Outline for June 2, 2005

1. IDS 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
4. Intrusion Response
   a. Prevention
   b. Handling
      i. Containment phase
      ii. Eradication phase
      iii. Follow-up phase