Introduction to Information Security

Assoc Prof. Nguyễn Linh Giang

Department of Data Communications and Computer Networks

Course outline

Introduction

Symmetric Key Ciphers

Public Key Crypto Systems

Message Authentication

Digital Signature

Authentication Protocols

Digital Watermarking

Reading

- References:
  - W. Stallings “Networks and Internetwork security”
  - W. Stallings “Cryptography and network security”
  - Introduction to Cryptography – PGP
  - D. Stinson – Cryptography: Theory and Practice

Grading

- Mid-term test and Project: 30%
  - Lecture attendance: 1/3.
- Exam: 70%

- Contact:
  - email: giangnl@soict.hust.edu.vn
  - Tel: 04 38682596; Cellphone:0984933165

Project themes

- 1. Public key crypto systems.
  - Basics of Public key cryptographic algorithms
  - Public key crypto systems.
  - Applications of Public key crypto systems.
- 2. Public Key Infrastructure (PKI)
  - Structure of PKI
  - Digital Certificate, Standards;
  - Deployment of PKI. Applications of PKI in electronic transactions;
  - Open source CA.

Project themes

- 3. Security of IP networks. IPSec protocol. Virtual Private Network (VPN). Applications.
- 4. Message authentication
  - Mechanisms of message authentication;
  - Hash functions and Message authentication functions;
  - Authentication protocols.
- 5. Digital signature
  - Mechanisms of digital signature generation;
  - Digital signature protocols;
  - Digital signature service;
  - Blind signature;
  - Applications

Project themes

- 6. Wireless LAN security;
  - Attacks to WLAN
  - Secure WLAN
  - Authentication protocols for WLAN security
- 7. System security and network security.
  - Policies and standards;
  - Security of Windows and Unix-Linux;
  - Cisco network security policy.
- 8. Web service security;

- 9. Single sign on with OpenID;
- 10. Kerberos authentication protocol;
- 11. SSL/TLS and applications;

Project themes

- 12. PGP and secure email
- 13. Secure electronic transaction
- 14. Firewall and Proxy;
- 15. Digital certificate X509;
- 16. IDS, IPS;
- 17. DDoS attacks detection and mitigation ;
- 18. SQL Injection attacks detection and prevention
- 19. System vulnarability detection and prevention
- 20. ISO 27001

