Computer and Network Security

- Traditionally, security was provided by **physical measures** (such as doors, locks, vaults, etc.) and **administrative mechanisms** (such as access procedures, security guards, etc.)
- Data and files stored in computer systems requires **automated tools** for their protection.
- Also, when data is exchanged between computing systems through **networks and communication links**, appropriate security must be enforced to **protect the data during the transmission**.

Computer and Network Security

- **Computer Security:** A generic name that refers to the **overall security of computing systems**, including the tools designed to protect data that are processed and stored in computer systems from various attacks.
- **Network Security:** Approaches, techniques, protocols, technologies, and tools adopted to protect data during their transmission from one computer to another, or from one network to another.
- The aim of both computer and network security consists of measures to ***deter***, ***prevent***, ***detect***, and ***correct*** security violations that involve **processing, storage, and transmission of data** (information).

Categories of Security Attacks

Passive Attacks

- A passive attack refers to a network attack where a ***system is observed and occasionally checked for open ports and vulnerabilities***. The objective of such an attack is to gather details about the targeted system, without engaging in any direct actions against it.

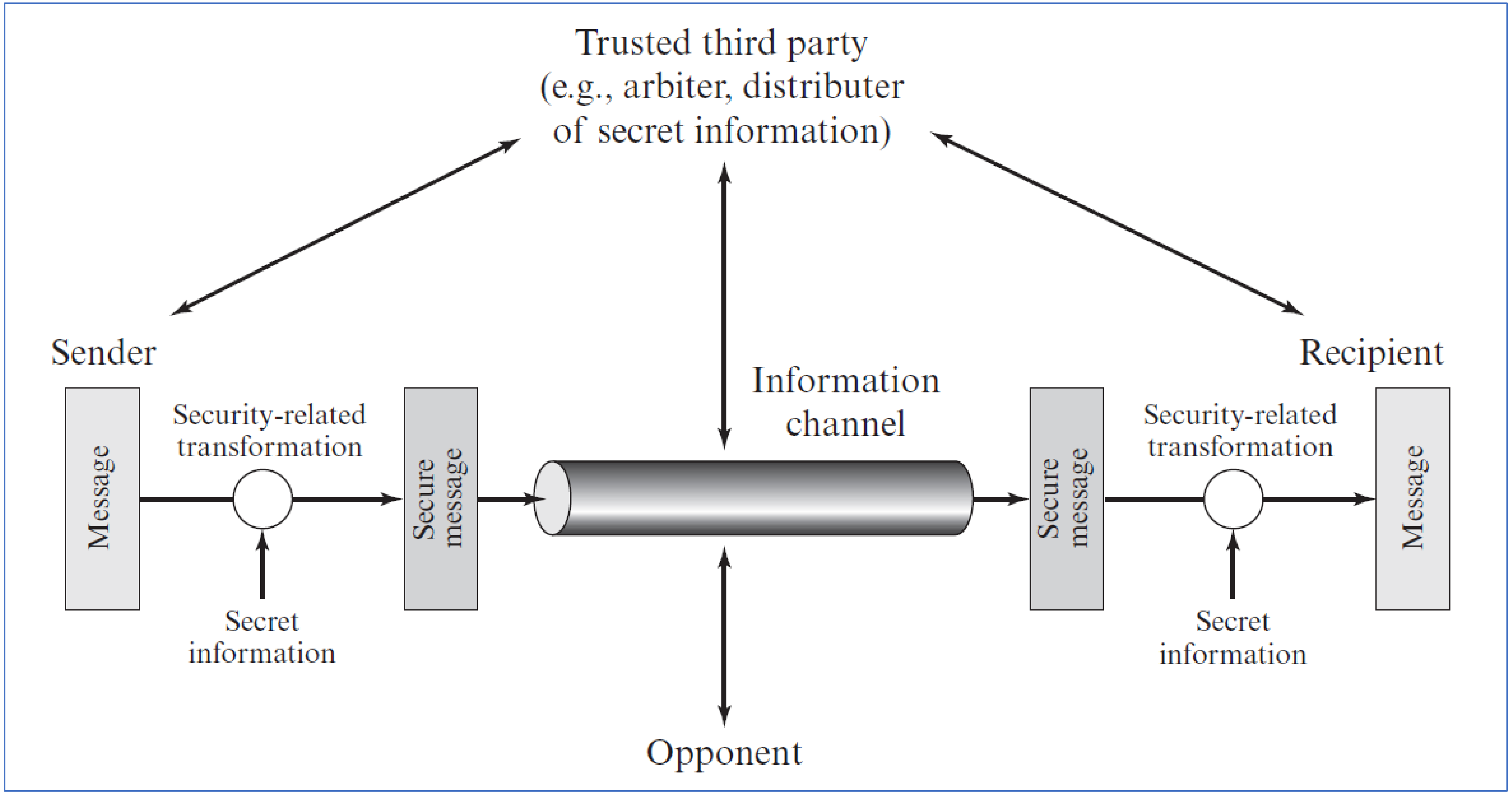
- Examples: Eavesdropping of data transmission, obtain message contents or monitoring of traffic flows in a network.

