Overview of Information Security

The slides are adapted from the slides of UT Dallas Murat Kantarcioglu

Information Protection - Why?

- Information are an important strategic and operational asset for any organization
- Damages and misuses of information affect not only a single user or an application; they may have disastrous consequences on the entire organization
- Additionally, the advent of the Internet as well as networking capabilities has made the access to information much easier

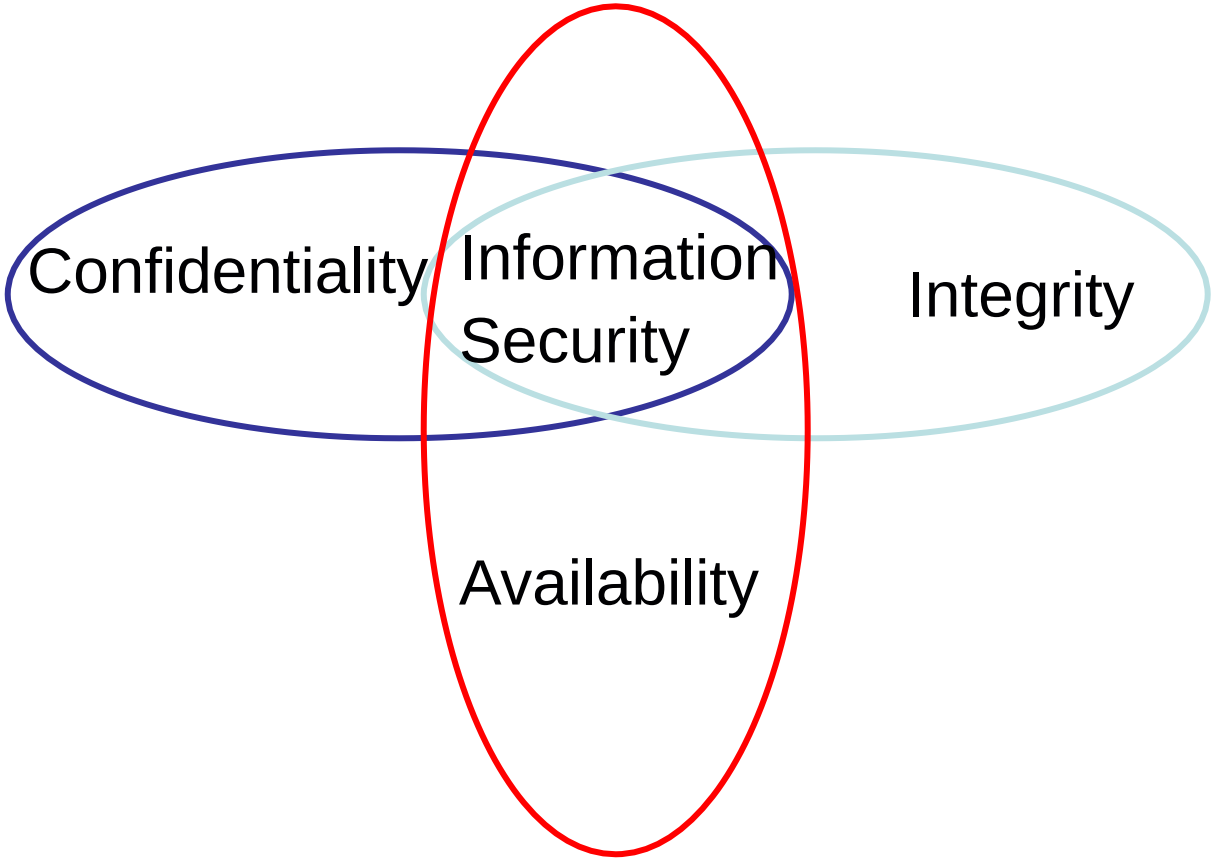
What Is Security?

The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information

- Includes information security management, data security, and network security

- Security Principles
  - C.I.A. triangle: Is a standard based on Confidentiality, Integrity, and Availability, Security Principles

Information Security: Main Requirements



Information Security: Examples

- Consider a payroll database in a corporation, it must be ensured that:
  - salaries of individual employees are not disclosed to arbitrary users of the database
  - salaries are modified by only those individuals that are properly authorized
  - paychecks are printed on time at the end of each pay period

Information Security: Examples

- In a military environment, it is important that:
  - the target of a missile is not given to an unauthorized user
  - the target is not arbitrarily modified
  - the missile is launched when it is fired

Information Security - main requirements

- *Confidentiality* - refers to information protection from unauthorized read operations
  - the need for keeping information secret arises from the use of computers in sensitive fields such as government and industry.
  - How to support confidentiality?
    - Access control mechanisms
    - Cryptography
- The term *privacy* is often used when data to be protected refer to individuals
  - Privacy restricts the public from accessing the personal details about a person, whereas Confidentiality protects the information from the range of unauthorized persons