Chapter I. Introduction

Examples of security violation

Introduction to Computer and Network Security

The OSI Security Architechture

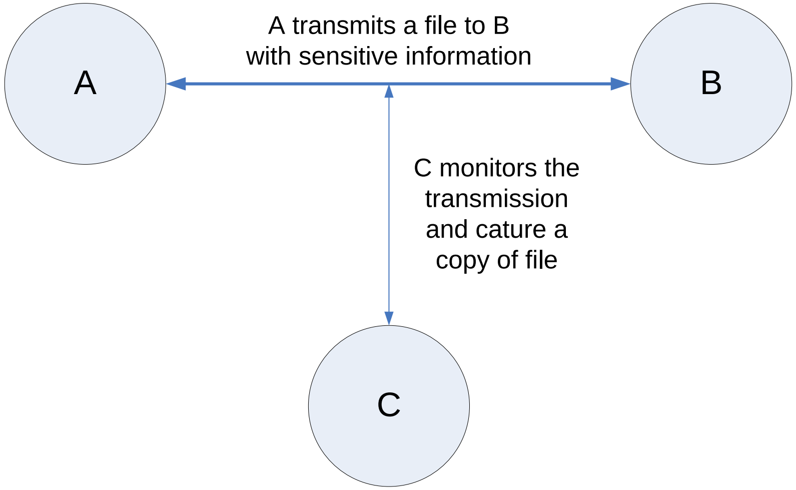
Classification of Security Attacks

Security services

Network security models

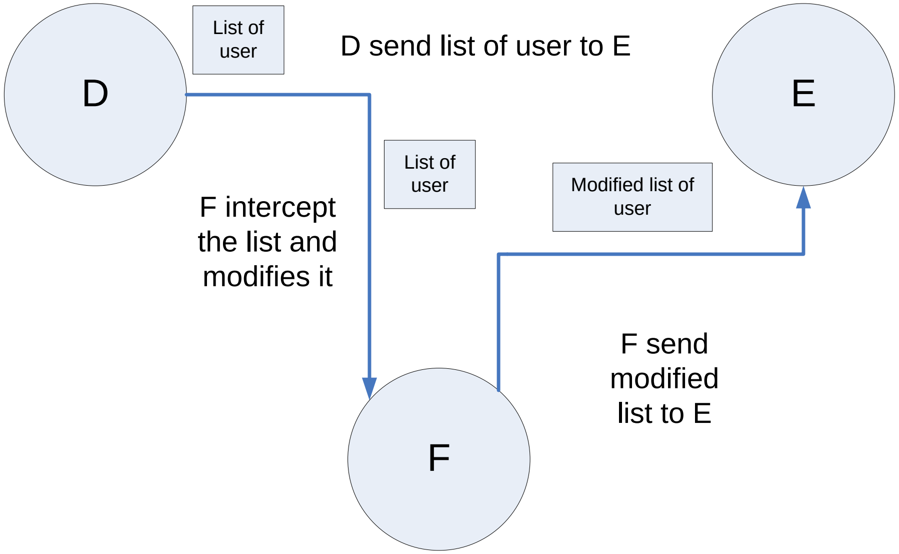
Examples of security violation

- File transfer over the networks
  - Eavesdropping



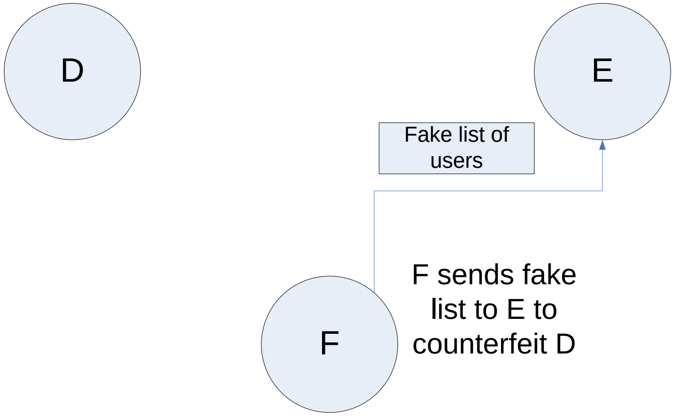
Examples of security violation

- Message interception
  - D – network manager
  - E – computer
  - F intercepts the list



Examples

- Impersonation:
  - F constructs its fake message
  - F transmits fake message as if had come from D



Introduction to Computer security

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

Introduction to Computer security

- Three key objectives of computer security:
  - **Confidentiality:** Preserving authorized restrictions on information access and disclosure;
  - **Integrity:** Guarding against improper information modification or destruction;
  - **Availability:** Assures that systems work promptly and service is not denied to authorized users

Introduction to Computer security

- **Confidentiality: This term covers two related concepts:**
  - **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.

Introduction to Computer security

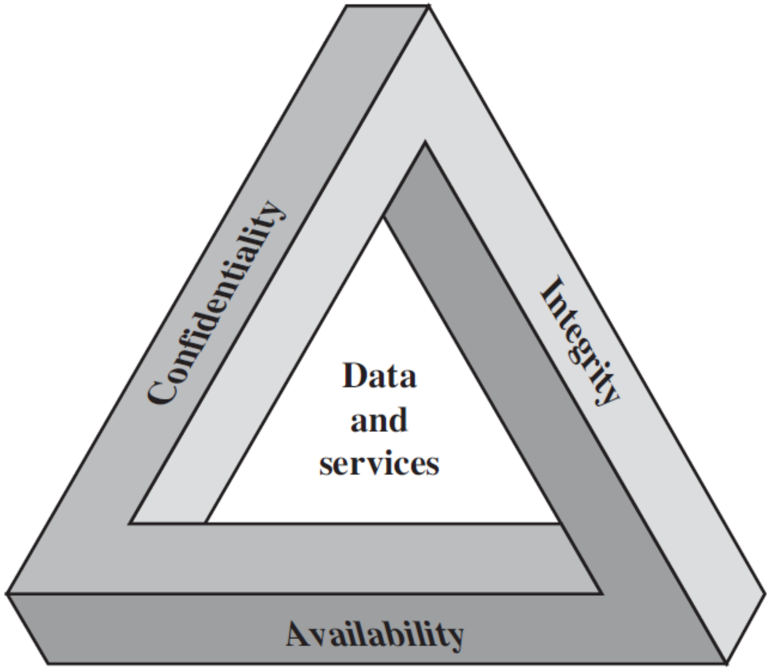
- Integrity: This term covers two related concepts:
  - **Data integrity: Assures that information and programs are changed only in** a specified and authorized manner.
  - **System integrity: Assures that a system performs its intended function in an** unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Introduction to Computer security

- Availability: Assures that systems work promptly and service is not denied to authorized users
  - 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.

Introduction to Computer security

- The security requirement triad:
  - These three concepts form what is often referred to as the **CIA triad**
  - The three concepts embody the fundamental security objectives for both data and for information and computing services.



Introduction to Computer security

- **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**,** including ensuring information nonrepudiation and authenticity.
  - A loss of integrity is the unauthorized modification or destruction of information.

Introduction to Computer security

- **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.

Introduction to Computer security

- **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.

Introduction to Computer security

- **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.

