Outline for October 27, 2025

Reading: *text*, §13.1–13.4 **Due:** Homework 3, due November 5; Project selection, due November 7

1. Greetings and Felicitations!
2. Authentication
   (a) Validating client (user) identity
   (b) Validating server (system) identity
   (c) Validating both (mutual authentication)
   (d) Basis: what you know/have/are, where you are
3. Passwords
   (a) Problem: common passwords, easy to guess passwords
   (b) Best: use passphrases: goal is to make search space as large as possible, distribution as uniform as possible
4. Attacks
   (a) Exhaustive search
   (b) Guessing
   (c) Scavenging: passwords often typed where they might be recorded as login name, in other contexts, etc.
   (d) Ask the user: very common with some public access services
5. Defenses
   (a) For thwarting dictionary attacks: salting