Outline for December 2, 2008

1. Access control
   a. Access control lists
   b. Capability lists
   c. Rings
   d. Example on the network: firewalls
2. Introduction to Cryptography
   a. What it is; keys
   b. Goals: secrecy, authentication, integrity
   c. Attacks: ciphertext only, known plaintext, chosen plaintext
   d. Operations: transposition, substitution
3. Classical cryptography
   a. What it is
   b. Cæsar cipher
   c. Enigma
   d. Data Encryption Standard (DES), Advanced Encryption Standard (AES)
4. Public key cryptography
   a. What it is
   b. Requirements for a public key cipher