Security as a Architectural Concern

Reid Holmes
NFP: Security

- Security: “The protection afforded a system to preserve its integrity, availability, and confidentiality if its resources.”

- Confidentiality
  - Preserving the confidentiality of information means preventing unauthorized parties from accessing the information or perhaps even being aware of the existence of the information.

- Integrity
  - Maintaining the integrity of information means that only authorized parties can manipulate the information and do so only in authorized ways.

- Availability
  - Resources are available if they are accessible by authorized parties on all appropriate occasions.
Security arch. principles

- Least privilege:
  - Give each component only the privileges it requires.

- Fail-safe defaults
  - Deny access if explicit permission is absent.

- Economy of mechanism
  - Adopt simple security mechanisms.

- Open design
  - Secrecy ≠ security.
Security arch. principles

- Separation of privilege
  - Introduce multiple parties to avoid exploitation of privileges.

- Least common mechanism
  - Limit critical resource sharing to only a few mechanisms.

- Psychological acceptability
  - Make security mechanisms usable.

- Defence in depth
  - Have multiple layers of countermeasures.