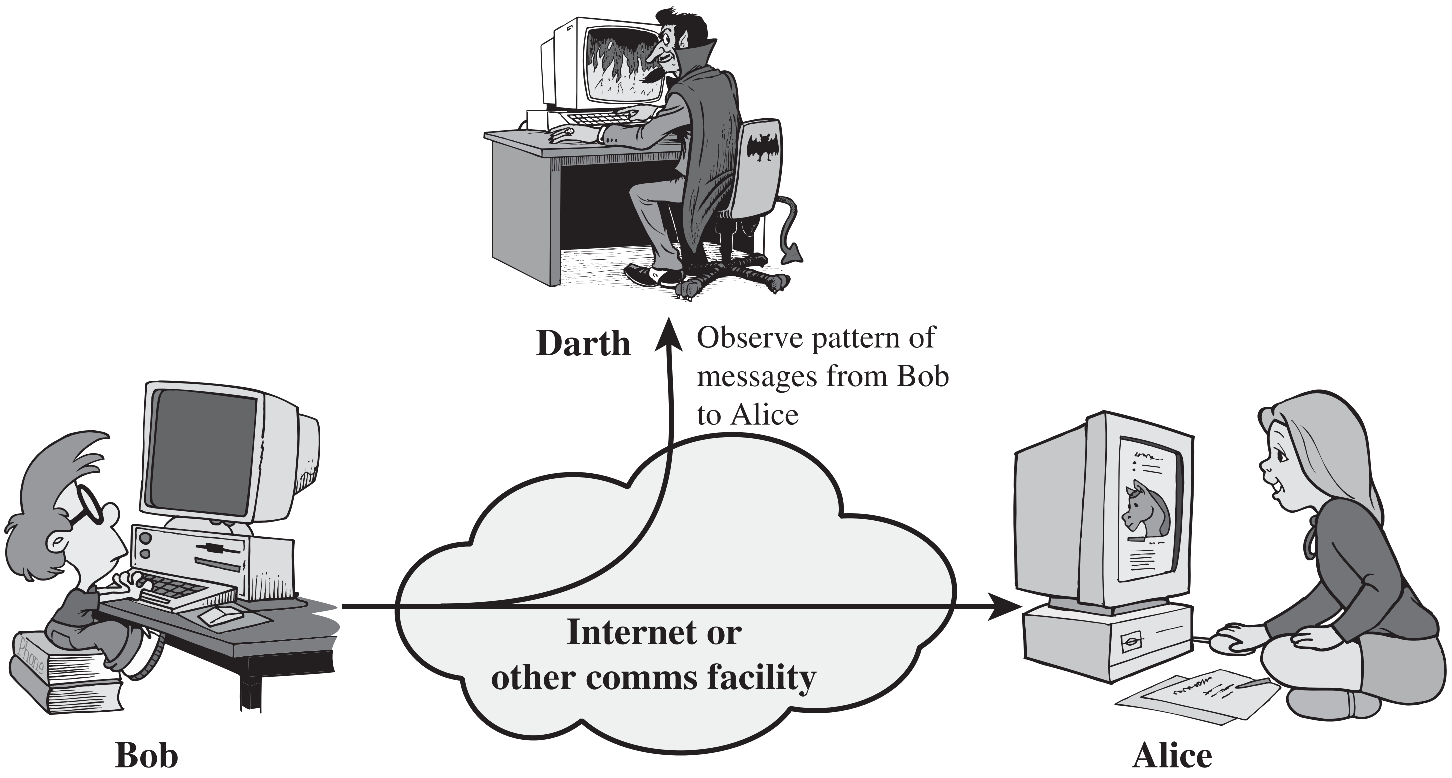
- Release of message contents


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

(a) Release of message contents

Passive Attack (2/2)

