Notes for March 18, 1997

1. Greetings and Felicitations
   a. **Reading**: *none*
   b. Review session: 176 Chemistry, Monday, March 23, 10:30-12:30
   c. Final: this room, Wednesday, March 25, 4:00-6:00
2. Puzzle
3. Intrusion Detection Systems
   a. Anomaly detectors: look for unusual patterns
   b. Misuse detectors: look for sequences known to cause problems
   c. Specification detectors: look for actions outside specifications
4. Anomaly Detection
   a. Original type: used login times
   b. Can be used to detect viruses, etc. by profiling expected number of writes
   c. Basis: statistically build a profile of users' expected actions, and look for actions which do not fit into the profile
   d. Issue: periodically modify the profile, or leave it static?
   e. User vs. group profiles
   f. Problems
5. Misuse Detection
   a. Look for specific patterns that indicate a security violation
   b. Basis: need a database or ruleset of attack signatures
   c. Issues: handling log data, correllating logs
   d. Problems: can't find new attacks
6. Specification Detection
   a. Look for violations of specifications
   b. Basis: need a representation of specifications
   c. Issues: similar to misuse detection
   d. Advantage: can detect attacks you don't know about.
7. Network IDS
   a. What they do
   b. Discuss DIDS organization

[*ended here*]