Introduction to Computer security

- Examples: three levels of impact on organizations:
- **Low:** The loss could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
  - A limited adverse effect means that, the loss of confidentiality, integrity, or availability might
    - (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced;
    - (ii) result in minor damage to organizational assets;
    - (iii) result in minor financial loss; or
    - (iv) result in minor harm to individuals

Introduction to Computer security

- **Moderate:** The loss could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
  - A serious adverse effect means that, for example, the loss might
    - (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced;
    - (ii) result in significant damage to organizational assets;
    - (iii) result in significant financial loss; or
    - (iv) result in significant harm to individuals that does not involve loss of life or serious, life-threatening injuries.

Introduction to Computer security

- **High:** The loss could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
  - A severe or catastrophic adverse effect means that, for example, the loss might
    - (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
    - (ii) result in major damage to organizational assets;
    - (iii) result in major financial loss; or
    - (iv) result in severe or catastrophic harm to individuals involving loss of life or serious, life-threatening injuries.

Introduction to Computer security

- The Challenges of Computer and Network security:
  - Security is not simple task:
    - The requirements seem to be straightforward: confidentiality, authentication, nonrepudiation, or integrity.
    - The mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.
  - In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
  - Because of previous point, the procedures used to provide particular services are often counterintuitive.Typically, a security mechanism is complex, and it is not obvious from the statement of a particular requirement that such elaborate measures are needed. It is only when the various aspects of the threat are considered that elaborate security mechanisms make sense.

Introduction to Information security

- Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP should mechanisms be placed].

Introduction to Information security

- Security mechanisms typically involve more than a particular algorithm or protocol.
  - They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information.
  - There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism.
  - For example, if the proper functioning of the security mechanism requires setting time limits on the transit time of a message from sender to receiver, then any protocol or network that introduces variable, unpredictable delays may render such time limits meaningless.

Introduction to Information security

- Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them.
  - The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

Introduction to Information security

- There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs;
- Security requires regular, even constant, monitoring, and this is difficult in today's short-term, overloaded environment;

Introduction to Information security

- Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.
- Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

The OSI Security Architechture

- To assess effectively the security needs of an organization and to evaluate and choose various security products and policies:
  - Security manager needs some systematic way of **defining the requirements for security** and **characterizing the approaches to satisfying those requirements**

The OSI Security Architechture

- ITU-T3 Recommendation X.800, *Security Architecture for OSI*
- The OSI security architecture focuses on:
  - Security attacks: Any action that compromises the security of information owned by an organization
  - Security mechanisms: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack, and
  - Security services: 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.

The OSI Security Architechture

- **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.That is, a threat is a possible danger that might exploit a vulnerability.
- **Attack**
  - An assault on system security that derives from an intelligent threat; that is, 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.

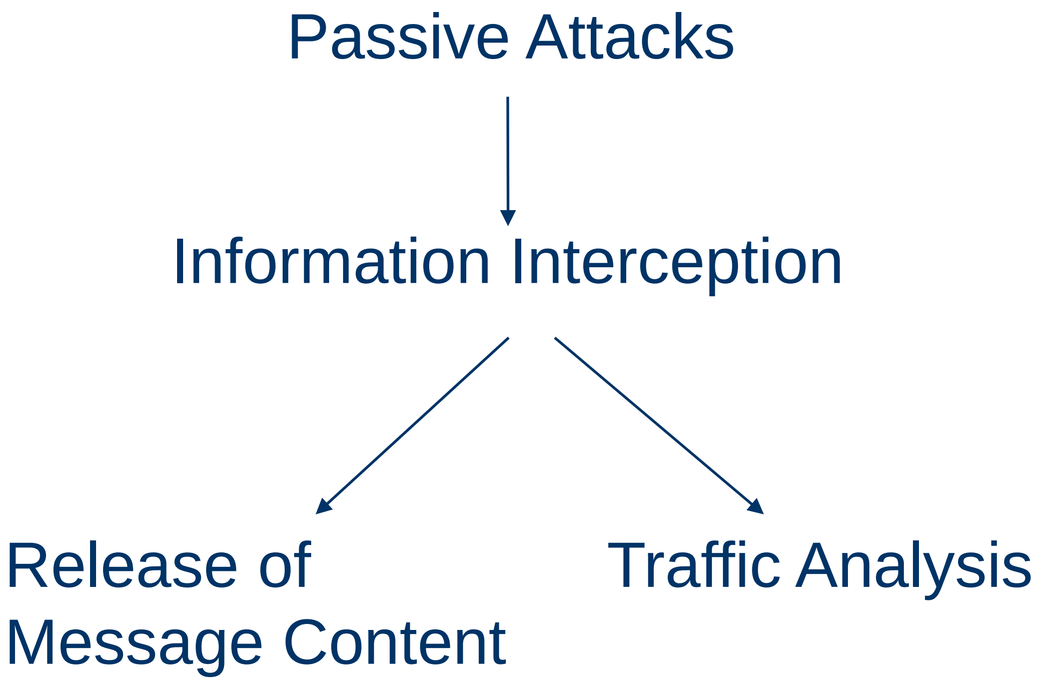
Security Attacks

- Classification of security attacks: in both X.800 and RFC 2828 - *passive attacks and active 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.

