Lecture notes for 4.5 user authentication

Authentication:
- Verification of an identity (user, computer)
- Examples: user logging into system, web server using SSL/TLS

Connection to access control:
- Access control determines authorization to access objects
- Authorization depends on correct authentication
- Authentication determines identity of subjects

Human authentication

Multi-factor authentication
- Reduces the types of valid threats
- Something the user has
  - Smartcard
- Something the user knows
  - Password, PIN
- Something the user is
  - Biometrics

Password-based authentication
- Secret word known to computer and user
- Attacks
  - Error message that reveal information
    - Incorrect username or incorrect password
  - Brute force
    - Trying all possible passwords
    - Long, complex passwords defend against this
  - Dictionary attacks
    - Try common dictionary words
    - Make adjustments: leet-speak, append numbers
  - Passwords likely for user
    - Relative's names, pets names, birthdates
  - Social engg
    - Offer something in exchange for password
  - Trojan login program

Computer storage of passwords
- Plaintext: read access must be blocked
- Encrypted passwords: compute one-way hash, store hash

Salt:
- Add random, (publicly-known) data to the start of each password before hash
- Same passwords then hashed differently

Password selection
- Use symbols from large character set (upper, lower, numeric, symbols)
- Long
- Avoid dictionary words
- Avoid names

Challenge-response
- System presents challenge, user generates response using secret info

Biometrics
- Measurement of biological properties of user
  - Fingerprints, hand geometry, iris, retina, voice
- Problems?

Interesting example from book
- Piggy-wiggly had difficulty switching to biometric-based payment
- "Even when P-W offered free turkeys to people who enrolled in their biometric program, the turnout was meager"
  - Social engg: A turkey would not alter the security or privacy of the system

Masquerade detection
- Identification of attacker masquerading as known user
- Look at patterns of use, time of use, objects accessed