CRYPTOGRAPHY AND NETWORK SECURITY PRINCIPLES AND PRACTICE

Chapter 1

1.1 Computer Security Concepts

1.1.1 A Definition of 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).

Three key objectives that are at the heart of computer security

Objectives	Concepts
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.
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.

These three concepts form what is often referred to as the **CIA triad** (Figure 1.1).

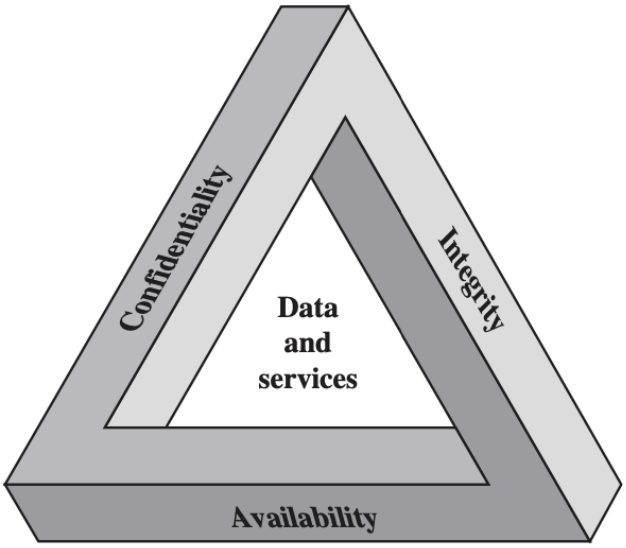


Figure 1.1 The Security Requirements Triad

Additional concepts

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. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.
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.

1.1.2 Examples

For these examples, we use three levels of impact on organizations or individuals should there be a breach of security.

LEVEL	IMPACT
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, for example, 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.
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 organi- zation 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.
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.

CONFIDENTIALITY

CONFIDENTIALITY RATING	INFORMATION
Low	Directory information, such as lists of students or faculty or departmental lists
Moderate	Student enrollment information
High	Grade information

INTEGRITY

INTEGRITY REQUIREMENT	INFORMATION
Low	An anonymous online poll
Moderate	A Web site that offers a forum to registered users to discuss some specific topic
High	A hospital patient’s allergy information stored

AVAILABILITY

AVAILABILITY REQUIREMENT	INFORMATION
Low	A system that provides authentication services for critical systems, applications, and devices
Moderate	A public Web site for a university; the Web site provides information for current and prospective students and donors
High	An online telephone directory lookup application

1.1.3 The Challenges of Computer Security

Computer and network security is both fascinating and complex. Some of the reasons follow:

REASON	DESCRIPTION		INSTANCE
Security is not as simple as it might first appear to the novice.	The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory,one-word labels .	But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.	confidentiality, authentication, nonrepudiation, or integrity
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 point 2, 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.	
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	should mechanisms be placed].	TCP/IP (Transmission Control Protocol/Internet Protocol)
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 compli- cate 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.
Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or	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		

administrator who tries to close them.	achieve perfect 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.			
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 strongse curity as animpediment to efficient and user-friendly operation of an information system or use of information.			

1.2 THE OSI SECURITY ARCHITECTURE

BACKGROUND

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.

FOCUS

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

Focus	Defination
Security attack	Any action that compromises the security of information owned by an organization.
Security mechanism	A process (or a device in corporating such 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.

