🥇

Reading for L1

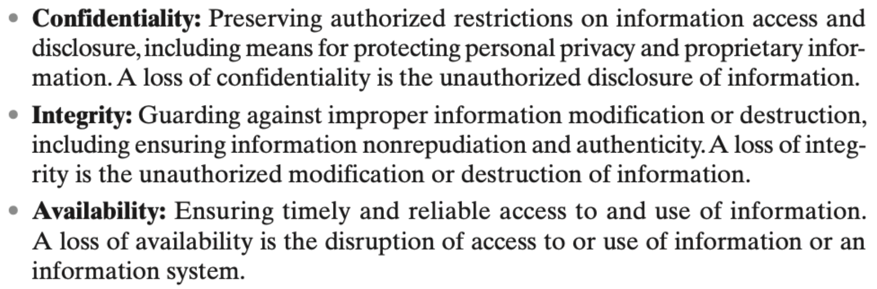
▼ Table of Content

1.1

> 📖 **Computer Security:** Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

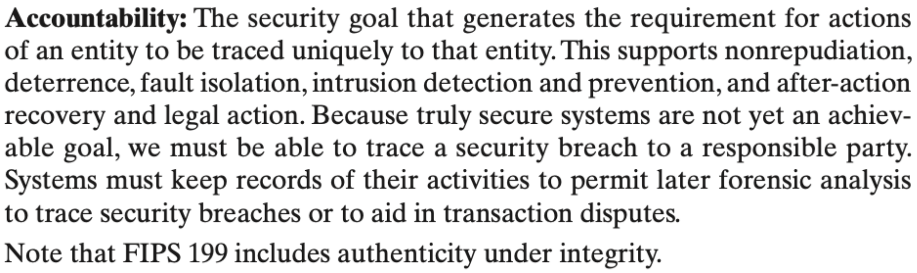
- CIA triad: Concepts that embody the fundamental security objectives for data and information and computer services.
    - Confidentiality: A loss of confidentiality is the unauthorized disclosure of information.
        - Data confidentiality: private or confidential info is not made available to unauthorized individuals.
        - privacy: individuals control/influence what info related to them may be collected and stored, and by whom and whom that information is available to.
    - Integrity: A loss of integrity is the unauthorized modification or destruction of information.
        - data integrity: Assuring data and programs are changed only in a specified and authorized way.

        - system integrity: Assuring a system performs its intended function, free from unauthorized manipulation.
    - Availability: the system works promptly and service is not denied to authorized users.



- **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, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

- There are also additional consepts
    - 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.
    - Accountability:



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. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Note that FIPS 199 includes authenticity under integrity.

