Computer Network Security

TE - IT

Lecture -4
20/07/2022

Session: 3:30 - 4:30 PM

Prof. Stella J
Department of Information Technology
Xavier Institute of Engineering

Module-1

✓ Contents

1. Computer Network Security Definition
2. CIA Triad

A definition of computer security

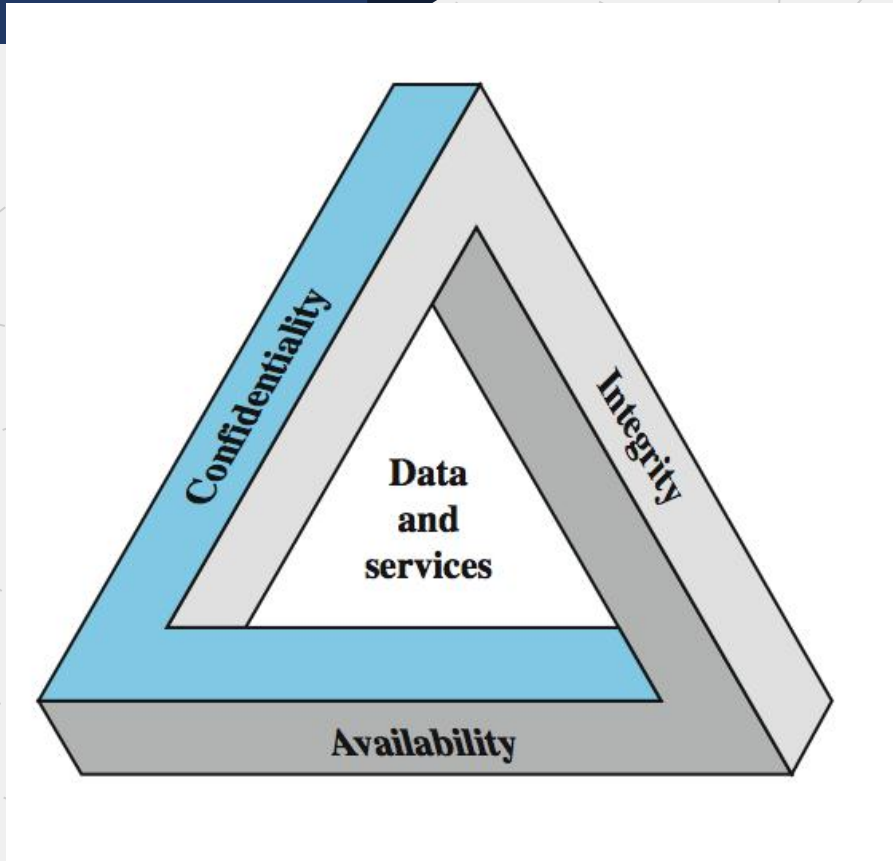
- **Computer security:** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)

NIST 1995

Three key objectives (the CIA triad)

- **Confidentiality**
  - **Data confidentiality**: Assures that confidential information is not disclosed to unauthorized individuals
  - **Privacy**: Assures that individual control or influence what information may be collected and stored
- **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 operations in unimpaired manner
- **Availability**: assure that systems works promptly and service is not denied to authorized users

Key Security Concepts



Other concepts to a complete security picture

Authenticity: the property of being genuine and being able to be verified and trusted; confident in the validity of a transmission, or a message, or its originator

Accountability: generates the requirement for actions of an entity to be traced uniquely to that individual to support nonrepudiation, deference, fault isolation, etc

Levels of security breach impact

- **Low**: the loss will have a limited impact, e.g., a degradation in mission or minor damage or minor financial loss or minor harm
- **Moderate**: the loss has a serious effect, e.g., significance degradation on mission or significant harm to individuals but no loss of life or threatening injuries
- **High**: the loss has severe or catastrophic adverse effect on operations, organizational assets or on individuals (e.g., loss of life)

Examples of security requirements: Confidentiality

Student grade information is an asset whose confidentiality is considered to be very high

The US FERPA Act: grades should only be available to students, their parents, and their employers (when required for the job)

Student enrollment information: may have moderate confidentiality rating; less damage if enclosed

Directory information: low confidentiality rating; often available publicly

Examples of security requirements: Integrity

A hospital patient's allergy information (high integrity data): a doctor should be able to trust that the info is correct and current

If a nurse deliberately falsifies the data, the database should be restored to a trusted basis and the falsified information traced back to the person who did it

An online newsgroup registration data: (moderate level of integrity)

An example of (low integrity) requirement: anonymous online poll (inaccuracy is well understood)

Examples of security requirements: Availability

A system that provides authentication: **high availability** requirement

If customers cannot access resources, the loss of services could result in financial loss

A public website for a university: a **moderate availably** requirement; not critical but causes embarrassment

An online telephone directory lookup: a **low availability** requirement because unavailability is mostly annoyance (there are alternative sources)

Challenges of computer security

1. Computer security is not simple
2. One must consider potential (unexpected) attacks
3. Procedures used are often counter-intuitive
4. Must decide where to deploy mechanisms
5. Involve algorithms and secret info (keys)
6. A battle of wits between attacker / admin
7. It is not perceived on benefit until fails
8. Requires constant monitoring
9. Too often an after-thought (not integral)
10. Regarded as impediment to using system

A model for computer security

- Systems resources
  - Hardware, software (OS, apps), data (users, system, database), communication facilities and network (LAN, bridges, routers, …)
- Our concern: vulnerability of these resources (corrupted, unavailable, leaky)
- Threats exploit vulnerabilities
- Attack is a threat that is accrued out
  - Active or passive; from inside or from outside
- Countermeasures: actions taken to prevent, detect, recover and minimize risks

THANK YOU