Outline for March 9, 1999

1. Greetings and felicitations!
2. Auditing
   a. Goals: reconstruction or deduction?
   b. Relationship to security policy
   c. Application logs
   d. System logs
3. Example analysis technique
   a. GOAL methodology
   b. Do it on local file accesses
4. Problems
   a. Log size
   b. Impact on system services
   c. Correllation of disparate logs
5. Intrusion detection
   a. Anomaly detection
   b. Misuse detection
   c. Specification detection
6. Anomaly detection
   a. Dorothy Denning's model and IDES
   b. Useful characteristics (examples)
   c. Cautions and problems
   d. Defeating it
7. Misuse detection
   a. TIM (from DEC)
   b. Rule-based analysis and attack recognition
   c. Cautions and problems
   d. Defeating it
8. Specification Detection
   a. Property-Based Testing (introduce specifications here)
   b. Example
   c. Cautions and problems
   d. Defeating it
9. Toss in a network
   a. NSM
   b. DIDS
   c. GrIDS