COMPUTER SECURITY

DR. MOCEHEB LAZAM SHUWANDY

FOURTH STAGE - **LECTURE 1**

CCMS-TU

FIRST COURSE:

2021-2022

TEXT BOOKS & REFERENCES

- Network Security Essentials: Applications & Standards, William S., Pearson Education Asia
- Modern operating System, 4th Edition. Andrew S. Tanenbaum, Pearson Education Asia
- Database Security Mechanisms for Computer Network- Sead Muftic, John wiles
- Designing Security Architecture Solutions – Jay Ramachandran, Wiley dreamtech
- CompTIA security+ - David L. Prowse, Pearson USA 4th Edition, 2019.

INTRODUCTION

- The information security has undergone two major changes with the evolution of computers.
- The need for automated tools for protecting information stored on the computer became evident.
- The collection of tools designed to protect data and to thwart hackers is computer security.
- The introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computer and computer leaded to network security.

TERMINOLOGY

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.

- The need for automated tools for protecting information stored on the computer became evident.

Attack

- An assault on system security that derives from an intelligent threat, i.e., 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.
- Attack can be active or passive, by insider or by outsider, or via attack mediator.

WHAT IS COMPUTER SECURITY?

- The National Institute of Standards and Technology (NIST) Computer Security Handbook [NIST95] defines the term *computer security* as follows:

Computer Security: The protection afforded 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).

WHAT IS COMPUTER SECURITY? …. CON.

- This definition provides three main objectives, which are fundamental 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.

WHAT IS COMPUTER SECURITY? …. CON.

- **Integrity :**This term covers two related concepts:

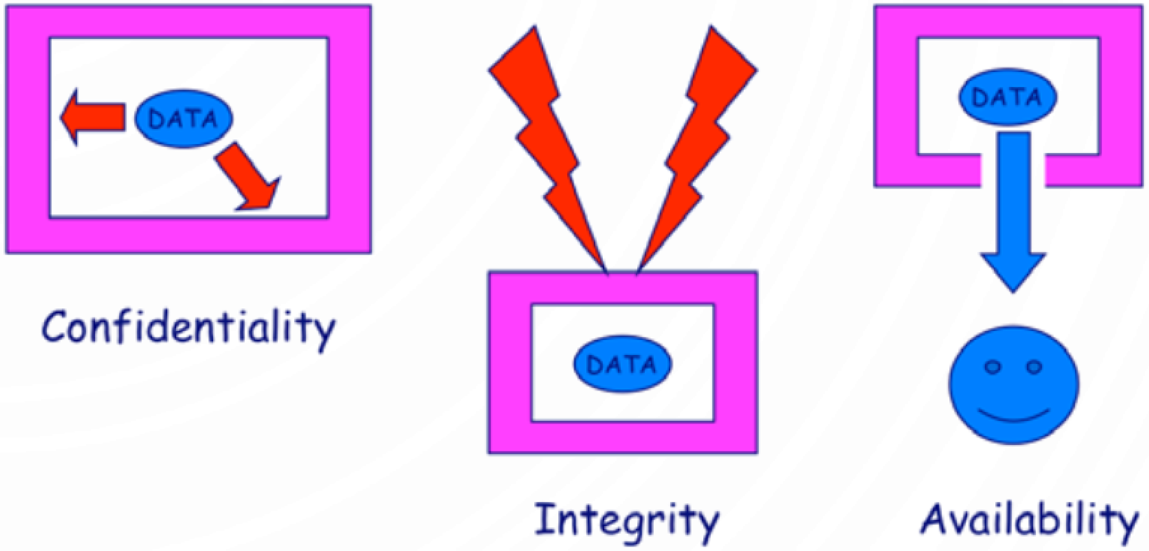
Data integrity: Assures that information and programs are changed only in a specified and authorized manner.

System integrity : Assures that a system performs its intended function in an unaffected manner , free from deliberate or unauthorized manipulation of the system.

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

SECURITY GOALS

- 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.
- For example, the **NIST** 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.



SECURITY GOALS…. CON.

- FIPS Publication (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 :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 .

A loss of integrity is the unauthorized modification or destruction of information.

SECURITY GOALS…. CON.

*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 :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.

THE CHALLENGES OF COMPUTER SECURITY

- Computer security is both fascinating 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 ,integrity. **But the mechanisms used to meet those requirements can be quite complex.**

THE CHALLENGES OF COMPUTER SECURITY…CON.

2. 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.*

3. Because of point 2, the procedures used to provide particular services are often counterintuitive .

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.

THE CHALLENGES OF COMPUTER SECURITY…CON.

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].

THE CHALLENGES OF COMPUTER SECURITY…CON.

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 such time limits meaningless.

THE CHALLENGES OF COMPUTER SECURITY…CON.

6. Computer security is essentially a battle of wits 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.

THE CHALLENGES OF COMPUTER SECURITY…CON.

7. There is a natural tendency on the part of users and system managers to perceive 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.

THE CHALLENGES OF COMPUTER SECURITY…CON.

10. 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 difficulties just enumerated will be encountered in numerous ways .

Q&A