Security Attacks

- Passive Attacks:
  - 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.

Security Attacks



Passive Attacks

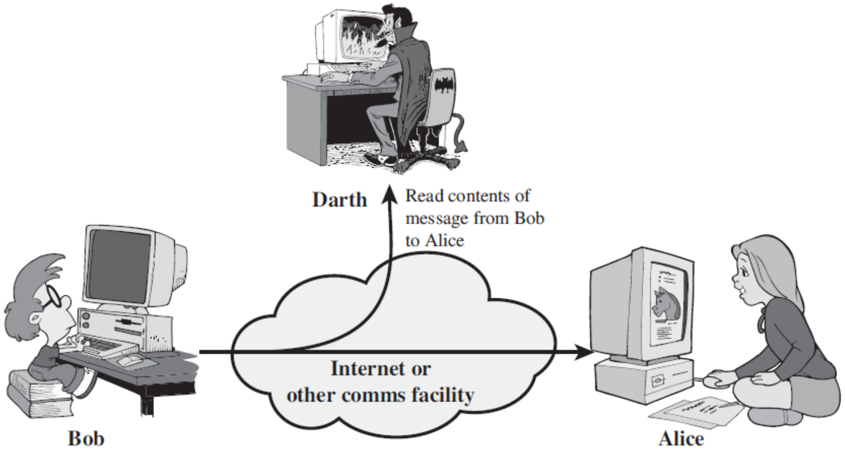
Information Interception

Release of
Message Content

Traffic Analysis

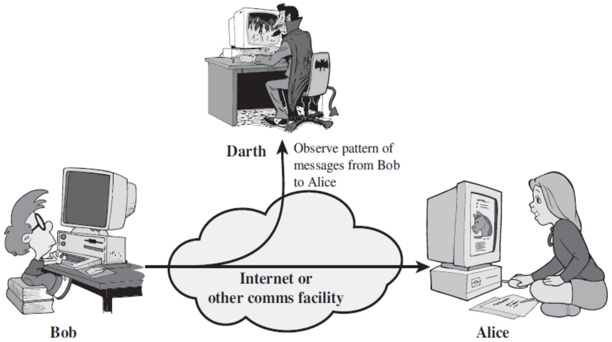
Security Attacks

- 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.


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

Security Attacks

- **Traffic analysis is subtler**
  - 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.
    - If we had encryption protection in place, an opponent might still be able to observe the pattern of these messages:
      - The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged.
      - This information might be useful in guessing the nature of the communication that was taking place.


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

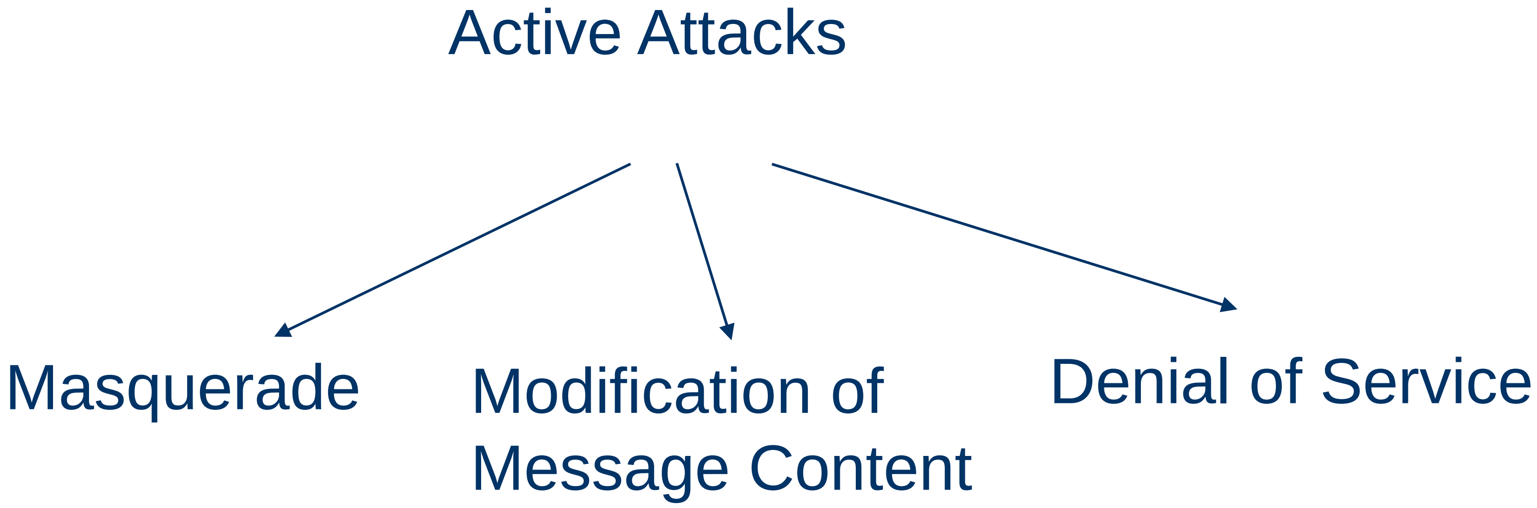
Security Attacks

- Passive attacks:
  - Passive attacks are very difficult to detect, because they do not involve any alteration of the data.
    - Typically, the message traffic is sent and received in an apparently normal fashion, and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern.
  - However, it is feasible to prevent the success of these attacks, usually by means of encryption.
  - Thus, the emphasis in dealing with passive attacks is on prevention rather than detection

