Notes for February 13, 1998

1. Greetings and felicitations!
   a. **Reading**: Pfleeger, pp. 176–198, 277–280; Garfinkel & Spaddord, pp. 327–340
2. Puzzle
   a. Writing to files that are symbolic links
3. Ideal: program to detect malicious logic
   a. Can be shown: not possible to be precise in most general case
   b. Can detect all such programs if willing to accept false positives
   c. Can constrain case enough to locate specific malicious logic
   d. Can use: writing, structural detection (patterns in code), common code analyzers, coding style analyzers, instruction analysis (duplicting OS), dynamic analysis (run it in controlled environment and watch)
4. Best approach: data, instruction typing
   a. On creation, it's type "data"
   b. Trusted certifier must move it to type "executable"
   c. Duff's idea: executable bit is "certified as executable" and must be set by trusted user
5. Practise: blocking writing to communicate information or do damage
   a. Limit writing (use of MAC if available; show how to arrange system executables)

[*ended here*]

   b. Isolation
   c. Quarantine
6. Practise: Trust
   a. Untrusted software: what is it, example (USENET)
   b. Check source, programs (what to look for); C examples
   c. Limit who has access to what
   d. Your environment (how do you know what you're executing); UNIX examples
   e. Least privilege; above with root
7. Practise: detecting writing
   a. Integrity check files a la binaudit, tripwire; go through signature block
   b. LOCUS approach: encipher program, decipher as you execute.
   c. Co-processors: checksum each sequence of instructions, compute checksum as you go; on difference, complain