Today’s plan: Some Review

- Properties
- Policies
- Mechanisms

Today’s plan: Review concepts in a more abstract way

- Properties: CIA
  - Confidentiality
  - Integrity
  - Availability

Properties

- **Confidentiality**: concealment of information
  - The need arises from sensitive fields (military, industry)
  - Examples: encryption (protect the key), access control, **existence of the data**, private information, resource hiding

Properties

- **Integrity**: prevent unauthorized or improper changes, is directly related to trustworthiness of data and sources
  - Include data integrity and origin integrity
  - Prevention:
    - prevent unauthorized changes
    - changes in unauthorized ways
  - Detection
    - Report integrity violation (confine dirty data??)

Properties

- **Availability**: ability to use the data or resources
    - Example of highway
    - DoS or DDoS attacks
    - Very difficult to detect
        - Is it attack or we are unlucky today
        - Attacker will mess with the security methods as well (packet tracing)

Threats

- **Threats**
  - A potential violation of security (not necessarily occur at this moment).
    - The actions that cause such violations are called attacks.
    - 4 classes of threats:
      - Disclosure: unauthorized access to data
      - Deception: acceptance of false data
      - Disruption: interruption or prevention of correct operation
      - Usurpation: unauthorized control of the system

Threats

- **Examples of threats:**
  - **Snooping**: unauthorized interception, is a kind of disclosure (eavesdrop on wireless). Countered by confidentiality or other information hiding methods.
  - **Modification**: unauthorized change of data, may lead to deception, disruption, and usurpation. Countered by integrity.
  - **Spoofing**: impersonation, may lead to deception and usurpation. Countered by integrity.
  - **Denial of receipt or origin**: is a kind of deception

Policies and Mechanisms

- Policy is a statement of what is and what is not allowed.
  - When two communicating parties have different policies, they may need to compromise (example b/w univ. and industry)
- Mechanism is a method to enforce a policy.
  - May (often) impact the system performance
  - Prevention: to fail an attack
  - Detection
  - Recovery: fix not only data, but also vulnerabilities
  - Tolerance

Example Policies & Mechanisms

- Policies examples
  - Our course policies: e.g., no cheating is allowed
  - Confidentiality: Eavesdropper (e.g., Eve) should not be able to see the content of messages between two parties (e.g., Alice and Bob)
  - Integrity: A manipulator (e.g., Mallory) should not be able to modify the messages without being noticed
  - Availability: The server (e.g., AWS) should be able to function 99.99% of the time
- Mechanisms: what we are learning mostly
  - Cryptographic techniques
  - Access control
  - Isolation
  - Secure programming and testing

Assumptions:

- Security rests on assumptions of the required security and application environments
- Assumptions of a security policy
    - A policy can correctly and unambiguously partitions system states into secure and insecure
    - A security mechanism will prevent a system from entering an insecure state
    - Examples:
        - Symmetric key encryption is secure, assumption?
        - Asymmetric key encryption is secure, assumption?