Security 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

Security Attacks



Active Attacks

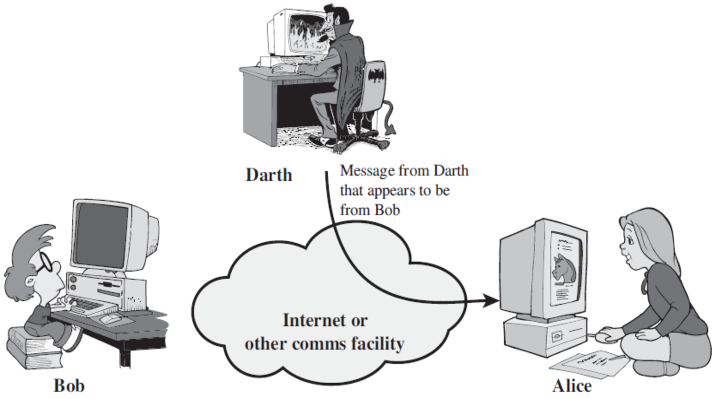
Masquerade

Modification of Message Content

Denial of Service

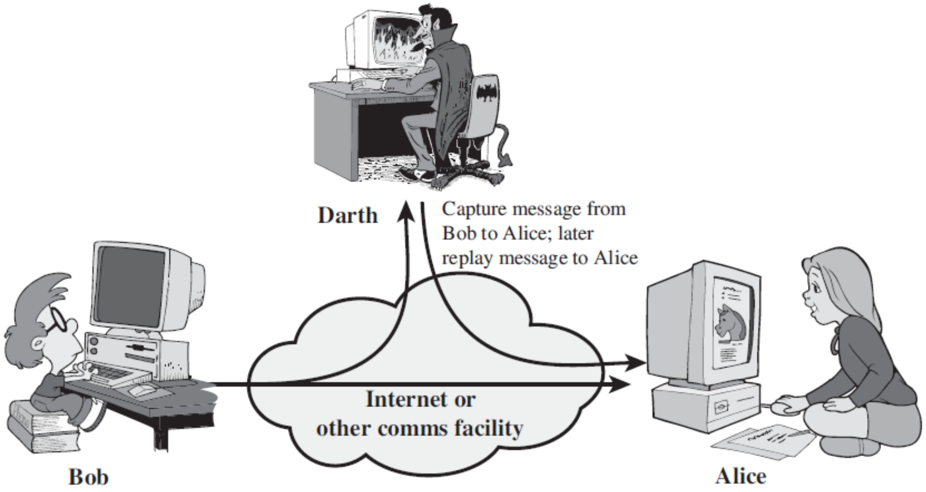
Security Attacks

- M**asquerade:** takes place when one entity pretends to be a different entity
  - A masquerade attack usually includes one of the other forms of active attack.
  - Example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.


Darth
Message from Darth that appears to be from Bob
Internet or other comms facility
Bob
Alice

Security Attacks

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

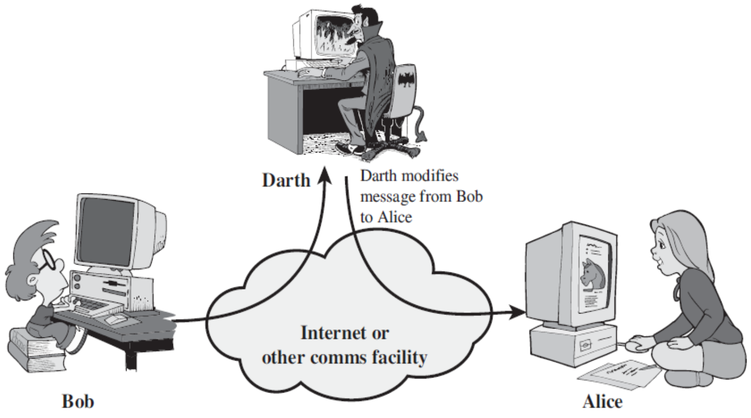

Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Security 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.
  - For example, a message meaning “Allow John Smith to read confidential file *accounts*”