THREAT AND ATTACK

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.**

1.3 SECURITY ATTACKS

PASSIVE ATTACKS & ACTIVE ATTACKS

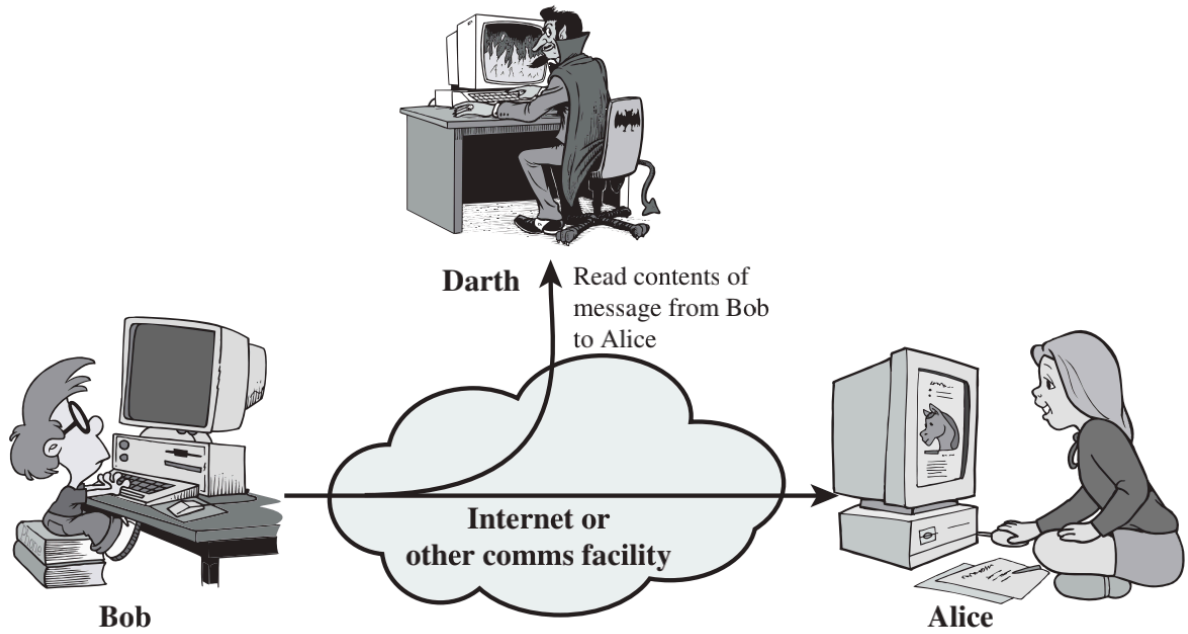
PASSIVE ATTACKS	**Attempting to learn or make use of information from the system but does not affect system resources.**
ACTIVE ATTACKS	Attempting to alter system resources or affect their operation.

1.3.1 PASSIVE ATTACKS

	SPECIFICATION
NATURE	Eavesdropping on, or monitoring of, transmissions, very difficult to detect, because they do not involve any alteration of the data.
GOAL	To obtain information that is being transmitted.
TYPES	The release of message contents and traffic analysis.
PREVENTION	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.

The release of message contents

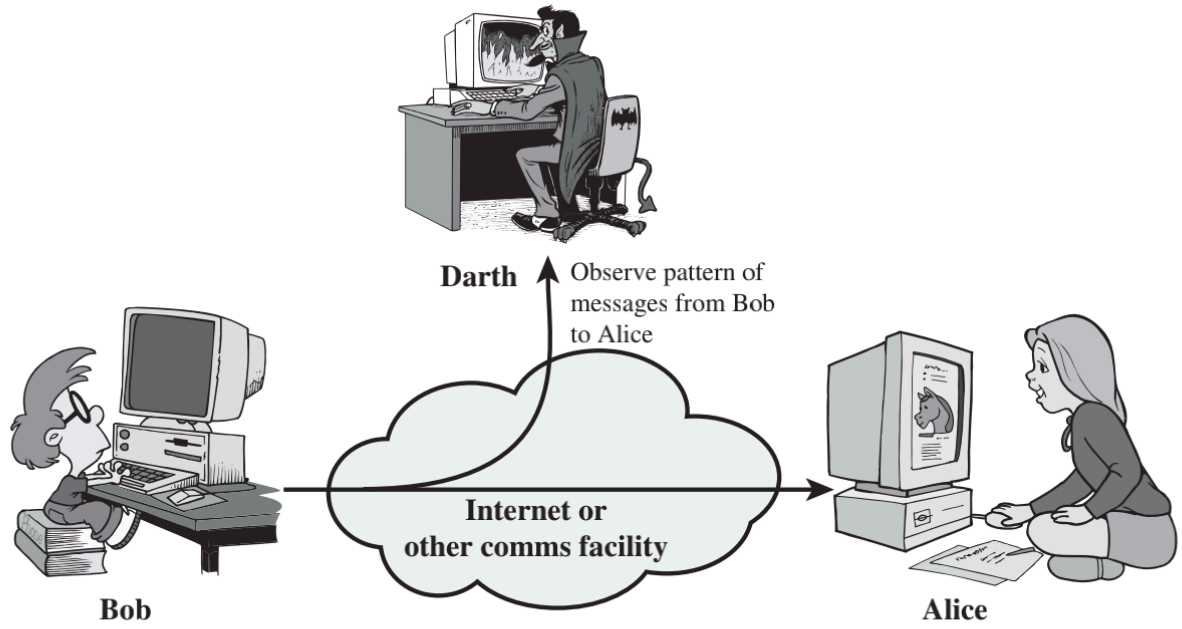
A telephone conversation, an electronic mail message, and a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