Active Attacks

- Active attacks are malicious attempts by cybercriminal to ***modify or manipulate the content of messages or information***. These attacks pose a risk to the integrity and availability of a system. As a result of active attacks, systems can be damaged, and the information within them can be modified.

- Examples: Denial of Service (DoS), masquerade (impersonate) of one entity as some other, replay previous messages, modify messages in transit.

Model for Network Security



Model for Network Security

- **Sender** wants to send a message to the **Recipient** in a confidential manner through the **Information Channel**.

- The Information Channel is considered insecure in nature.

- Therefore, if some third party (shown as **Opponent**) somehow gets the message, it will not be legible to the Opponent (that is, opponent must not be able to get any meaningful information from the message).

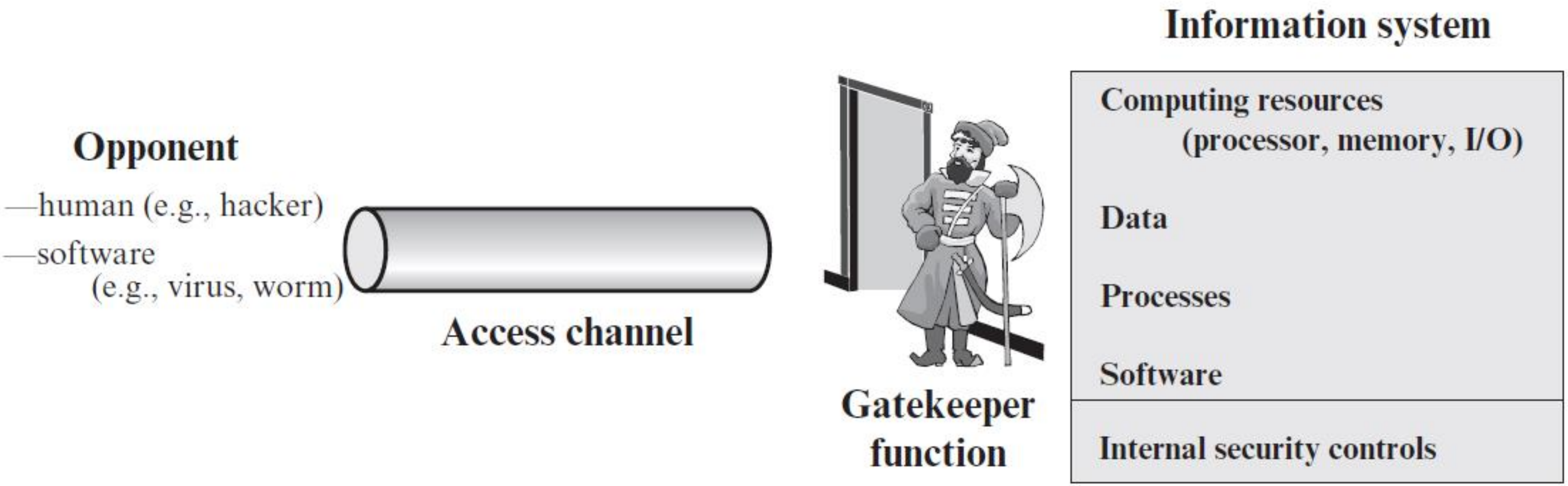
- To achieve the goal, Sender performs some security-related transformation of the message (called ***Encryption***) to convert the original message to a secure message. The Sender uses some secret information (called ***Key***) for the conversion.