is modified to mean “Allow Fred

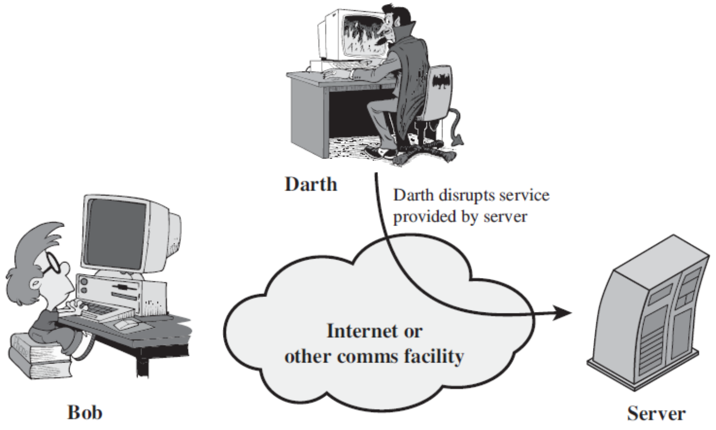
Brown to read confidential file *accounts*


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

(c) Modification of messages

Security Attacks

- **Denial of service**: prevents or inhibits the normal use or management of communications facilities
  - This attack may have a specific target;
  - For example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service).
  - Another 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.


Darth
Darth disrupts service provided by server
Internet or other comms facility
Bob
Server

(d) Denial of service

Security Attacks

- Active attacks present the opposite characteristics of passive attacks.
  - Whereas passive attacks are difficult to detect, measures are available to prevent their success.
- On the other hand, it is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities.
- Instead, the goal is to detect active attacks and to recover from any disruption or delays caused by them.
  - If the detection has a deterrent effect, it may also contribute to prevention.

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.
- Conform to RFC 2828: 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

Security Services

- X.800 divides these services into five categories and fourteen specific services:
  - Authentication
  - Data Integrity
  - Access Control
  - Data Confidentiality
  - Non-Repudiation

Security Services

- AUTHENTICATION
  - The assurance that the communicating entity is the one that it claims to be.
  - Peer Entity Authentication
    - Used in association with a logical connection to provide confidence in the identity of the entities connected.
  - Data-Origin Authentication
    - In a connectionless transfer, provides assurance that the source of received data is as claimed.

Security Services

- ACCESS CONTROL
  - The prevention of unauthorized use of a resource
    - This service controls who can have access to a resource,
    - Under what conditions access can occur,
    - What those accessing the resource are allowed to do

Security Services

- DATA CONFIDENTIALITY
  - The protection of data from unauthorized disclosure.
  - Connection Confidentiality
    - The protection of all user data on a connection.
  - Connectionless Confidentiality
    - The protection of all user data in a single data block
  - Selective-Field Confidentiality
    - The confidentiality of selected fields within the user data on a connection or in a single data block.
  - Traffic-Flow Confidentiality
    - The protection of the information that might be derived from observation of traffic flows.

Security Services

- DATA INTEGRITY
  - The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
  - Connection Integrity with Recovery
    - Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Security Services

- Connection Integrity without Recovery
  - As above, but provides only detection without recovery
- Selective-Field Connection Integrity
  - Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Security Services

- Connectionless Integrity
  - Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.
- Selective-Field Connectionless Integrity
  - Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

Security Services

- NONREPUDIATION
  - Provides protection against denial by one of theentities involved in a communication of havingparticipated in all or part of the communication.
  - Nonrepudiation, Origin
    - Proof that the message was sent by the specified party.
  - Nonrepudiation, Destination
    - Proof that the message was received by the specified party.

Security Mechanisms

- May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.
- Encipherment
  - The use of mathematical algorithms to transform data into a form that is not readily intelligible.The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Security Mechanisms

- Digital Signature
  - Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).
- Access Control
  - A variety of mechanisms that enforce access rights to resources.

Security Mechanisms

- Data Integrity
  - A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- Authentication Exchange
  - A mechanism intended 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.

Security Mechanisms

- Routing Control
  - Enables selection of particular physically secure routes for certain data and allows routing changes, especially when a breach of security is suspected.
- Notarization
  - The use of a trusted third party to assure certain properties of a data exchange.

Security Mechanisms
PERVASIVE SECURITY MECHANISMS

- Mechanisms that are not specific to any particular
  - OSI security service or protocol layer.
- Trusted Functionality
  - That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).

