==========

THREATS, ATTACKS, AND ASSETS

An **attack** is a threat that is carried out (threat action) and, if successful, leads to an undesirable violation انتهاك of security.

The agent carrying out the attack is referred to as an **attacker**, or **threat agent** .

We can distinguish two types of attacks:

· **Active attack:** An attempt to alter system resources or affect their operation.

· **Passive attack:** An attempt to learn or make use of information from the system that does not affect system resources.

Threats and Attacks

Table 1.2 , based on , describes four kinds of threat consequences and lists

the kinds of attacks that result in each consequence.

Table 1.2 Threat Consequences, and the Types of Threat Actions that Cause Each Consequence.

Threat Consequence	Threat Action (attack)
Unauthorized Disclosure A circumstance ظرفor event an entity gains access to data for which the entity is not authorized	**1-Exposureالتعرض :** Sensitive data are directly released to an unauthorized entity. **2-Interceptionاعتراض :** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **3-Inferenceالاستدلال :** A threat action an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications. **4-Intrusionالتسلل :** An unauthorized entity gains access to sensitive data by circumventing التحايل على a system's security protections.
Deceptionالخداع A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**1-Masqueradeقناع:** An unauthorized entity gains access to a system or performs a malicious act by posing الانتحال as an authorized entity. **2-Falsificationتزوير :** False data deceiveتخدع an authorized entity. **3-Repudiationرفض:** An entity deceives another by falsely denying responsibility for an act.
Disruptionاضطراب A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**1-Incapacitationالعجز :** Prevents or interrupts system operation by disabling a system component. **2-Corruption:** Undesirably alters system operation by badly modifying system functions or data.

	3-Obstruction انسداد : A threat action that interrupts delivery of system services by prevention منع system operation.
Usurpation استحواذ A circumstance or event that results in control of system services or functions by an unauthorized entity.	**1-Misappropriation اختلاس :** An entity assumes unauthorized logical or physical control of a system resource. **2-Misuse:** Causes a system component to perform a function or service that is harmful to system security.

Unauthorized disclosure is a threat to confidentiality. The following types of attacks can result in this threat consequence:

1• **Exposure:** This can be deliberate, as when an insider intentionally بغرض releases sensitive information, such as credit card numbers, to an outsider. It can also be the result of a human, hardware, or software error, which results in an entity gaining unauthorized knowledge of sensitive data. There have been numerous instances of this, such as universities accidentally posting student confidential information on the Web.

2• **Interception:** Interception is a common attack in the context of communications. On a shared local area network (LAN), such as a wireless LAN or a broadcast Ethernet, any device attached to the LAN can receive a copy of packets proposed for another device. On the Internet, a determined hacker can gain access to e-mail traffic and other data transfers. All of these situations create the potential for unauthorized access to data.

3• **Inference:** An example of inference is known as traffic analysis, in which an adversary is able to gain information from observing the pattern of traffic on a network, such as the amount of traffic between particular pairs of hosts on the network. Another example is the inference of detailed information from
a database by a user who has only limited access; this is accomplished by repeated queries whose combined results enable inference.

4• **Intrusion:** An example of intrusion is an adversary gaining unauthorized access to sensitive data by overcoming the system’ s access control protections.

Deception is a threat to either system integrity or data integrity. The following types of attacks can result in this threat consequence:

1• **Masquerade:** One example of masquerade is an attempt by an unauthorized user to gain access to a system by posing as an authorized user; this could happen if the unauthorized user has learned another user’ s logon ID and password.
Another example is malicious logic, such as a Trojan horse, that appears to perform a useful or desirable function but actually gains unauthorized access to system resources or tricks a user into executing other malicious logic.

2• **Falsification:** This refers to the altering or replacing of valid data or the introduction of false data into a file or database.
For example, a student may alter his or her grades on a school database.
3• **Repudiation:** In this case, a user either denies sending data or a user denies receiving or having the data.