Information Security - main requirements

- Confidentiality also applies to the existence of data, which is sometimes more revealing than the data itself.
  - Access control mechanisms sometimes conceal the mere existence of data, lest the existence itself reveal information that should be protected.
- Resource hiding: for example: Sites often wish to conceal their configuration as well as what systems they are using

Information Security - main requirements

- *Integrity* – is the accuracy, consistency, and trustworthiness of data during its entire life cycle.
  - refers to information protection from modifications or unauthorized change;
  - it involves several goals:
    - Origin integrity: the source of the data
      - Assuring the integrity of information with respect to the origin (relevant especially in web environment) – often referred to as authenticity
    - Data integrity: the content of the information
      - Protecting information from unauthorized modifications
      - Protecting information from incorrect modifications – referred to as *semantic integrity*

Integrity mechanisms

Prevention mechanisms

- seek to maintain the integrity of the data by blocking
  - any unauthorized attempts to change the data
    - Can be stopped using adequate authentication and access controls
  - any attempts to change the data in unauthorized ways

Integrity mechanisms

Detection mechanisms

- report that the data's integrity is no longer trustworthy
  - analyze system events (user or system actions) to detect problems
  - analyze the data itself to see if required or expected constraints still hold.
- Report either
  - the actual cause of the integrity violation.
  - the file is now corrupt

Integrity

Evaluating integrity is often very difficult

- because it relies on assumptions about the source of the data and about trust in that source

Integrity includes both the correctness and the trustworthiness of the data.

- The origin of the data (how and from whom it was obtained),
- How well the data was protected before it arrived at the current machine, and
- How well the data is protected on the current machine

Information Security - main requirements

- *Availability* – the need to maintain availability of information systems and services at all times
  - it ensures that access to information is not denied to authorized subjects
  - The aspect of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable.
  - Denial of service attacks
    - Attempts to block availability

EXAMPLE: Suppose Anne has compromised a bank's secondary system server, which supplies bank account balances. When anyone else asks that server for information, Anne can supply any information she desires. Merchants validate checks by contacting the bank's primary balance server. If a merchant gets no response, the secondary server will be asked to supply the data. Anne's colleague prevents merchants from contacting the primary balance server, so all merchant queries go to the secondary server. Anne will never have a check turned down, regardless of her actual account balance. Notice that if the bank had only one server (the primary one), this scheme would not work. The merchant would be unable to validate the check.

Information Security - main requirements

We can say that an asset (resource) is available if:

- Timely request response
- Fair allocation of resources (no starvation!)
- Fault tolerant (no total breakdown)
- Easy to use in the intended way
- Provides controlled concurrency (concurrency control, deadlock control, ...)

Methods used to ensure availability include:

- system redundancy
- system backups
- increased system resiliency (flexibility)
- equipment maintenance
- up-to-date operating systems and software
- plans in place to recover quickly from unforeseen disasters.

Threats

- *Threat* – a potential violation of security
  - The fact that the violation might occur means that those actions that could cause it to occur must be guarded against.

- *Classes of Threats:*
  - Disclosure: unauthorized access to information
  - Deception: acceptance of false data
  - Disruption: interruption or prevention of correct operation
  - Usurpation: unauthorized control of some part of a system

Threats

- Snooping: form of disclosure
  - unauthorized interception of information
  - *Passive Wiretapping* is a form of snooping in which a network is monitored
- Confidentiality services counter this threat

Threats

- Modification or Alteration
  - form of deception:
    - some entity relies on the modified data to determine which action to take
    - incorrect information is accepted as correct and is released
  - form of disruption and usurpation:
    - the modified data controls the operation of the system
  - *Example: Active Wiretapping*
    - *man-in-the middle* attack
  - Integrity services counter this threat

Threats

- *Masquerading* or *spoofing*
  - impersonation of one entity by another
  - form of deception and usurpation:
  - Integrity services counter this threat
    - Authentication services
- Spoofing vs Delegation

Threats

- *Repudiation of origin*
  - false denial that an entity sent (or created) something
  - form of deception
  - Integrity mechanisms deal with this threat

Threats

- *Denial of receipt*
  - false denial that an entity received some information or Message
  - form of deception
  - Integrity and availability mechanisms deal with this threat

Threats

- *Delay*
  - a temporary inhibition of a service
  - form of usurpation
    - Sometimes deception
  - Availability mechanisms deal with this threat

Threats

- *Denial of service*
  - a long-term inhibition of service
  - form of usurpation
  - The attacker prevents a server from providing a service.
  - Different types:
    - At source:
      - preventing the server from obtaining the resources needed to perform its function),
    - At destination:
      - blocking the communications from the server
    - At intermediate path
      - discarding messages from either the client or the server, or both
  - Infinite delay
  - Availability mechanisms counter with this threat