Computer Systems Security

Introduction – Lesson 1

Security Requirements

- The needs for information security described under:
  - Confidentiality: Controls who gets to access information.
  - Integrity: Controls how the information changes
  - Authentication: Determining who is responsible for a request
  - Authorization: Ensuring that only who is trusted to utilize the service gets access to it.
  - Non-repudiation:
  - Availability: Providing access to information when needed.

Confidentiality

- Controls who gets to access information.
- Seeks to keep information from being disclosed to unauthorized recipient.
- Information usually classified at levels of sensitivity and isolated compartments
- Access strictly on “need to know” basis
- Discretionary classification: Information has an owner. The owner determine who can access/see the information.

Integrity

- Controls how the information changes
- Information is maintained in a valid and intended state.
- Keeps information from being changed improperly.
- Not synonymous with accuracy

Authentication

- Necessary to know what sort of entities can be responsible for statements.
- Determines who is responsible for a request.
- Entities can be human or computer. They are collectively known as ***principals***.

Availability

- Seeks to ensure that the system works promptly
- The system can provide information even in the event of malicious attacks or environmental mishaps.

Authorization

- Determines who is trusted for a given purpose/role/ activity i.e. determines whether a particular principal, who has been authenticated as the source of a request to do something, is trusted for that operation.
- Can include controls on time limits, source terminal etc.
- Important task should not be undertaken by one person

Non-repudiation

- Ensures that a principal upon having made access to an information resource, will not later be able to claim that the statement (or accesss) was forged and he/she never made it.

- Example in the manual environment???