(a) Release of message contents

Traffic Analysis

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.



(b) Traffic analysis

Figure 1.2 Passive Attacks

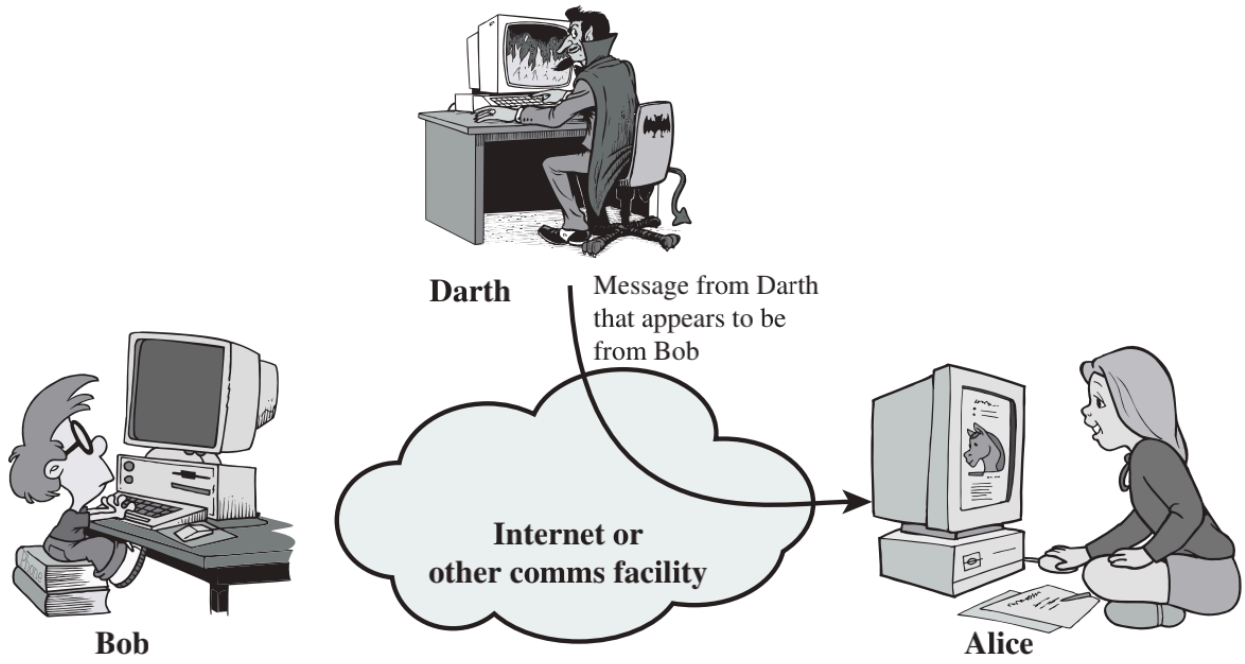
1.3.2 ACTIVE ATTACKS

	SPECIFICATION
NATURE	It is quite difficult to prevent active attacks absolutely because of the wide variety of potential physical, software, and network vulnerabilities.
GOAL	Some modification of the data stream or the creation of a false stream.
TYPES	Masquerade, replay, modification of messages, and denial of service.
PREVENTION	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.

