

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

- NIST Computer Security Handbook

Network Security Requirements:

- Confidentiality:
 - **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to **unauthorized** individuals;
 - **Privacy:** Assures that individual's control or influence **what information** related to them may be collected and stored and **by whom** and **to whom** that information may be disclosed

i.e., student grade information
- Integrity:
 - **Data integrity:** Assures that data (both stored and in transmitted packets) 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

i.e., a hospital patient's allergy information
- **Availability:** Assures that systems work promptly, and service is not denied to authorized users, ensuring **timely** and **reliable** access to and use of information

i.e., denial of service attack

- **Authenticity**
- **Accountability**
 - traceable data source,
 - fault isolation
 - intrusion detection and prevention,
 - recovery and legal action
 - system must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes

Challenges to achieve a secure system

- The mechanisms used to meet those requirements can be quite **complex**, and understanding them may evolve rather **subtle** reasoning
- When developing security mechanisms, must always consider **potential attacks**
- Sometimes, security mechanisms are **counterintuitive**
- **Where** to use them?
- Involve **more** than a particular algorithm or protocol
- **No agreement** on security for complex and heterogeneous systems i.e. trusts on data in different countries etc.

OSI Security Architecture

- International Telecommunication Union – Telecommunication (ITU-T) recommends X.800
- Security Architecture for Open Systems Interconnection (OSI)
- Defines a systematic way of defining and providing security requirements
- Used by IT managers and vendors in their products

Other Security Architectures

- OWASP - Open Web Application Security Project
- web application security
- OWASP foundation
- NIST, Cybersecurity Framework
- <https://www.nist.gov/cyberframework>
- [VIRTUAL WORKSHOP #2](https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2) | February 15, 2023 (9:00 AM – 5:30 PM EST). Join us to discuss potential significant updates to the CSF as outlined in the soon-to-be-released CSF Concept Paper.
- <https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2>

Security attack

Definition: any action that compromises the security of information owned by an organization

Two types of security attacks

- Passive attack
- Active attack

Passive attack

•i.e. eavesdropping on or monitoring of transmissions

- Goal: obtain information being transmitted
- release of message contents
- traffic analysis – a promiscuous sniffer
- Very difficult to detect – no alteration of the data
- But easy to prevent, **why?**

Active attack

- active attack includes:
- replay
- Modification of messages
- Denial of service
- Masquerade

Know Your Threat Model

- **Threat model:** A model of who your attacker is and what resources they have
- One of the best ways to counter an attacker is to attack their reasons

Example: adversary model

- “The adversary is assumed to be intelligent and has limited number of resources. Before capturing the nodes, it exploits the various vulnerabilities of the networks. It knows the topology of the network, routing information. It aims to capture the sink node so as to disrupt the whole traffic. If it is not able to capture the sink node, it will capture the nearby nodes of the sink. It tries to disrupt the whole traffic of the network

with minimum number of captured nodes. It is also assumed that the adversary tends to attack more on the nodes closer to the data sink than nodes that are far away”.