Security Mechanisms

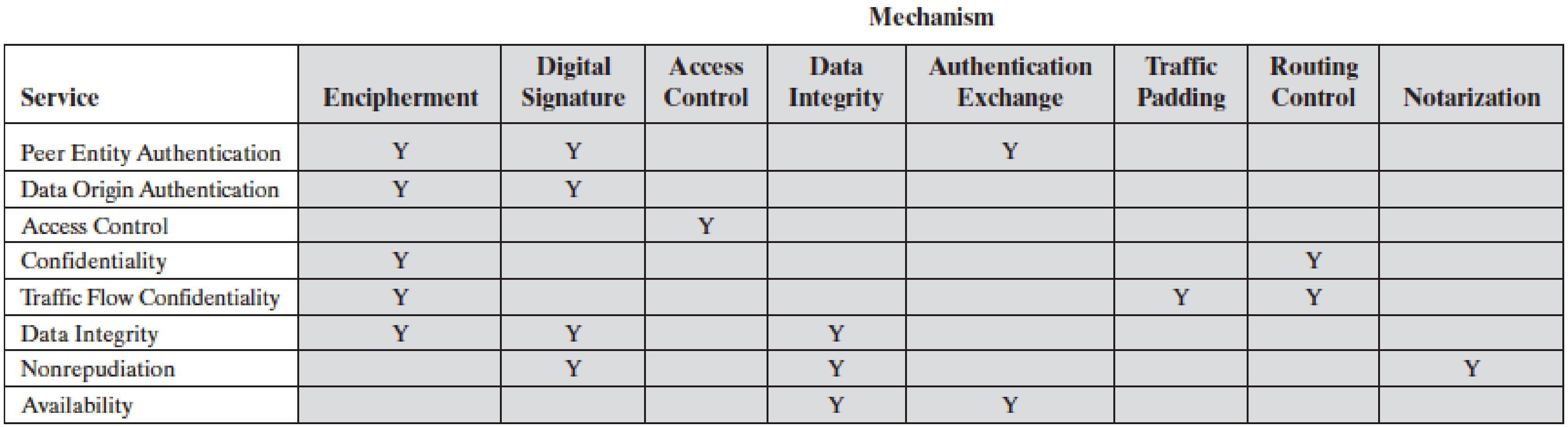
- Security Label
  - The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
- Event Detection
  - Detection of security-relevant events.

Security Mechanisms

- Security Audit Trail
  - Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
- Security Recovery
  - Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

Security Mechanisms

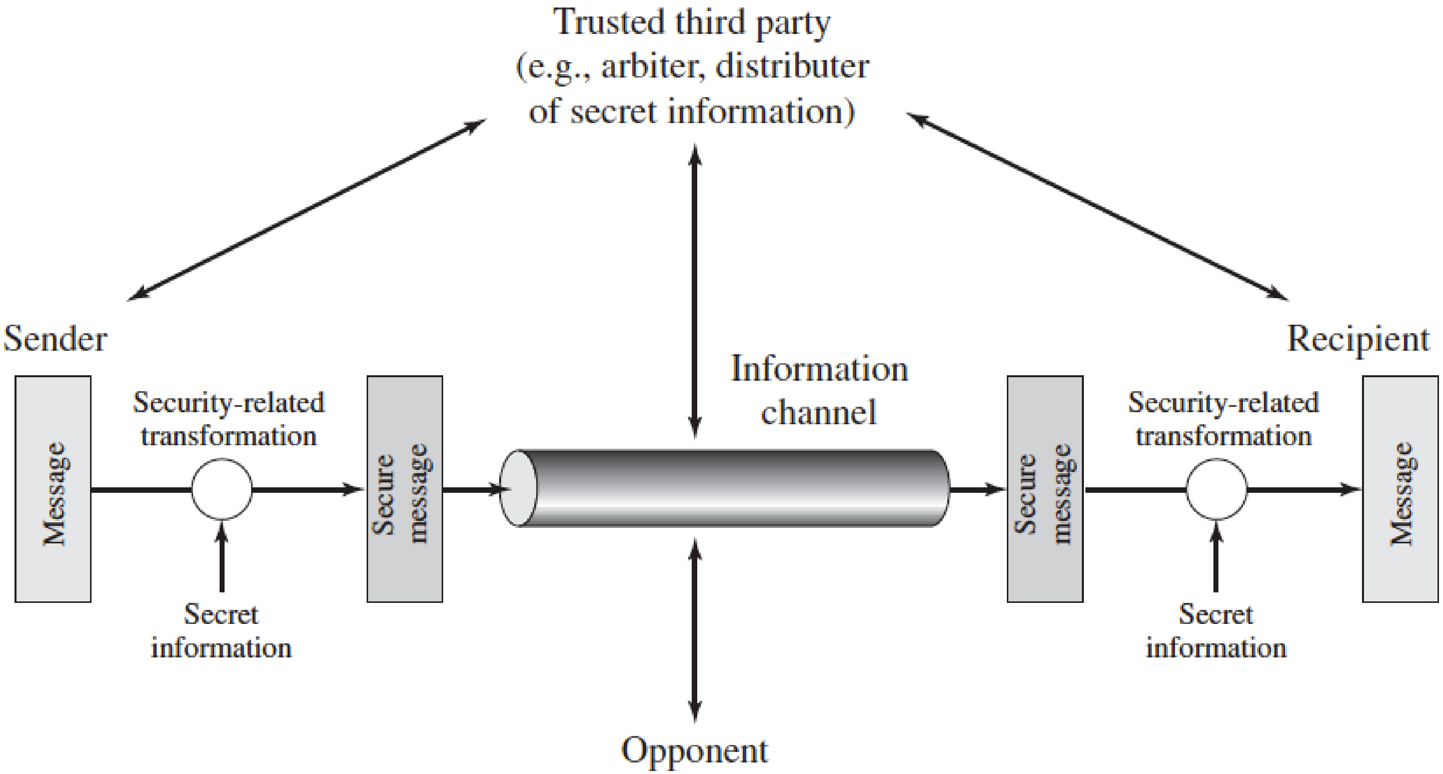
- Relationship between security services and mechanisms



