Outline for October 28, 2022

Reading: *text*, §24.1–24.5

Assignments: Homework 3, due November 11;
Progress report, due Nov 11 (Note change in due date!)

1. Aslam
   (a) Goal: Treat vulnerabilities as faults
   (b) Coding faults: introduced during software development
      i. Synchronization errors
      ii. Validation errors
   (c) Emergent faults: introduced by incorrect initialization, use, or application
      i. Configuration errors
      ii. Environment faults
   (d) Introduced decision procedure to classify vulnerabilities in exactly one category
2. Standards
   (a) CVE
   (b) CWE
3. Penetration Studies
   (a) Goals
   (b) Where to start
      i. Unknown system
      ii. Known system, no authorized access
      iii. Known system, authorized access
4. Flaw Hypothesis Methodology
   (a) System analysis
   (b) Hypothesis generation
   (c) Hypothesis testing
   (d) Generalization
5. System Analysis
   (a) Learn everything you can about the system
   (b) Learn everything you can about operational procedures
   (c) Compare to other systems
6. Hypothesis Generation
   (a) Study the system, look for inconsistencies in interfaces
   (b) Compare to other systems' flaws
   (c) Compare to vulnerabilities models
7. 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
8. 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
9. Elimination
10. Examples
   (a) Burroughs B6700 System