Masquerade

***DEFINATION*:** masquerade takes place when one entity pretends to be a different entity (Figure 1.3a).

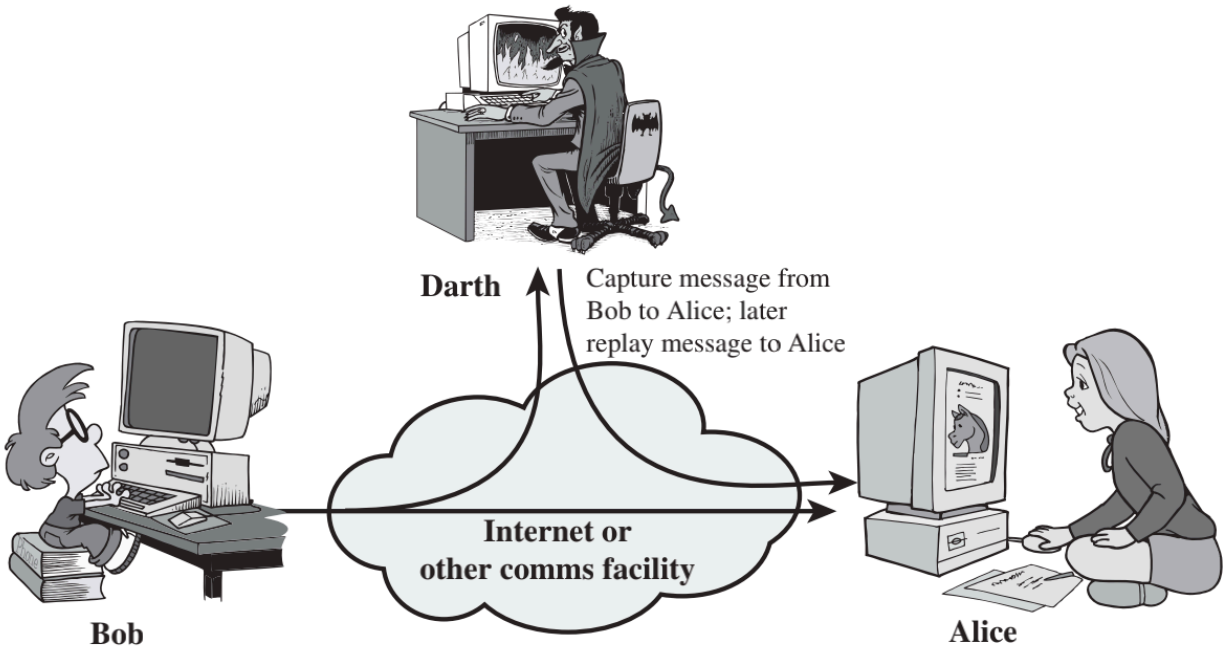
***INSTANCES*:** An authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.



