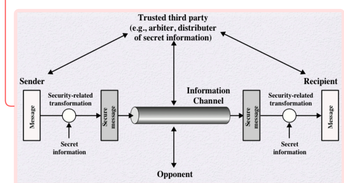
Network Security

Concepts

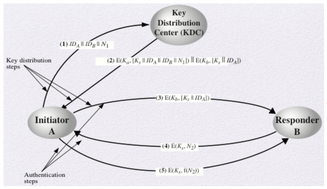
- **Cryptographic Algorithms**
  - **Symmetric Encryption** — Used to conceal the contents of blocks or streams of data of any size
  - **Asymmetric Encryption** — Used to conceal small blocks of data
    - such as encryption keys
    - and hash function values
    - which are used in digital signatures
  - **Data Integrity Algorithms** — Used to protect blocks of data — such as messages — from alteration
  - **Authentication Protocols** — use of cryptographic algorithms — designed to authenticate the identity of entities
- **Network Security** — measures to
  - deter
  - prevent
  - detect
  - correct
  - security violations — that involves the transmissions of information
- **Computer Security Objectives**
  - **Confidentiality**
    - Data confidentiality — Assures that private or confidential information is not made available or disclosed to unauthorized individuals
    - Privacy — Assures that individuals control or influence what information related to them
      - may be collected and stored and by whom
      - and to whom that information may be disclosed
  - **Integrity**
    - Data integrity — Assures that information and programs are changed only in a specified and authorized manner
    - System integrity — Assures that a system performs its intended function in an unimpaired manner
  - **Availability** — Assures that systems work promptly and service is not denied to authorized users
- **Security Requirements** — these and
  - **Authenticity**
  - **Accountability**
- **OSI Security Architecture**
  - Security **Attack** — Any action that compromises the security of information owned by an organization
  - Security **Mechanism** — A process (or a device incorporating such a process) — that is designed to
    - detect
    - prevent
    - recover
    - from a security attack
  - Security **Service** — processing or communication service
    - that enhances the security of the data processing systems
    - and the information transfers of an organization
    - Intended to counter security attacks — and they make use of one or more security mechanisms to provide the service
- **Threats & Attacks**
  - **Threat** — potential for violation of security
  - **Attack** — assault on system security
    - 2 types
      - **passive** attacks
        - attempts to learn or make use of information — does not affect system resources
        - like
          - The release of message contents
          - Traffic analysis
      - **active** attack
        - attempts to alter system resources or affect their operation
        - like
          - **Masquerade** — one entity pretends to be a different entity
          - **Replay** — passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect
          - **Modification of messages** — message is altered, or messages are delayed or reordered to produce an unauthorized effect
          - **Denial of service** — Prevents or inhibits the normal use or management of communications facilities



Network Security Model

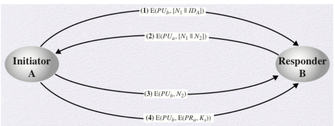
Key Management and Distribution

- **Key Distribution Technique**
  - **definition**
    - refers to the means of delivering a key
      - to two parties who wish to exchange data
      - without allowing others to see the key
  - For **symmetric** encryption to work
    - two parties to an exchange must share the **same** key
      - and that key must be **protected** from access by others
  - Frequent key changes are desirable
    - to limit the amount of data compromised
      - if an attacker learns the key

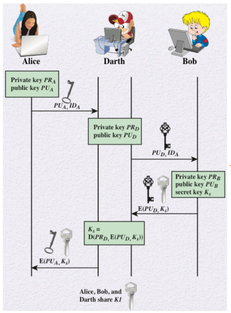


Key Distribution Scenario

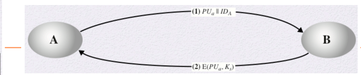
- **Hierarchical Key Control**
  - means that Local KDC (Key Distribution Center)
    - is responsible for local key distribution
  - but if they are in different domain
    - local KDCs communicate with global KDCs
- **Session Key Lifetime**
  - security manager must balance competing considerations
    - The distribution of session keys
      - delays the start of any exchange
        - the more frequently session keys are exchanged
          - the more secure they are



public key distribution of secret keys

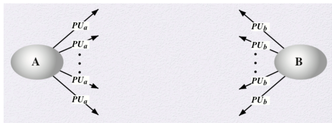


Man in the Middle Attack

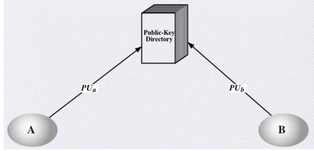


use of public key encryption to make a session key

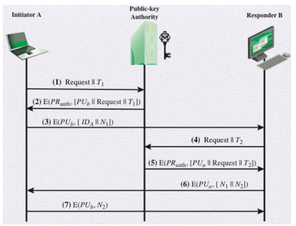
- **Public announcement**



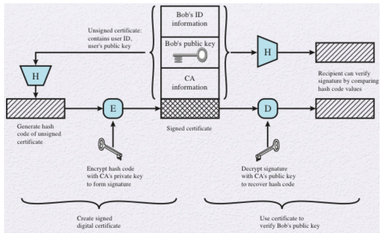
- **Publicly available directory**



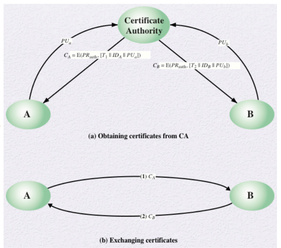
- **Public-key authority**

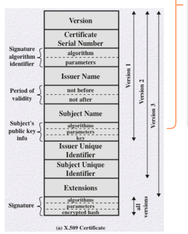


- **Distribution of public keys**
  - **use of it**



- **Public-key certificates**





different versions of 509 certificate

For more MindMaps
Check our Blitz Website
https://blitz.deveopix.com/

Created by
Omar Alkhateeb

Presented with xmind