Outline for June 6, 2000

1. Greetings and felicitations!
2. Implementation
   a. Object naming
   b. Process environment
   c. Process interaction
   d. Error and exception handling
3. Object naming
   a. Trojan horses
   b. Race conditions (TOCTTOU)
4. Process environment
   a. Privileges
   b. Environment variables
   c. System constraints (root directory, *etc*.)
5. Process interaction
   a. IPC and pipes
   b. Use of the network
   c. Multithreading and synchronization (locking)
6. Error and exception handling
   a. Assumptions
   b. Signals and race conditions
7. Auditing
   a. Goals: reconstruction or deduction?
   b. Relationship to security policy
   c. Application logs
   d. System logs
8. Example analysis technique
   a. GOAL methodology
   b. Do it on local file accesses
9. Problems
   a. Log size
   b. Impact on system services
   c. Correllation of disparate logs
10. Intrusion detection
    a. Anomaly detection
    b. Misuse detection
    c. Specification detection
11. Anomaly detection
    a. Dorothy Denning's model and IDES
    b. Useful characteristics (examples)
    c. Cautions and problems
    d. Defeating it
12. Misuse detection
    a. TIM (from DEC)
    b. Rule-based analysis and attack recognition
    c. Cautions and problems
    d. Defeating it

13. Specification Detection
    a. Property-Based Testing (introduce specifications here)
    b. Example
    c. Cautions and problems
    d. Defeating it
14. Toss in a network
    a. NSM
    b. DIDS
    c. GrIDS