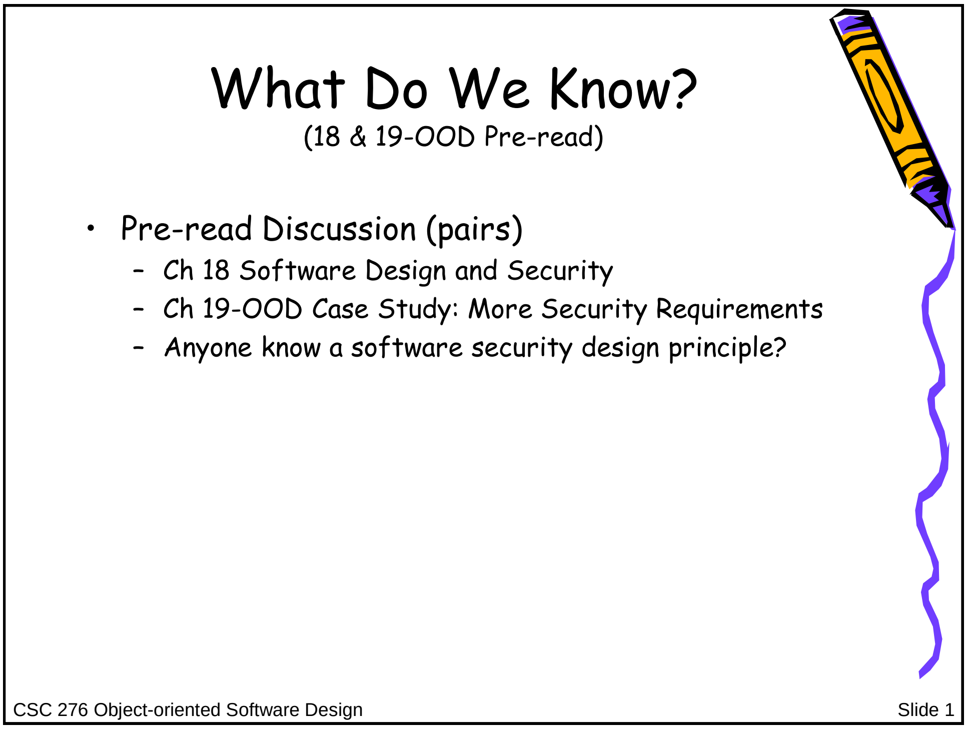
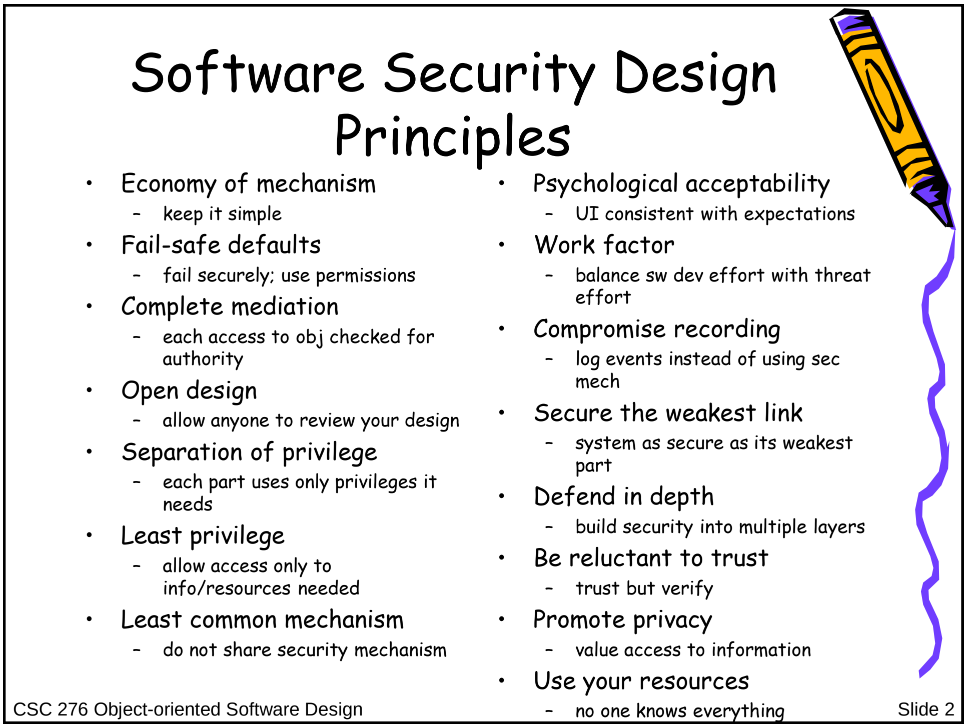


What Do We Know?

(18 & 19-OOD Pre-read)

- Pre-read Discussion (pairs)
  - Ch 18 Software Design and Security
  - Ch 19-OOD Case Study: More Security Requirements
  - Anyone know a software security design principle?



Software Security Design Principles

- Economy of mechanism
  - keep it simple
- Fail-safe defaults
  - fail securely; use permissions
- Complete mediation
  - each access to obj checked for authority
- Open design
  - allow anyone to review your design
- Separation of privilege
  - each part uses only privileges it needs
- Least privilege
  - allow access only to info/resources needed
- Least common mechanism
  - do not share security mechanism
- Psychological acceptability
  - UI consistent with expectations
- Work factor
  - balance sw dev effort with threat effort
- Compromise recording
  - log events instead of using sec mech
- Secure the weakest link
  - system as secure as its weakest part
- Defend in depth
  - build security into multiple layers
- Be reluctant to trust
  - trust but verify
- Promote privacy
  - value access to information
- Use your resources
  - no one knows everything