(a) Masquerade

Replay

***DEFINATION*:** The passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect (Figure 1.3b).



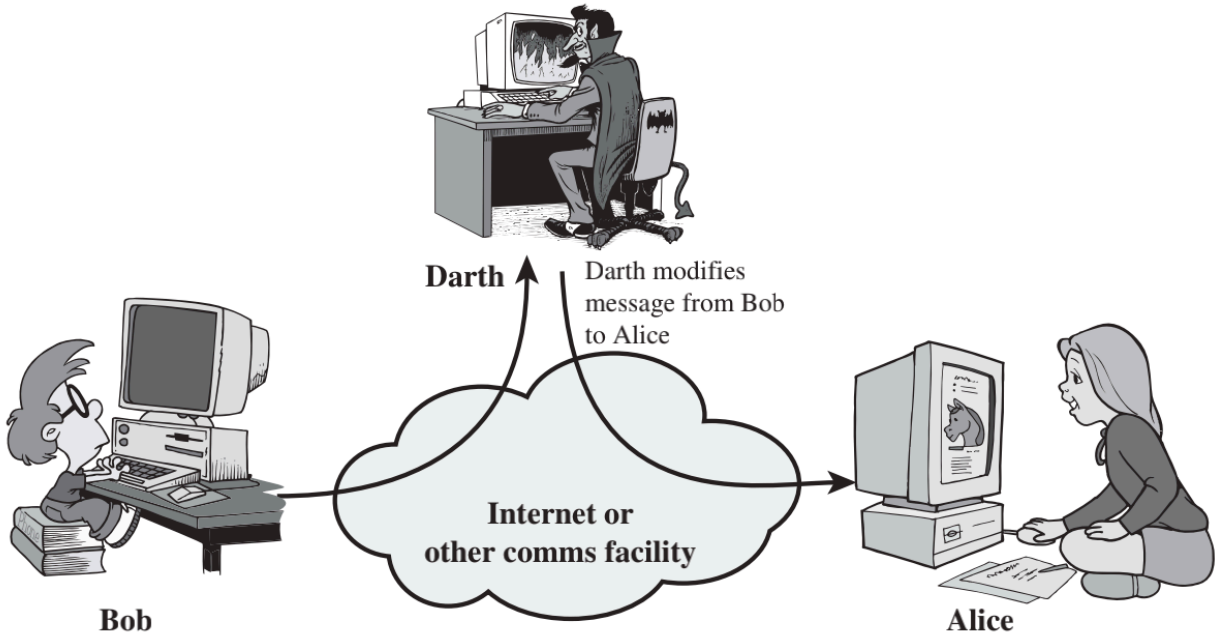
(b) Replay

Figure 1.3 Active attacks (*Continued*)

Modification of messages

DEFINATION: Some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect (Figure 1.3c).

INSTANCES: A message meaning "Allow John Smith to read confidential file *accounts*" is modified to mean "Allow Fred Brown to read confidential file *accounts.*"

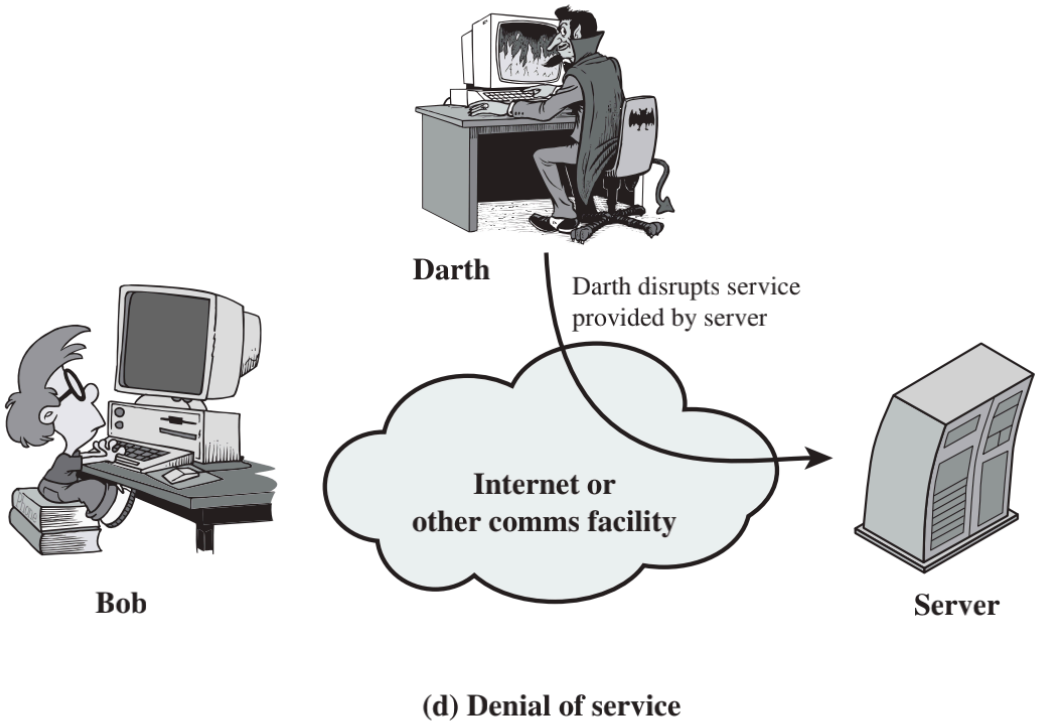


(c) Modification of messages

Denial of service

DEFINATION: Prevents or inhibits the normal use or management of communications facilities (Figure 1.3d).

