Notes for March 6, 1998

1. Greetings and felicitations!
   a. **Reading**: Pfleeger, pp. 377–426; Garfinkel & Spafford, pp. 449–478, 669–700
2. Puzzle
3. PEM, PGP
   a. Goals: confidentiality, authentication, integrity, non-repudiation (maybel)
   b. Design goals: drop in (not change), works with any RFC 821-conformant MTA and any UA, and exchange messages without prior interaction
   c. Use of Data Exchange Key, Interchange Key
   d. Review of how to do confidentiality, authentication, integrity with public key IKs
   e. Details: canonicalization, security services, printable encoding (PEM)
   f. Certificate-based key management
   g. PGP v. PEM
4. Certificates
   a. Binding key to name, notion of issuer
   b. PEM trust hierarchy, certificate types
   c. X.509/PGP web of trust model
5. Common Implementation Vulnerabilities
   a. Unknown interaction with other system components (DNS entry with bad names, assuming finger port is finger and not chargen)
   b. Overflow (year 2000, lpr overwriting flaw, sendmail large integer flaw, su buffer overflow)
   c. Race conditions (xterm flaw, ps flaw)
   d. Environment variables (vi one-upsmanship, loadmodule)
   e. Not resetting privileges (Purdue Games incident)

[*ended here*]