Outline for June 3, 2004

1. Models
   a. Anomaly detection
   b. Misuse modeling
   c. Specification modeling
2. Architecture
   a. Agent
   b. Director
   c. Notifier
3. Organization of IDS
   a. Monitoring network traffic
   b. Combining host and network monitoring
   c. Autonomous agents