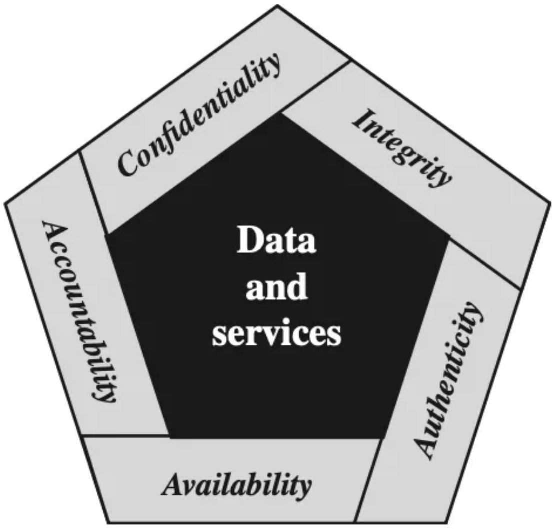


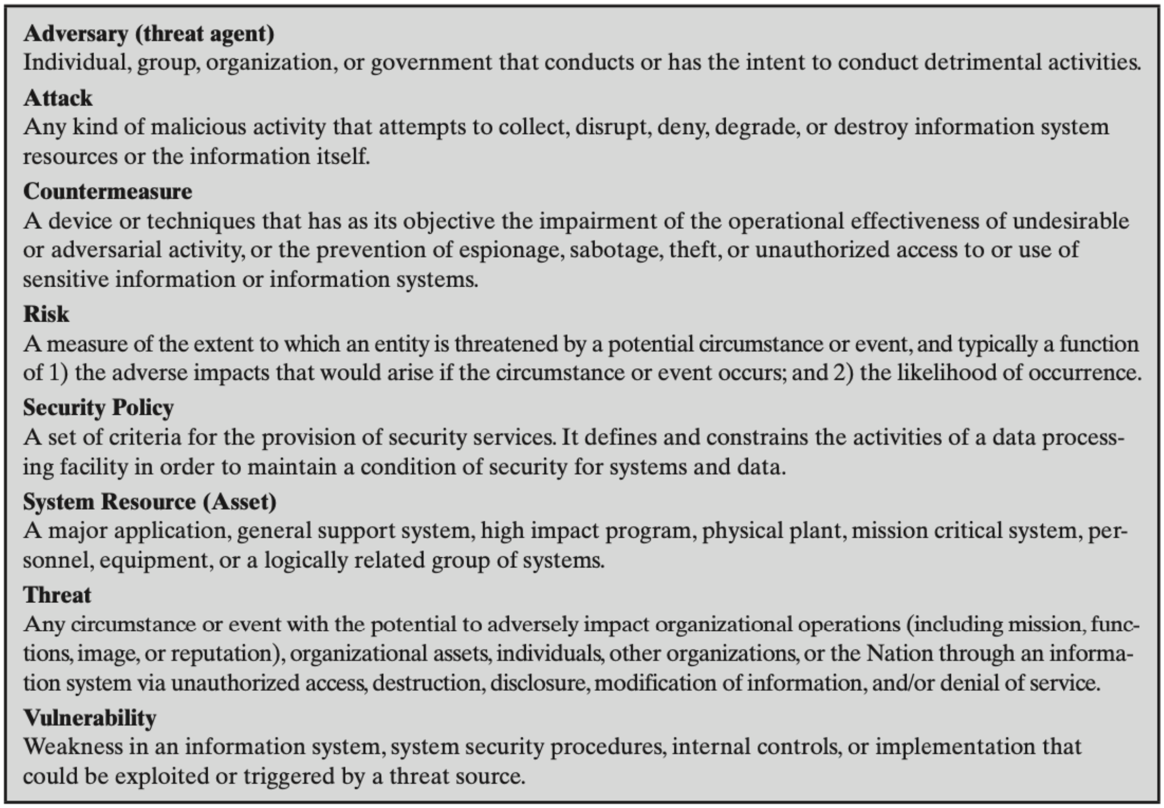
Figure 1.1 Essential Network and Computer Security Requirements

Example given in text uses levels of impact and discusses the different requirements with a respective example of the level of impact:

- confidentiality → Student's grades → low
- Integrity → Hospitals and patient data → high
    - low integrity requirement → online poll
- Availability → public website for university → moderate

- Terminology

Table 1.1 Computer Security Terminology



Adversary (threat agent)
Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Attack
Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Countermeasure
A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Risk
A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence.

Security Policy
A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

System Resource (Asset)
A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Vulnerability
Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

