Outline for January 16, 2002

1. Greetings and Felicitations!
    a. Homework turn-in directory had a problem; if submitted before 8PM on Sunday, please *resubmit*
2. Puzzle of the day
3. Common Implementation Vulnerabilities
    a. Unknown interaction with other system components (DNS entry with bad names, assuming finger port is finger and not chargen)
    b. Overflow (year 2000, *lpr* overwriting flaw, *sendmail* large integer flaw, *su* buffer overflow)
    c. Race conditions (*xterm* flaw, *ps* flaw)
    d. Environment variables (*vi* one-upsmanship, *loadmodule*)
    e. Not resetting privileges (Purdue Games incident)
4. Vulnerability Models
    a. PA model
    b. RISOS
    c. NSA
5. PA Model (Neumann's organization)
    a. Improper protection (initialization and enforcement)
        i. improper choice of initial protection domain
        ii. improper isolation of implementation detail
        iii. improper change
        iv. improper naming
        v. improper deallocation or deletion
    b. Improper validation
    c. Improper synchronization;
        i. improper indivisibility
        ii. improper sequencing
    d. Improper choice of operand or operation
6. RISOS
    a. Incomplete parameter validation
    b. Inconsistent parameter validation
    c. Implicit sharing of privileged/confidential data
    d. Asynchronous validation/Inadequate serialization
    e. Inadequate identification/authentication/authorization
    f. Violable prohibition/limit
    g. Exploitable logic error
7. Comparison and Problems
    a. Levels of abstraction
    b. Point of view