What is Security?

- Can not be by-passed (complete mediation)
- Should handle threats (threat model)
  - External
  - Internal
- Has trust boundaries (trusted computing base),
  - Desired small TCB
- Takes care of consequences and mitigation
- What are v protecting
- What property is being protected

"Security is the study of computing in the presence of an adversary"
Security Goals

- Availability
  - Those who are entitled to access can access the data
  - Can be denied by "denial of service" attacks. Could be due to:
    - Network bandwidth exhaustion
    - Man in the middle attack
    - OS resources
    - System crash due to bad inputs (king of death)
    - CPU time, ram, disk

- Secrecy
- Maintain anonymity

- Examples of confidential data:
  - password, encryption key, cookies, contacts, source code, credit card info etc
Security Goals contd...

- Integrity
- Data should be modified only in authorized ways
  - Authentication is a tool in security. It helps to:
    - Identify users
    - Identify property of the users
    - Examples of data which should preserve integrity:
      - Database contents
      - Source code
    - Could be violated by passive attack (modify a message in transit)
Threat Model

- Defines power and limits of attacker. These could be:
  - Computation
  - Access
  - Remote vs local
  - Bandwidth
  - Time
  - Knowledge of defenses
    - Example: password, login, os, browser, encryption keys and algorithms, source code (everything except explicitly denoted secrets like password, encryption keys, random numbers etc)