Disruptionالخداع is a threat to availability or system integrity. The following types of attacks can result in this threat consequence:

1• **Incapacitation:** This is an attack on system availability. This could occur as a result of physical destruction of or damage to system hardware. More typically, malicious software, such as Trojan horses, viruses, or worms, could operate in such a way as to disable a system or some of its services.

2• **Corruption:** This is an attack on system integrity. Malicious software in this context could operate in such a way that system resources or services function in an unintended manner. Or a user could gain unauthorized access to a system and modify some of its functions.
An example of the latter is a user placing backdoor logic in the system to provide subsequent access to a system and its resources by other than the usual procedure.

3• **Obstruction**انسداد **:** One way to obstruct system operation is to interfere with communications by disabling communication links or altering communication control information. Another way is to overload the system by placing excess load on communication traffic or processing resources.

Usurpation استحواذ is a threat to system integrity. The following types of attacks can result in this threat consequence:

1• **Misappropriation:** This can include theft of service. An example is a distributed denial of service attack, when malicious software is installed on a number of hosts to be used as platforms to launch traffic at a target host. In this case, the malicious software makes unauthorized use of processor and operating system resources.

2• **Misuse:** Misuse can occur by means of either malicious logic or a hacker that has gained unauthorized access to a system. In either case, security functions can be disabled or thwarted.

Threats and Assets

The assets of a computer system can be categorize تصنف as hardware, software, data, and communication lines and networks. In this subsection, we briefly describe these four categories and relate these to the concepts of integrity, confidentiality, and availability introduced in Section 1.1 (see Figure 1.3 and Table 1.3).

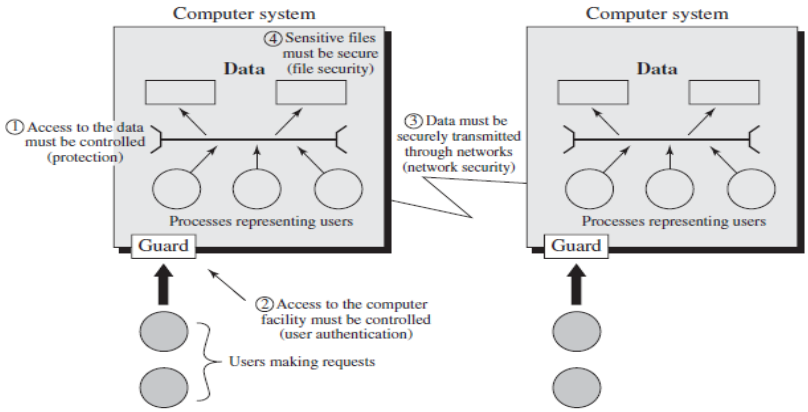


Figure 1.3 **Scope of Computer Security**

Table 1.3 **Computer and Network Assets, with Examples of Threats.**

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.		
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

HARDWARE A major threat to computer system hardware is the threat to availability. Hardware is the **most** vulnerable to attack and the **least** susceptible عرضه to automated controls. Threats include accidental عرضي and deliberate متعمد damage to equipment as well as theft.

The increase of personal computers and workstations and the widespread use of LANs increase the potential امكانية for losses in this area. Theft of CD-ROMs and DVDs can lead to loss of confidentiality. Physical and administrative security measures are needed to deal with these threats.

SOFTWARE Software includes the operating system, utilities, and application programs. A key threat to software is an attack on availability. Software, especially application software, is often easy to delete. Software can also be altered or damaged to make it useless. Careful software configuration management, which includes making backups of the most recent version of software, can maintain high availability.

A more difficult problem to deal with is software modification that results in a program that still functions but that behaves سلوك differently than before, which is a threat to integrity/authenticity. Computer viruses and related attacks fall into this group. A final problem is protection against software piracyقرصنة . Although certain countermeasures are available, by and large the problem of unauthorized copying of software has not been solved.

DATA. A much more widespread problem is data security, which involves files and other forms of data controlled by individuals, groups, and business organizations.

