

## Outline for October 30, 2024

**Reading:** *text*, §18

**Due:** Homework 3, due November 6; Project progress report, due November 8 (Note extension)

---

1. Standards
  - (a) CVE
  - (b) CWE
2. Penetration Studies
  - (a) Goals
  - (b) Where to start
    - i. Unknown system
    - ii. Known system, no authorized access
    - iii. Known system, authorized access
3. Flaw Hypothesis Methodology
  - (a) System analysis
  - (b) Hypothesis generation
  - (c) Hypothesis testing
  - (d) Generalization
4. System Analysis
  - (a) Learn everything you can about the system
  - (b) Learn everything you can about operational procedures
  - (c) Compare to other systems
5. Hypothesis Generation
  - (a) Study the system, look for inconsistencies in interfaces
  - (b) Compare to other systems' flaws
  - (c) Compare to vulnerabilities models
6. Hypothesis testing
  - (a) Look at system code, see if it would work (live experiment may be unneeded)
  - (b) If live experiment needed, observe usual protocols
7. Generalization
  - (a) See if other programs, interfaces, or subjects/objects suffer from the same problem
  - (b) See if this suggests a more generic type of flaw
8. Elimination
9. Examples
  - (a) Burroughs B6700 System
  - (b) Corporate computer system