Computer Security

Security Concepts

What is Computer Security?

- X.800* Security Services:
  - Authentication
  - Access Control
  - Data Confidentiality
  - Data Integrity
  - Non-repudiation

* International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) Recommendation X.800, *Security Architecture for OSI (Open Systems Interconnection)*, RFC 2828 (`http://www.ietf.org/rfc/rfc2828.txt`)

Authentication

- Is a communication authentic?
  - For messages:
    - Assures recipient of a message that the message really is from the source it claims to be from.
  - For connections:
    - Assures both entities involved in a connection that each entity is authentic (determined at connection initiation)
    - Assures no interference with a connection during the life of that connection
    - Assures that no third party can masquerade as one of the two entities.

Access Control

- Can an entity (user, computer) access resources?
  - Host systems
  - Communications links
  - Applications
  - Files
  - etc.
- Typically, access rights are tailored to each individual entity
  - Clearly depends on accurate authentication of an entity!

Data Confidentiality

- Is data (for example, in messages) held confidential to the appropriate set of entities?
  - Once accessed, is the data readable by a third party?
  - Can file contents be read?
  - Can a third party eavesdrop on messages sent between entities?

Data Integrity

- Is data secure from accidental or deliberate changes?
  - If an entity sends a series of messages, do they arrive in the proper order, and do they contain the original contents?
  - Can a third party change the contents of a message, file, database, etc?

Non-repudiation*

- Can an entity deny that a completed action never took place, when it really did?
  - Like someone trying to deny having signed a contract
  - Assures that the sending or receiving of a message by the entity can be proven to have actually happened

***re·pu·di·ate**
1 : to divorce or separate formally from (a woman)
2 : to refuse to have anything to do with
3 a : to refuse to accept; *especially* **:** to reject as unauthorized or as having no binding force
b : to reject as untrue or unjust <*repudiate* a charge>
4 : to refuse to acknowledge or pay

What is Computer Security?

- X.800 Security Mechanisms, including:
  - Encipherment (or Encryption)
  - Digital Signature
  - Access Control
  - Data Integrity
  - Authentication Exchange
  - Notarization
  - Audit Trails

Encipherment (or Encryption)

- The use of mathematical algorithms to transform data into a form that is not readily readable by third parties.
  - The original data is readily readable, and is known as *cleartext*, or *plaintext*
  - The enciphered data is not readily readable, and is known as *ciphertext*.
  - Transforming ciphertext back into its original cleartext is known as *decipherment* or *decryption*.

Digital Signature

- Data attached to, or a cryptographic transformation of, data which allows the recipient to ensure the source and integrity of the data, and to protect against forgery.
  - Corresponds to a handwritten signature on an official document

Access Control

- Mechanisms to enforce access rights to resources
  - Typically implemented (usually by an operating system) as access control lists (ACLs) associated with each resource (such as a file)
  - An ACL specifies which entities have what kind of access (read only, read-write, etc.) to the resource.

Data Integrity

- Mechanisms used to assure the integrity of data.
  - In communications, assures that a series of messages sent to a recipient arrive in the proper order, and containing the original contents
  - In databases. assures that the relationships among data items within a database are valid (correspond to the business rules of the organization), and remain valid over time, despite updates to the database.

Authentication Exchange and Notarization

- Authentication Exchange
  - Mechanism to ensure the identity of one or more entities by appropriate exchange of information
- Notarization:
  - The use of a trusted third party to assure authentication and data integrity
  - Analogous to a Notary Public in signing public documents.

Audit Trails

- Data collected to track security-related events in a system
  - Can be used to verify (or otherwise) the security of a system in a security audit.
  - Essential for security experts to be able to detect a security breach, and track down the perpetrator(s)

Security Attacks

- Passive Attack
  - Attempt to gain information without changing contents of messages or state of system
- Active Attack
  - Attempt to change contents of messages or change the state of a system or impact its operation.

Passive Attack

- Eavesdropping or monitoring of transmissions
  - Direct:
    - Reading message contents
  - Indirect:
    - Use of traffic analysis to determine patterns which can help the perpetrator to guess the nature of the communication.
    - More subtle
  - Very difficult to detect
  - Usually, encryption used for prevention

Active Attack

- Involves modification or alteration of message or system
  - Types:
    - Masquerade
    - Replay
    - Modification of Messages
    - Denial of Service
  - Easier to detect, but harder to prevent.