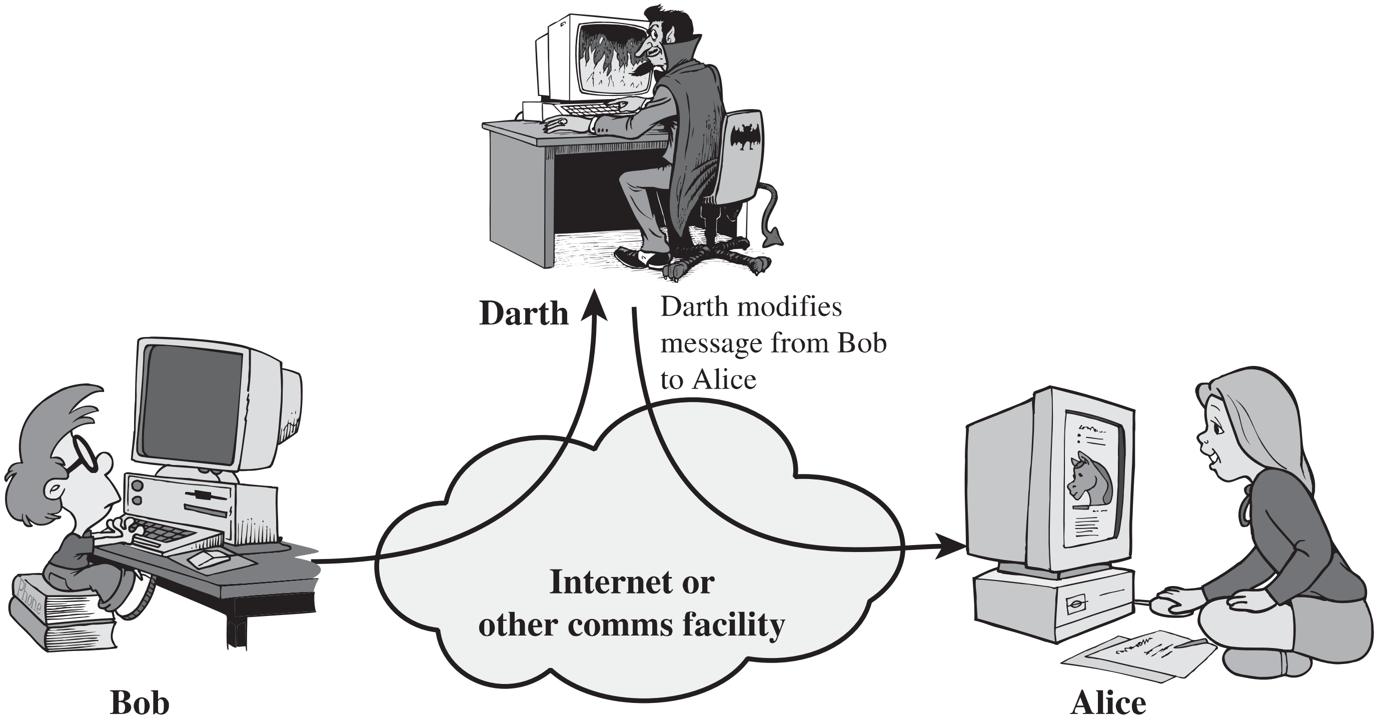
- Traffic analysis


Darth
Observe pattern of messages from Bob to Alice
Bob
Internet or other comms facility
Alice
Phone

(b) Traffic analysis

Active Attack (1/2)