INSTANCES: 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 soas to degrade performance.



(d) Denial of service

Figure 1.3 Active attacks

1.4 SECURITY SERVICES

DEDINATION

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.

X.800 divides these services into five categories and fourteen specific services (Table 1.2).

Table 1.2 Security Services (X.800)

AUTHENTICATION	DATA INTEGRITY
The assurance that the communicating entity is the one that it claims to be.	The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).
Peer Entity Authentication Used in association with a logical connection to provide confidence in the identity of the entities connected.	**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.
Data-Origin Authentication In a connectionless transfer, provides assurance that the source of received data is as claimed.	**Connection Integrity without Recovery** As above, but provides only detection without recovery.
ACCESS CONTROL	**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.
The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).	**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.
DATA CONFIDENTIALITY	**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.
The protection of data from unauthorized disclosure.	**NONREPUDIATION**
Connection Confidentiality The protection of all user data on a connection.	Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.
Connectionless Confidentiality The protection of all user data in a single data block	**Nonrepudiation, Origin** Proof that the message was sent by the specified party.
Selective-Field Confidentiality The confidentiality of selected fields within the user data on a connection or in a single data block.	**Nonrepudiation, Destination** Proof that the message was received by the specified party.
Traffic-Flow Confidentiality The protection of the information that might be derived from observation of traffic flows.	

AUTHENTIFICATION

The authentication service is concerned with assuring that a communication is authentic.

Cases

1. In the case of a single message, such as a warning or alarm signal, the function of the authentication service is to assure the recipient that the message is from the source that it claims to be from.
2. In the case of an ongoing interaction, such as the connection of a terminal to a host, two aspects are involved. First, at the time of connection initiation, the service assures that the two entities are authentic, that is, that each is the entity that it claims to be. Second, the service must assure that the

connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties for the purposes of unauthorized transmission or reception.

Services

SERVICES	SPECIFICATIONS
Peer entity authentication	Provides for the corroboration of the identity of a peer entity in an association. Two entities are considered peers if they implement to same protocol in different systems; e.g., two TCP modules in two communicating systems. Peer entity authentication is provided for use at the establishment of, or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection.
Data origin authentication	Provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail, where there are no prior interactions between the communicating entities.

ACCESS CONTROL

The ability to limit and control the access to host systems and applications via communications links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

DATA CONFIDENTIALITY

Confidentiality is the protection of transmitted data from passive attacks.

Levels

LEVELS	SPECIFICATIONS	EXAMPLES
The broadest service	The broadest service protects all user data transmitted between two users over a period of time.	When a TCP connection is set up between two systems, this broad protection prevents the release of any user data transmitted over the TCP connection.
Narrower forms of this service	Narrower forms of this service can also be defined, including the protection of a single message or even specific fields within a message.	

The other aspect

The protection of traffic flow from analysis. This requires that an attacker not be able to observe the source and destination,
frequency, length, or other characteristics of the traffic on a communications facility.

NONREPUDIATION

Nonrepudiation prevents either sender or receiver from denying a transmitted message. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

AVAILABILITY

Definition

the property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system (i.e., a system is available if it provides services according to the system design whenever users request them).

Actions

1. Some of these attacks are amenable to automated countermeasures, such as authentication and encryption.
2. Require some sort ofphysical action to prevent or recover from loss of availability of elements of a distributed system.

Availability Services

An availability service is one that protects a system to ensure its availability. This service addresses the security concerns raised by denial-of-service attacks. It depends on proper management and control of system resources and thus depends on access control service and other security services.