- Afterwards, Sender sends the message to the Recipient via the insecurity channel.

Model for Network Security

- Afterwards, Sender sends the message to the Recipient via the insecurity channel.
- Upon receipt, the Recipient performs another security-related transformation of the message (called ***Decryption***) to convert the secure message to the original message. The Recipient uses some secret information (called Key) for the conversion.
- The secured message is such that even though some opponent collects it during the transit, it will not be readable (that is, it would be impossible to get any useful meaning from the secure message).
- **Trusted Third Party** is some kind of service or company that both Sender and Recipient trusts for their secure communications.
- Most often, the Trusted Third Party sends a secret Key to both the Sender and Recipient via pre-established secure communication channels between itself and the Sender and Recipient.

Model for Network Access Security



Model for Network Access Security

- **Information System** is a very important component of any organization or company.
- There may be some legitimate users who may need to access the information system from outside the organization's network through the **Access Channel** (such as, MAN, WAN, or Internet).
- This provides opportunities to the **Opponents** (human opponents such as cybercriminals, and software opponents such as virus, worms) to try to access the information system through the Access Channel.
- **Gatekeeper Functions** are installed at the entry point of the organization's network.
- Such Gatekeeper Functions can be configured in network and security devices and software, such as Routers, Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Gateways.

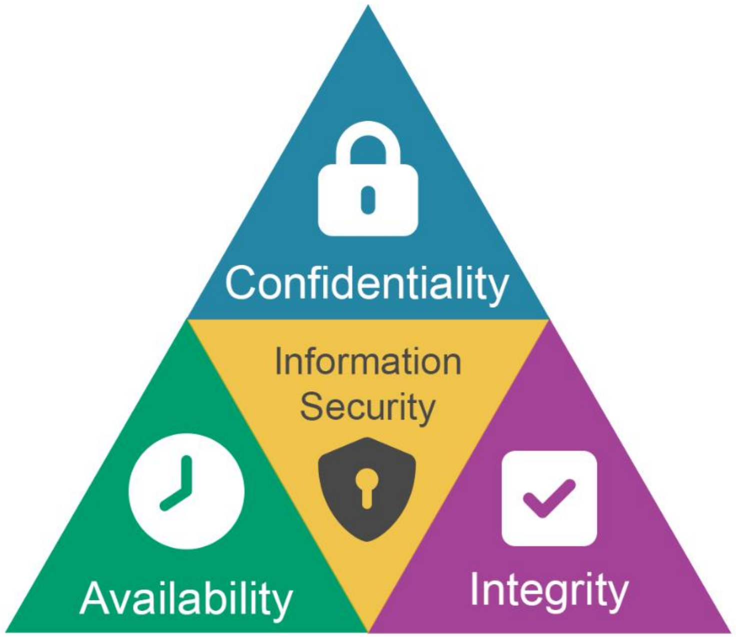
CIA Triad

Confidentiality

- Confidentiality in information security assures that information is accessible only by authorized individuals.
- Encryption mechanisms are effectively used for ensuring confidentiality of information during transmission.

Integrity

- Integrity of information means assuring that data has not been tampered with and can be trusted.
- Measures that protect data integrity comprise encryption, hashing, digital signatures, and digital certificates by trusted certificate authorities (CAs) to organizations to verify their originality to website users.



https://appcheck-ng.com/broken-access-control

CIA Triad

Availability

- Availability indicates that networks, systems, and applications are up and operating. It assures that authorized users have timely, trustworthy access to resources when they are required.
- Multiple things can threaten availability, including hardware collapse or software issues, power failure, natural circumstances beyond one's control, human error, security attacks such as Denial-of-Service (DoS) or DDoS attack
- Measures to help guarantee availability include redundancy in servers, internal networks, applications, hardware fault tolerance, regular software patching, system upgrades, backups, comprehensive disaster recovery plans, etc.