Outline for April 25, 1997

1. Greetings and Felicitations
   a. Remember to write up what you find
2. Vulnerabilities Models
   a. RISOS (1975), to let managers, etc. know about integrity problems
   b. PA (1976-78), automated checking of programs
   c. NSA, contents unknown but similar to PA and RISOS
   d. Aslam, fault-based; for C programs
   e. Landwehr, classify according to attack purpose as well as type; based on RISOS
   f. Bishop, still being developed
3. RISOS (Research Into Secure Operating Systems); Abbott *et al.*
   a. Improper parameter validation
   b. Inconsistent parameter validation
   c. Implicit sharing of privileged data
   d. Asynchronous validation/incorrect serialization (*eg.*, TOCTTOU)
   e. Inadequate identification/authorization/authentication
   f. Violable prohibition/limit
   g. Exploitable logic error
4. PA (Protection Analysis); Bisbey *et al*.
   a. Improper protection domain; 5 subclasses
   b. * Improper initial protection domain
   c. * Improper isolation of implementation details
   d. * Improper change, (TOCTTOU flaws)
   e. * Improper naming
   f. * Improper deletion/deallocation
   g. improper validation
   h. Improper synchronization; 2 subclasses
   i. * Improper divisibility
   j. * Improper sequencing
   k. Improper choice of operand and operation
5. Note: PA classes map into RISOS classes and vice versa