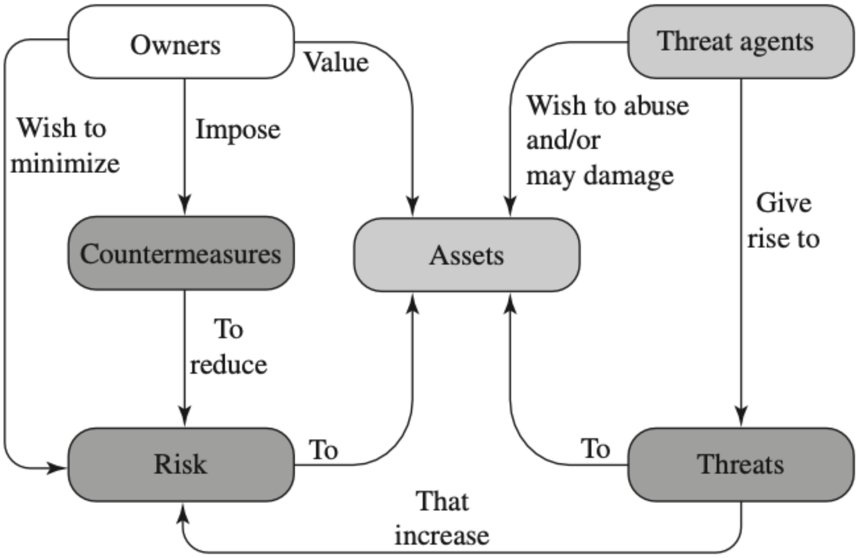
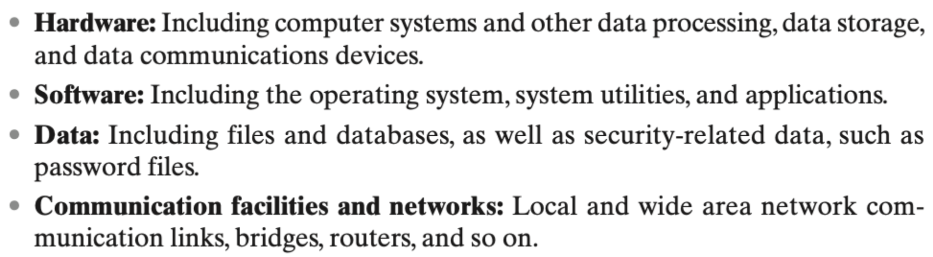


Figure 1.2 Security Concepts and Relationships

- Assets of a computer system:



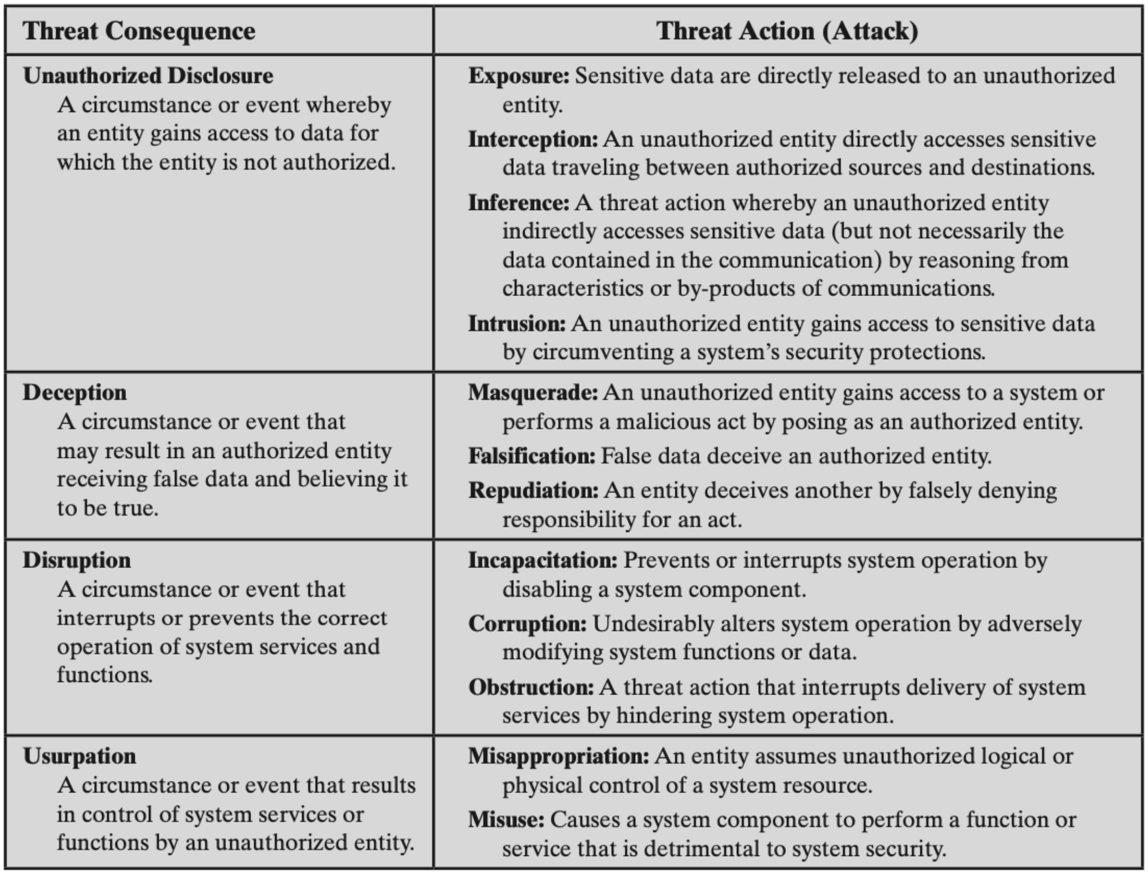
- **Hardware:** Including computer systems and other data processing, data storage, and data communications devices.
- **Software:** Including the operating system, system utilities, and applications.
- **Data:** Including files and databases, as well as security-related data, such as password files.
- **Communication facilities and networks:** Local and wide area network communication links, bridges, routers, and so on.

