Course Logistics

- Read chapter 13.
- FEAU?
Design Principles for Secure Systems

- Two basic themes:
  - Simplicity – KISS
    - Makes design and interactions easy
    - Easy to prove its safety
    - Example: Sendmail – Not!
  - Restriction
    - Minimize the power of entities
    - NTK & Compartmentalization
    - Inmates of a prison

- Also, one needs a healthy dose of (un)Common Sense!
Principles of design

1. Principle of least privilege
2. Principle of fail-safe defaults
3. Principle of economy of mechanism
4. Principle of complete mediation
5. Principle of open design
6. Principle of separation of privilege
7. Principle of least common mechanism
8. Principle of psychological acceptability
Principle of least privilege

- Entity should be given only those privilege needed to finish a task
  - Function/role should control the rights
  - Temporary elevation of privilege should be relinquished immediately
  - Granularity of privileges
  - Unix root and Windows Administrator.
  - Append permission only for logging process.
Principle of fail-safe defaults

- Unless a subject is given explicit access to an object, it should be denied access to the object.
  - Default access to an object is *none*
  - If subject is unable to complete its task before it terminates it should undo changes made to the state of the system.
- Mail server example
- Restricting privileges at the time of creation
Principle of economy of mechanism

- Security mechanism should be as simple as possible.
  - Fewer errors
  - Testing and verification is easy
  - Assumptions are less

- Interface to modules
  - Implicit assumptions of modules
  - Finger example
Principle of complete mediation

- All accesses to objects should be checked to ensure they are allowed.
  - UNIX file descriptor.
  - DNS cache poisoning.
  - Restrict caching policies
  - Security vs. performance issues
Principle of open design

- Security of a mechanism should not depend upon secrecy of its design or implementation
  - Secrecy $\neq$ security
  - Complexity $\neq$ security
  - “Security through obscurity”
  - Cryptography and openness
  - DeCSS, DMCA, RIAA
Principle of separation of privilege

- System should not grant permission based on single condition
  - Company checks over $75,000 to be signed by two officers.
  - Example: “su” on BSD requires
    1. User be in group “wheel”
    2. User knows root password
  - Restrictive because it limits access
Principle of least common mechanism

- Mechanisms used to access resources should not be shared
  - Restrictive because it limits sharing
  - Amazon website – Denial of service attacks!!
Principle of psychological acceptability

- Security mechanism should not make the resource difficult to access
- Recognizes the most important element in computer security? Human