COMPUTER SECURITY CONCEPTS

A Definition of Computer Security

The NIST Computer Security Handbook [NIST95] defines the term *computer security* as follows:

Computer Security: The protection afforded(توفرها)to an automated information system in order to achieve the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

This definition introduces three key objectives that are at the heart of computer security:

· **Confidentiality سرية :** This term covers two related concepts:

– **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals.

– **Privacy خصوصية :** 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 سلامة :** 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 unaffected manner , free from deliberate الاعتماديةor unauthorized manipulation معالجة of the system.

· **Availability توفر :** Assures that systems work immediately and service is not denied to authorized users.

These three concepts form what is often referred to as the **CIA triad**

(Figure 1.1). The three concepts embody the fundamental security objectives for both data and for information and computing services. For example, the NIST

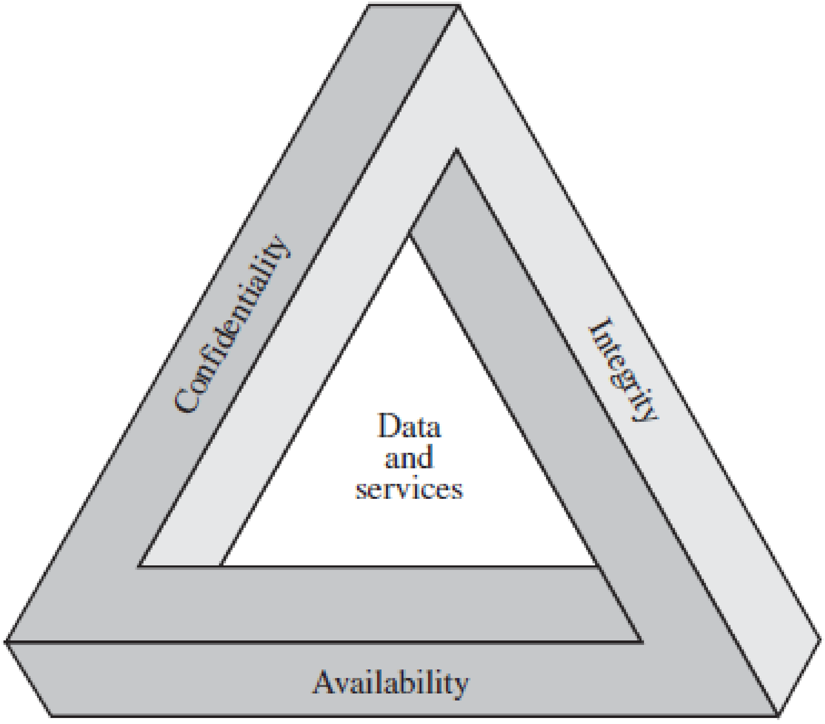

Figure 1.1 **The Security Requirements Triad**

standard FIPS 199 (*Standards for Security Categorization of Federal Information and Information Systems*) lists confidentiality, integrity, and availability as the three security objectives for information and for information systems. FIPS PUB 199 provides a useful characterization of these three objectives in terms of requirements and the definition of a loss of security in each category:

· **Confidentiality سرية :** Preserving authorized restrictions قيود on information access and disclosure كشف , including means for protecting personal privacy and proprietary امتلاك information. A loss of confidentiality is the unauthorized disclosure of information.

· **Integrity سلامة :** Guarding حراسةagainst improper information modification or destruction تدمير . A loss of integrity is the unauthorized modification or destruction of information.

· **Availabilityتوفر:** Ensuring timely and reliable access to and use of information.

A loss of availability is the disruption اضطراب of access to or use of information or an information system.

*Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture.

Two of the most commonly mentioned are as follows:

· **Authenticity اصالة :** The property of being genuine حقيقي and being able to be verified التحقق 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.

· **Accountabilityالمساءلة :** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiationعدم الانكار , deterrence الرد , fault خطأisolation, intrusion التسلل detection and prevention, and after-action recovery and legal action.

The Challenges of Computer Security

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

1. Computer security is not as simple as it might first appear to the beginner. The requirements seem to be straightforward; most of the major requirements for security services can be given understandable one-word labels:

confidentiality, authentication, nonrepudiation عدم الإنكار, integrity. But the mechanisms used to meet those requirements can be quite complex.