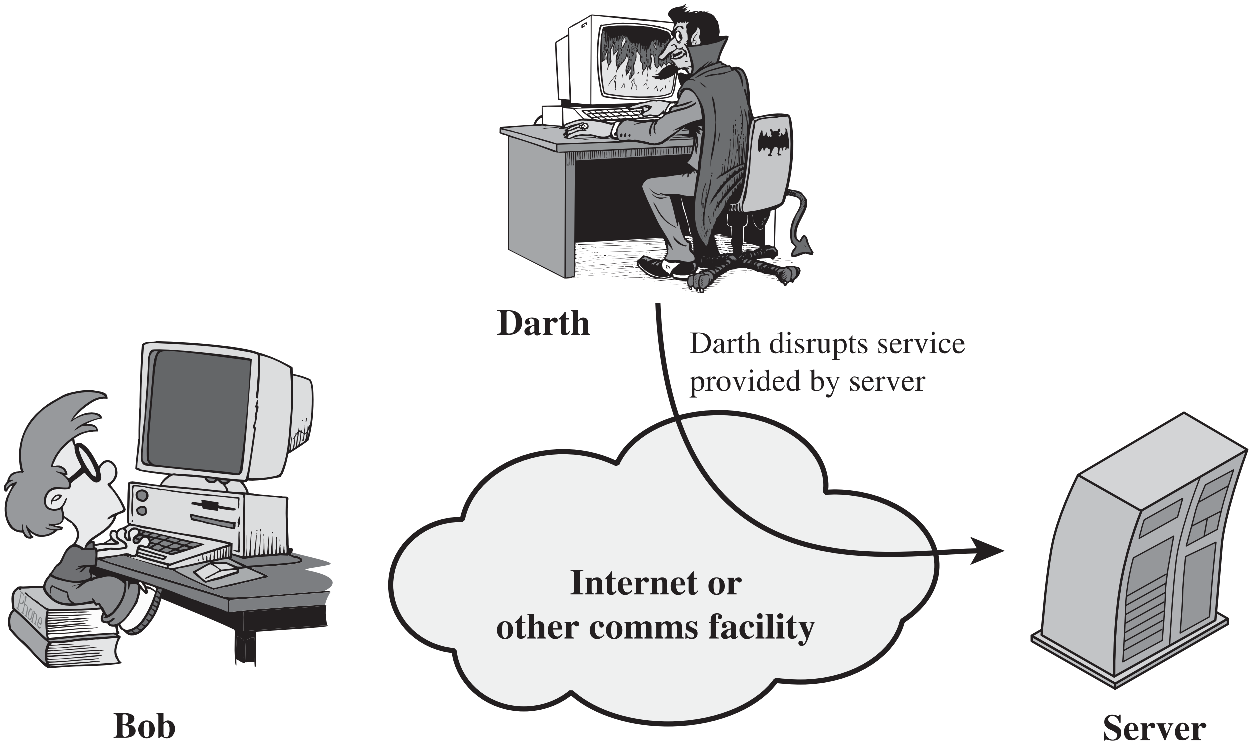
- Modification of message


Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

(c) Modification of messages

Active Attack (2/2)

- Denial of service



(d) Denial of service

Passive & Active Attack

- Response to Attacks
  - Identify key assets
  - Evaluate threat posed to assets
  - Implement suitable countermeasures
  - Manage implementation of Security services

Security Services (1/3)

- Security services normally associated with physical documents
  - Include signatures, dates; Protect from disclosure, tampering, or destruction; be witnessed; be recorded or licensed.
- Intended to counter security attacks.
- Enhances the security of the data processing systems and the information transfers of an organization.
- Make use of one or more security mechanisms to provide the security services.

Security Services (2/3)

- International Telecommunication Union – Telecommunication Standardization Sector (ITU-T) X.800 Security Architecture for Open System Interconnection (OSI) defines a systematic way of defining and providing security requirements.
- The OSI security architecture is useful to managers as a way of organizing the task of providing security.
- It provides a useful overview of concepts.

Security Services (3/3)

- **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.
- X.800 defines it in **5 major categories**

X.800 Security Service (1/3)

- **Confidentiality**
  - protection of data from unauthorized disclosure
- **Integrity**
  - assurance that data received is as sent by an authorized entity
- **Authentication**
  - assurance that the communicating entity is the one claimed
- **Access Control**
  - prevention of the unauthorized use of a resource
- **Non-Repudiation**
  - protection against denial by one of the parties in a communication

