Outline for March 16, 1999

1. Greetings and felicitations!
2. Security in Programming
   a. Specification/Requirements
   b. Design
   c. Implementation
3. Design: use MTA on UNIX
   a. Principle of Least Privilege
   b. Principle of Fail-Safe Defaults
   c. Principle of Economy of Mechanism
   d. Principle of Complete Mediation
   e. Principle of Open Design
   f. Principle of Separation of Privilege
   g. Principle of Least Common Mechanism
   h. Principle of Psychological Acceptability
4. Implementation
   a. Object naming
   b. Process environment
   c. Process interaction
   d. Error and exception handling
5. Object naming
   a. Trojan horses
   b. Race conditions (TOCTTOU)
6. Process environment
   a. Privileges
   b. Environment variables
   c. System constraints (root directory, *etc*.)
7. Process interaction
   a. IPC and pipes
   b. Use of the network
   c. Multithreading and synchronization (locking)
8. Error and exception handling
   a. Assumptions
   b. Signals and race conditions