Lecture 22 Outline (May 18, 2015)

Reading: §10.4, 10.6, 11.3, 11.4.1, 12 **Assignment**: Homework 3, due May 20, 2015

1. Greetings and felicitations!
2. Key Exchange
3. Cryptographic Key Infrastructure
   a. Certificates (X.509, PGP)
   b. Certificate, key revocation
4. Digital Signatures
   a. Judge can confirm, to the limits of technology, that claimed signer did sign message
   b. RSA digital signatures: sign, then encipher
5. Networks and ciphers
   a. Where to put the encryption
   b. Link vs. end-to-end
6. PEM, PGP
   a. Goals: confidentiality, authentication, integrity, non-repudiation (maybe)
   b. Design goals: drop in (not change), works with any RFC 821-conforment 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
7. 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
8. 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

---

During the depths of the Great Depression, Grouch Marx and his brothers went to Central Park in New York City. They tried to sell money, asking everyone they met to purchase a $5 bill for $1. No-one bought; everyone they asked looked at them like they were crazy, or asked what was wrong with the $5 bill. Eventually, a policeman came over and, when they made him the same offer, arrested the brothers on suspicion of counterfeiting.

Why do you think the Marx brothers couldn't find a buyer? What does this inability say to an attacker who is planning how to attack a computer system? What does it say to a system administrator seeking to defend her system?