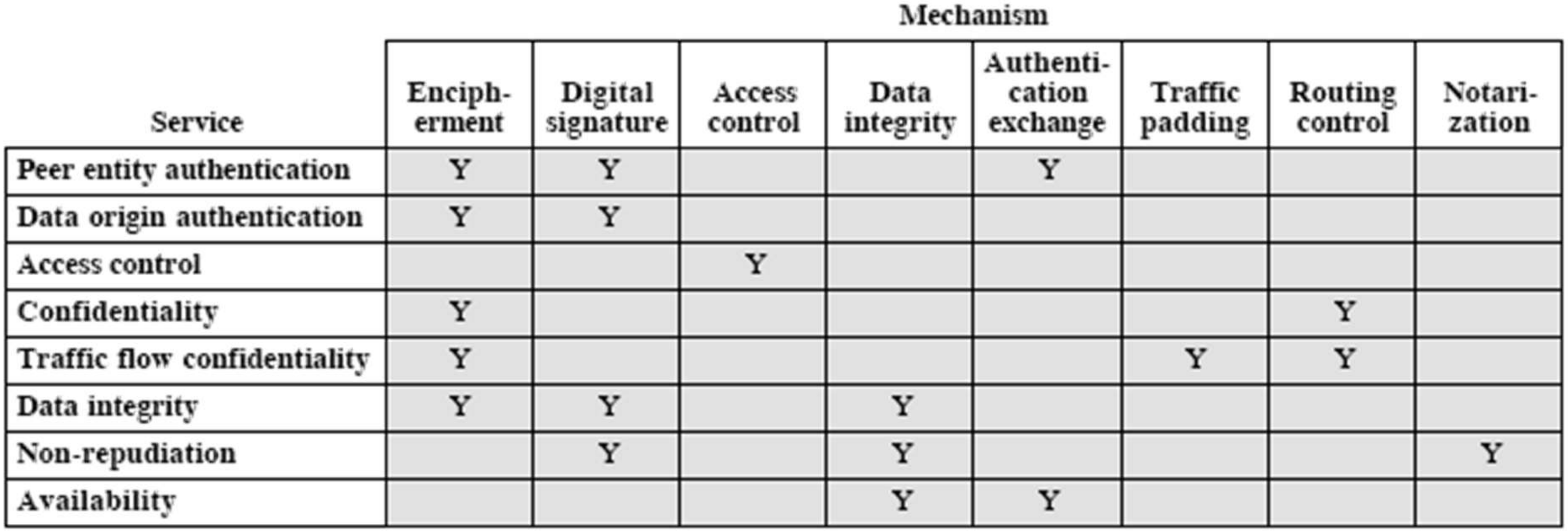
X.800 Security Service (2/3)

- Security Mechanisms
  - A mechanism that is designed to detect, prevent, or recover from a security attack
  - No single mechanism that will support all functions required
  - However one particular element underlies many of the security mechanisms in use: cryptographic techniques (Hence we focus on this area)
- Specific security mechanisms
  - May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services
  - Decipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, Notarization

X.800 Security Service (3/3)

- Pervasive security mechanisms
  - Mechanisms that are not specific to any particular OSI security service or protocol layer
  - Trusted functionality, security labels, event detection, security audit trails, security recovery.

- Security Services and Mechanisms



	Mechanism							
Service	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				
Non-repudiation		Y		Y				Y
Availability				Y	Y			

Some Cryptography Terms (1/3)

- **Cryptography**
  - The study of secret (crypto-) writing (-graphy)
  - The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and retransforming that message back to its original form
- **Cryptanalysis (code-breaking)**
  - The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key.
- **Cryptology**
  - The field encompassing both cryptography and cryptanalysis

Some Cryptography Terms (2/3)

- **Cipher**
  - An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods

- **Encipher (encode)**
  - The process of converting plaintext to ciphertext using a cipher and a key

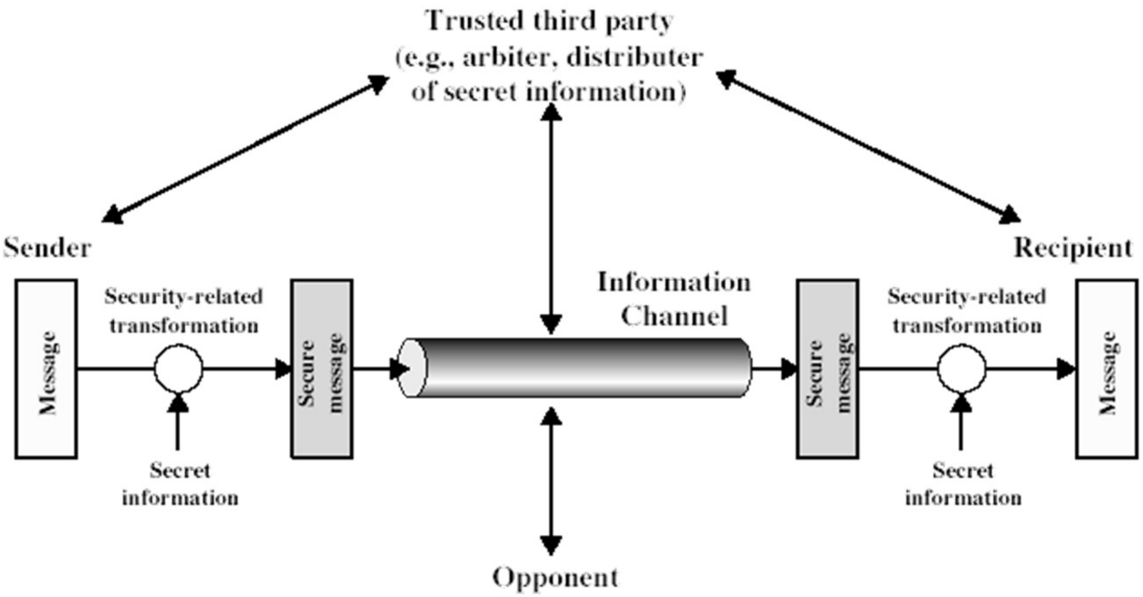
- **Decipher (decode)**
  - The process of converting ciphertext back into plaintext using a cipher and a key

