Lecture 23 Outline

Reading: *text*, §11.4.1, 12 **Assignments due:** Homework 4, due May 23, 2011

1. PEM, PGP
   a. Quick review
      i. Goals: confidentiality, authentication, integrity, non-repudiation (maybe)
      ii. Design goals: drop in (not change), works with any RFC 821-conformant MTA and any UA, and exchange messages without prior interaction
      iii. Use of Data Exchange Key, Interchange Key
      iv. Review of how to do confidentiality, authentication, integrity with public key IKs
   b. Details: canonicalization, security services, printable encoding (PEM)
   c. PGP v. PEM
2. Authentication
   a. validating client (user) identity
   b. validating server (system) identity
   c. validating both (mutual authentication)
3. Basis: what you know/have/are, where you are
4. Passwords
   a. Problem: common passwords
   b. May be pass phrases: goal is to make search space as large as possible, distribution as uniform as possible
   c. Other ways to force good password selection: random, pronounceable, computer-aided selection
5. Password Storage
   a. In the clear; Multics story
   b. Enciphered; key must be kept available
   c. Hashed; show UNIX versions, including salt