- Vulnerabilities of a computer system:
  - corrupted system = A system that does the wrong thing or gives a wrong answer.
  - leaky system = unauthorized users have access to information through the network.
  - unavailable /very slow system = using the system or network becomes impossible or impractical.
- Attacks:
  - Active attack = an attempt to alter system resources or affect their operation.
  - Passive attack = An attempt to learn or make use of information from the system that does not affect system resources.
- Based of the origin of the attack
  - Inside attack = initiated by an entity inside the security perimeter, an insider has authorization but uses it in an unauthorized manner.
  - outside = initiated from an outside perimeter.

1.2

- **Unauthorized disclosure ⇔ threat to confidentiaity**

Table 1.2 **Threat Consequences, and the Types of Threat Actions that Cause Each Consequence**



Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

- Assets can be chategorised as
  - Hardware: A threat to hardware is the threat to availability. Hardware is the most vulnerable to attack and the least susceptible to automated controls. Threats include accidental and deliberate damage to equipment as well as theft. Physical and administrative security measures are needed to deal with these threats.
  - Software: A **key threat** to software is an attack on availability. Software, especially application software, is often easy to delete. Software can also be altered or damaged to render it useless. Careful software configuration management, which includes making backups of the most recent version of software, can **maintain high availability**. A more difficult problem to deal with is **software modification that results in a program that still functions but that behaves differently** than before, which is a threat to integrity/authenticity. Computer **viruses and related attacks** fall into this category. Another problem is **software piracy**, which is yet to be solved.

  - Data: Data security involves files and other forms of data controlled by individuals, groups, and business organizations. Security concerns with respect to data are broad, encompassing availability, secrecy, and integrity. In the case of availability, the concern is with the destruction of data files, which can occur either accidentally or maliciously.

    The obvious concern with secrecy is the unauthorized reading of data files or databases, and this area has been the subject of perhaps more research and effort than any other area of computer security. **A less obvious threat** to secrecy involves the analysis of data and manifests itself in the use of so-called statistical databases, which provide summary or aggregate information.
    Finally, data integrity is a major concern in most installations. Modifications to data files can have consequences ranging from minor to disastrous.

  - Communication lines and network: Network security attacks can be classified as *passive attacks* and *active attacks*.

    - **Passive attacks** are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the attacker is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic
      analysis.
      A second type of passive attack,
      traffic analysis, is more subtle. The common technique for masking contents is **encryption**, however the encryption can still be cracked if an opponent ses the pattern.

      Passive attacks are very difficult to detect because they do not involve any alteration of the data. Typically, the message traffic is sent and received in an apparently normal fashion and neither the sender nor receiver is aware that a third party has read the messages or observed the traffic pattern. However, it is feasible to prevent the success of these attacks, usually by means of **encryption**. Thus, the emphasis in dealing with passive attacks is on prevention rather than detection.