	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				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

Models for Computer and Network Security

- Model for Network Security



- A message is to be transferred from one party to another across some sort of Internet service.
  - The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the Internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals

Models for Computer and Network Security

- Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

    –

Models for Computer and Network Security

- A security-related transformation on the information to be sent.
  - Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent,
  - And the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

Models for Computer and Network Security

- – Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

Models for Computer and Network Security

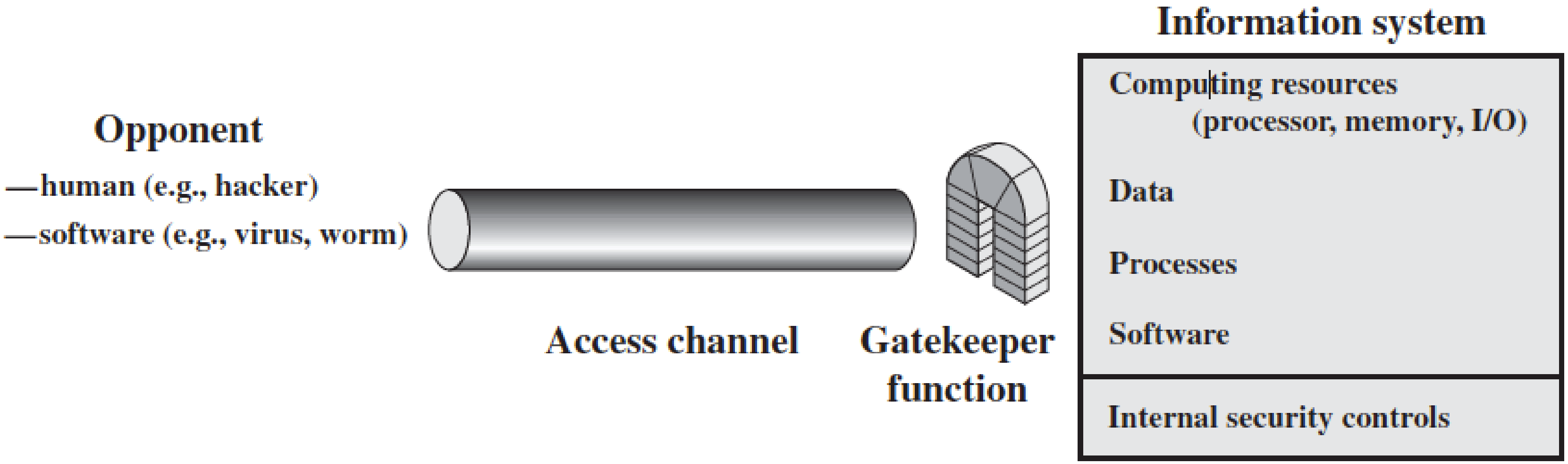
- Four basic tasks in designing a particular security service:
- 1. Design an algorithm for performing the security-related transformation.
  - The algorithm should be such that an opponent cannot defeat its purpose.
- 2. Generate the secret information to be used with the algorithm.

Models for Computer and Network Security

- 3. Develop methods for the distribution and sharing of the secret information.
- 4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Models for Computer and Network Security

- Network Access Security Model



Models for Computer and Network Security

- Protecting an information system from unwanted access:
  - Existence of hackers, who attempt to penetrate systems that can be accessed over a network.
    - The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system.
    - The intruder can be a disgruntled employee who wishes to do damage or a criminal who seeks to exploit computer assets for financial gain (e.g., obtaining credit card numbers or performing illegal money transfers).

Models for Computer and Network Security

  - Another type of unwanted access is the placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs, such as editors and compilers.
- Programs can present two kinds of threats:
  - Information access threats: Intercept or modify data on behalf of users who should not have access to that data.
  - Service threats: Exploit service flaws in computers to inhibit use by legitimate users.

Models for Computer and Network Security

- Viruses and worms are two examples of software attacks.
  - Such attacks can be introduced into a system by means of a disk that contains the unwanted logic concealed in otherwise useful software.
  - They can also be inserted into a system across a network; this latter mechanism is of more concern in network security.

Models for Computer and Network Security

- The security mechanisms needed to cope with unwanted access fall into two broad categories:
  - The first category: a 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. Once either an unwanted user or unwanted software gains access,
  - The second line of defense consists of a variety of internal controls that monitor activity and analyze stored information in an attempt to detect the presence of unwanted intruders