Security concerns الاهتمامات with respect to data are broad, including availability, secrecy, and integrity. In the case of availability, the worry is with the destruction of data files, which can occur either accidentally or maliciously.

The obvious worry with secrecy is the unauthorized reading of data files or databases, and this area has been the subject of perhaps more research and effort than any other area of computer security.

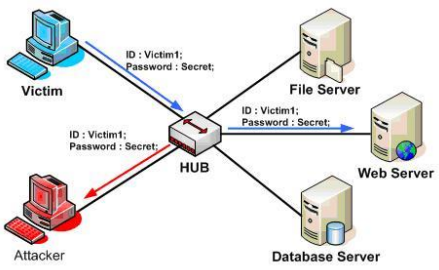
COMMUNICATION LINES AND NETWORKS Network security attacks can be classified as *passive attacks* and *active attacks* . A passive attack attempts to learn or make use of information from the system but does not affect system resources. An active attack attempts to alter system resources or affect their operation.

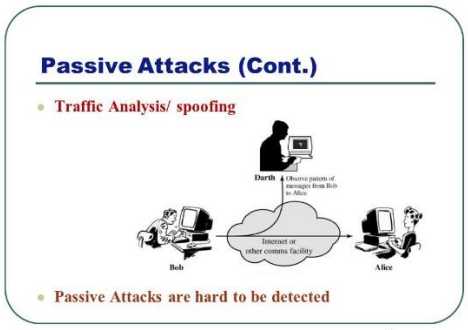
***Passive attacks** are in the nature of eavesdropping التنصت on, or monitoring of, transmissions. The goal of the attacker is to obtain information that is being transmitted. Passive attacks are very difficult to detect because they do not involve any alteration of the data.

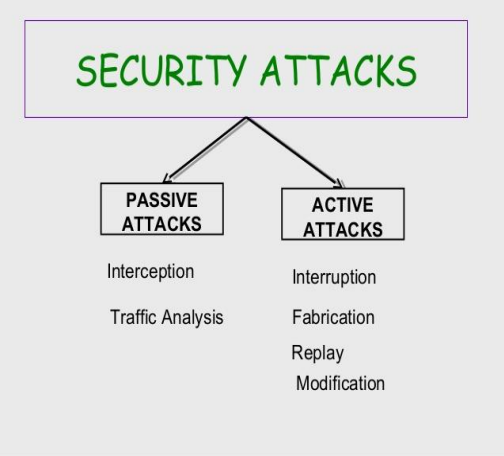
Typically, the message traffic is sent and received in an apparently ويبدو أن normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of **encryption.**

Thus, the emphasisالتركيز in dealing with passive attacks is on prevention rather than detection.

***Active attacks** involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: replay, masquerade, modification of messages, and denial of service.







A SECURITY ARCHITECTURE FOR OPEN SYSTEMS

To evaluate effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for security needs a systematic way of defining the requirements for security and characterizing وصف the approaches to satisfying those requirements.

The OSI security architecture is useful to managers as a way of organizing the task of providing security. Furthermore, because this architecture was developed as an international standard, computer and communications vendors have developed security features for their products and services that relate to this structured definition of services and mechanisms

Although X.800 focuses on security in the contextالسياق of networks and communications, the concepts apply also to computer security.

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

- **Security attack:** Any action that negotiations the security of information owned المملوكة by an organization.
- **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 are intended تعتزمto counter تصدي security attacks, and they make use of one or more security mechanisms to provide the service.

==========

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 suitable security of the systems or of data transfers. Perhaps a clearer أوضح definition is found in RFC 2828, which provides the following definition: 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 6 categories and 14 specific services (Table 1.5).

AUTHENTICATION The assurance that the communicating entity is the one that it rights 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. **ACCESS CONTROL** 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). **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. **AVAILABILITY** Ensures that there is no denial of authorized access to network elements, stored information, information flows, services, and applications due to events impacting the network. Disaster recovery solutions are included in this catego1ry.	**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. **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. **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. **NONREPUDIATION** Provides protection against denial by one of the entities involved in a communication of having participated 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.