Discussion:

Quiz...

Project 1 slides and presentation (see PDF)

Authentication:

- What is the most common?
  - Username / password

- Creating an identifier (username, email) and a verifier (password). Binds identifier to verifier.

- Discretionary access control: you as the owner, have the right to define privileges for the object.

- Mandatory access control: the system has the right to define privileges.

4 main ways to identify you:

1. Password
2. Possess something (smartcard, token)
3. Something I am (biometrics, fingerprint) static
4. Something I Do (voice, writing) dynamic
How do we crack/stole passwords?

- Social engineering: using information you know about the user to get their password
- Dictionary attacks: using dictionary words to guess the password
- Hijacking: taking over someone else's session
- Attack database/files themselves: try to get into where the passwords are stored

- Popular passwords: "password"

- Exploiting multiple password use: using the same password over and over on different websites

Defenses

- Hashed passwords: instead of storing in plaintext, store passwords as hashed values

- Salt: a random set of bits to add to the password so the hash is not "generic". With a salt, "password" and "password" would have different hashes

Due Thursday: Two hand-written paragraphs on what Blow Fish is.

User training: Train end users

Password composition: long length, special characters, etc
Slides:

RFC: request for comment; for people to agree upon, a standard.

Wireless escalation: taking over a root or sysadmin account.

Risk:

Assurance level: what is our confidence in identifying the user?

Level 1-4

*Do not depend on user training*