        - **Active attacks** involve some modification of the data stream or the creation of a false stream, and can be subdivided into four categories:
            - replay: involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.
            - masquerade: when one entity pretends to be a different entity, usually includes one of the other forms of active attack.
            - modification of messages: some portion of a legitimate message is altered, or that messages are delayed or reordered, to produce an unauthorized effect.
            - denial of service: prevents or inhibits the normal use or management of communication facilities. This attack may have a specific target. Another form of service denial is the disruption of an entire network.
        - Active attacks present the opposite characteristics of passive attacks. it is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

1.4

- Fundamental security principles (As described by US homeland security)
    - Economy of mechanism:
        - security measures in both hardware and software should be designed to be as simple and small as possible. Simpler designs are easier to test, verify, and maintain.
        - The goal is to minimize unnecessary complexity during system design to enhance security and reduce potential vulnerabilities.
    - Fail-safe defaults:
        - access decisions should be based on permission rather than exclusion. In this approach, the default state is no access, and the

        system explicitly defines the conditions under which access is granted.

        - This makes mistakes easier to detect and correct.

    - Complete mediation:

        - requires every access to a resource to be checked against the access control mechanism, without relying on previously cached access decisions. This means that the system should verify permissions each time access is requested, ensuring that changes in user authority are immediately reflected and enforced.

        - True complete mediation would involve re-evaluating permissions every time a user interacts with data, but this is resource-intensive and is rarely fully implemented in most systems.

    - Open design

    - Separation of privilege

    - Least privilege

    - Least common mechanism

    - Psychological acceptability

    - Isolation

    - Encapsulation

    - Modularity

    - Layering

    - Least astonishment

1.6

A comprehensive security strategy involves three aspects:

- **Specification/policy:** What is the security scheme supposed to do?

- a security policy is a formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources, enforced by the system's technical controls as well as its management and operational controls.
- Concidering the following factors:
  - The value of the assets being protected
  - The vulnerabilities of the system
  - Potential threats and the likelihood of attacks
- As well as, the following trade-offs:
  - **Ease of use vs security:**
    The trade-off between making systems secure and ensuring they remain user-friendly.
    In general, stronger security measures often result in a more complex or slower user experience, requiring a balance between both aspects.
  - **Cost of security vs cost of failure and recovery:**

    Balance between the expenses involved in implementing and maintaining security measures and the potential costs associated with security breaches and recovery.

    When evaluating security costs, it's important to consider:

    - **Direct monetary costs**: These include the expenses related to security implementation, maintenance, and ongoing management.
    - **Cost of failure and recovery**: This includes the value of the assets being protected, the damages from a breach, and the risk involved, which is the probability of a threat exploiting a vulnerability and causing harm.

    The key is to weigh the costs of preventive security measures against the potential financial and operational impact of a security failure, taking into account both the likelihood and severity of possible breaches.

- **Implementation/mechanisms:** How does it do it?

involves four complementary actions to protect systems:

1. **Prevention**: The goal is to stop attacks before they happen. For instance, using secure encryption and safeguarding encryption keys can prevent unauthorized access to transmitted data, protecting confidentiality.
2. **Detection**: Since absolute security isn't always possible, detecting attacks is essential. For example, intrusion detection systems identify unauthorized access, and systems can detect denial of service (DoS) attacks, where resources are overwhelmed.
3. **Response**: When an attack is detected, systems can respond to mitigate the damage. For instance, during a DoS attack, the system might take measures to stop the attack and prevent further disruption.
4. **Recovery**: After an attack, recovery mechanisms, like backup systems, allow the restoration of compromised data to a prior, correct version, ensuring system integrity is regained.

Together, these actions provide a comprehensive approach to managing security risks.

- **Correctness/assurance:** Does it really work?

  Assurance and Evaluation in Computer Security are key concepts that ensure security systems meet requirements and enforce policies effectively.

  - **Assurance** is the confidence that a system's security measures work as intended. It examines whether both the design and implementation of the system meet security requirements. Assurance is expressed as a degree of confidence, not as absolute proof, because it's not yet possible to prove designs or implementations are entirely correct. Assurance is built through formal models, logical, and mathematical techniques, but remains a matter of degree.
  - **Evaluation** is the process of assessing a computer system or product against specific security criteria. This involves testing and may include formal analysis. The goal is to develop standardized criteria that can be applied to any security system, enabling comparisons between products and ensuring they meet agreed-upon security standards.

Together, assurance and evaluation help security "consumers" (like system managers, vendors, and users) trust that security measures are effective and meet security policies.