2. In developing a particular معين 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 *exploitingاستغلال an unexpected weakness in the mechanism.*

3. Because of point 2, the procedures used to provide particular services are often counterintuitive الحدس. Typically, a security mechanism is _, and it is not apparent from the declaration of a particular requirement that such precise measures are needed. *It is only when the various aspects of the threat are considered that precise security mechanisms make sense.*

4. 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/ (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].

5. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants (members) be in control of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There may also be a trust 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 تقديم such time limits meaningless.

6. Computer security is essentially a battle of wits معركة دهاء between a guilty party 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.

7. There is a natural tendency ميل on the part of users and system managers to perceive تصور little benefit from security until a security failure occurs.

8. Security requires regular , even constant, monitoring, and this is difficult in today’ short-term, overloaded environment.

9. Security is still too often an addition to be incorporated into a system after the design is complete rather than being an integral part of the design process.

10. Many users and even security administrators view strong security as an impediment عائق to efficient and user-friendly operation of an information system or use of information.

The difficulties just enumerated will be encountered واجه in numerous ways .

A Model for Computer Security:-

We now introduce some terminology that will be useful throughout the book, relying on RFC 2828, *Internet Security Glossary* . 3 Table 1.1 defines terms and Figure 1.2 [CCPS09a] shows the relationship among some of these terms. We start with the concept of a **system resource** , or **asset** , that users and owners wish to protect. The assets of a computer system can be categorized as follows:

· **Hardware:** Including computer systems and other data processing, data storage, and data communications devices

· **Software:** Including the operating system, system utilities, and applications

· **Data:** Including files and databases, as well as security-related data, such as password files.

Table 1.1 Computer Security Terminology

Adversary (threat agent)

An entity that attacks, or is a threat to, a system.

Attack

An assault الاعتداء on system security that derives from an intelligent threat; that is, an intelligent act that is a attempt (especially in the sense of a method or technique) to avoid security services and violate the security policy of a system.

Countermeasure

An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk

An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with harmful result.

Security Policy

A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)

Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component–hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event, that could breach خرق security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Vulnerability

A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate انتهاك the system’s security policy.

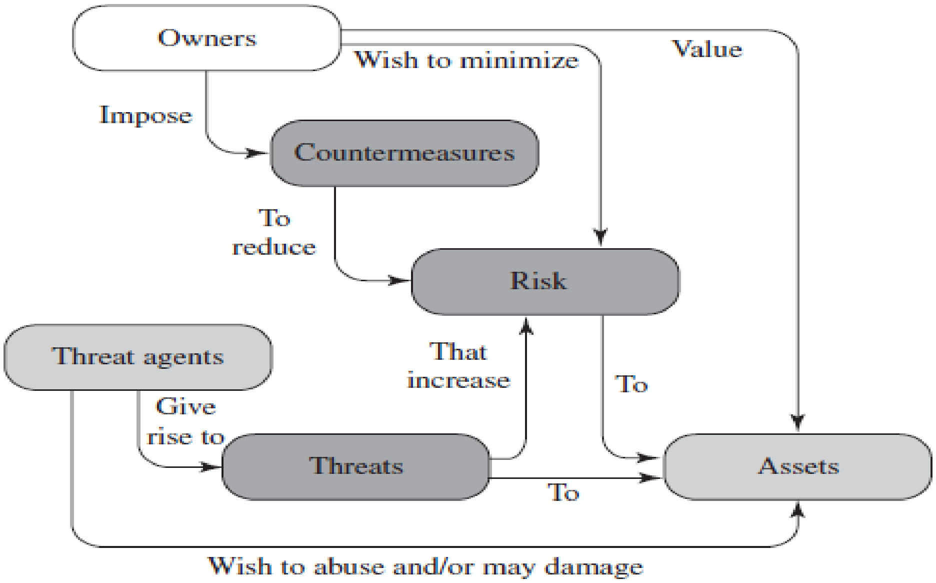

Figure 1.2 Security Concepts and Relationships