Notes for October 21, 1998

1. Greetings and Felicitations!
   a. Office hours 3:00–4:00PM today.
   b. Security lab seminar 1:00–2:00PM in 1131 EU-II. We will talk about ongoing projects!
2. Puzzle of the Day
3. Examples
   a. Go through Burroughs B6700 penetration
   b. Go through Michigan Terminal System penetration
4. 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
5. 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
6. 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
7. 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.
8. Classical
   a. monoalphabetic (simple substitution): $f(a) = a + k \bmod n$
   b. example: Caesar with $k = 3$, RENAISSANCE -> UHQDLVVDQFH
   c. polyalphabetic: Vigenère, $f_i(a) = (a + k_i) \bmod n$\
   d. cryptanalysis: first do index of coincidence to see if it's monoalphabetic or polyalphabetic, then Kasiski method.
   e. problem: eliminate periodicity of key