Some Cryptography Terms (3/3)

- Encryption
  - The mathematical function mapping plaintext to ciphertext using the specified key: C = EK(P)
- Decryption
  - The mathematical function mapping ciphertext to plaintext using the specified key: P = EK^{-1} (C)=DK(C)
- Plaintext
  - The original intelligible message.
- Ciphertext
  - The transformed message.
- Key (Password)
  - Some critical information used by the cipher, known only to the sender & receiver.

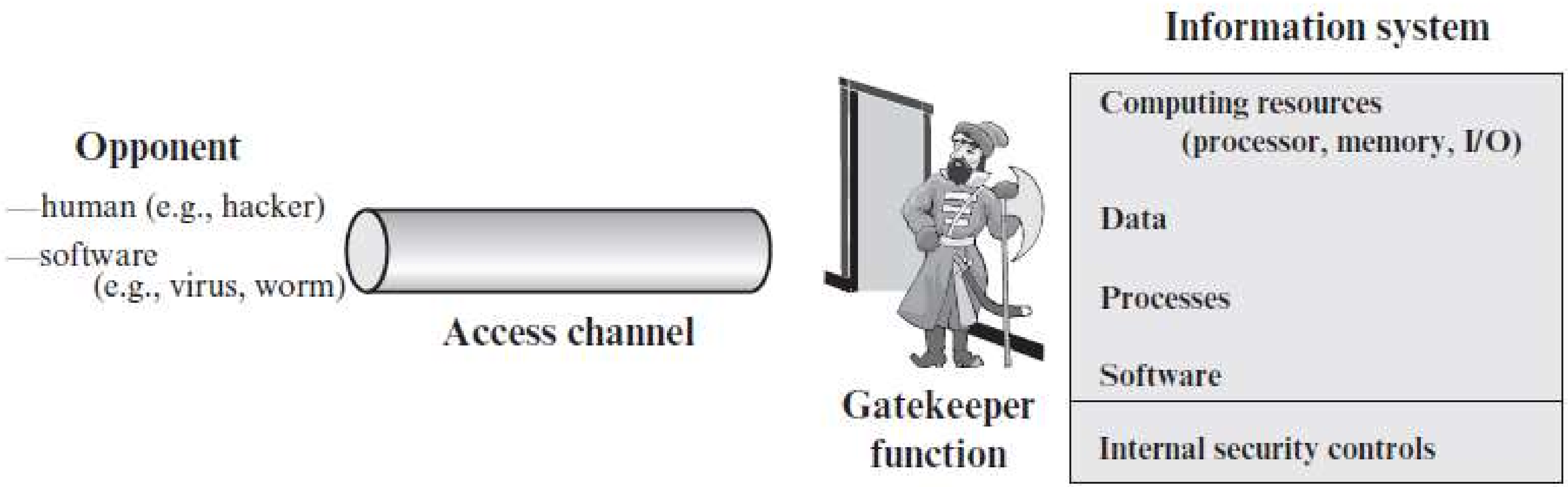
Model for Network Security

- Using this model, four basic tasks are required in designing a particular security service
  - Design an algorithm for the security transformation
  - Generate the secret information used by the algorithm
  - Develop methods to distribute the secret information
  - Specify a protocol enabling the two principals to use the transformation & secret info for a security service.



Model for Network Access Security

- **The gatekeeper function:** It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks.



澳門理工學院
INSTITUTO POLITÉCNICO DE MACAU
MACAO POLYTECHNIC INSTITUTE