Lecture 24 Outline (May 22, 2015)

Reading: §11.4.1, 12, 15 **Assignment**: Homework 4, due June 3, 2015 (*no late assignments accepted*)

1. Greetings and felicitations!
2. Anonymous mailings
   a. Cypherpunk remailer
   b. Mixmaster remailer
3. 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
4. Passwords
   a. Selection techniques
   b. Storage techniques such as hashing
   c. Password sniffing
5. Challenge-response techniques
   a. One-time passwords
   b. Encrypted key exchange
   c. Hardware support
6. Biometrics
   a. Depend on physical characteristics
   b. Examples: pattern of typing (remarkably effective), retinal scans, etc.
7. Location
   a. Bind user to some location detection device (human, GPS)
   b. Authenticate by location of the device
8. Access Control Lists
   a. UNIX method
   b. ACLs: describe, revocation issue
9. Capabilities
   a. Capability-based addressing
   b. Inheritance of C-Lists
   c. Revocation: use of a global descriptor table

Discussion Problem. Last fall, in the wake of the Snowden revelations of widespread NSA snooping, Google, Apple, and a number of other technology companies announced plans to encrypt user data. FBI Director James Comey demanded that technology companies build in "backdoors". That way, if law enforcement needed access to the data, would be able to obtain the data even if the data were encrypted.

What technical problems might such a wiretap "back door" create?