CS356 - 9/21/17

- Quiz 3 is up

**Security Considerations of Biometric Authentication**
- Biometrics are not secrets
  - Physical characteristics used for authentication do not change
  - Biometric data can be used as unique a way to create a stored hash value
  - Because they are known, they can be spoofed or modified
  - There is no recourse for revoking a compromised identifier
- Threatens individual privacy (e.g. DNA, fingerprints)
  - Extra care should be taken when storing data
- Cultural and religious concerns

**Remote User Authentication**
- If a client and verifier are using passwords from a list of one-time passwords, they can’t fall out of sync or else the verification will fail
- Authentication over networks introduces complexity
  - Replay attacks
  - Eavesdropping
  - Geographic distance
- **Challenge-Response Authentication**
  - Most secure method
  - Client sends identity
  - Verifier responds with challenge: a non-repeating random number r and two functions h (hash function) and f (combines random number and value from h)
  - h is used to hash the client’s password
  - f is used to combine r with value from h:
    - \( f(r, h(password)) \)
  - Verifier has client’s hashed password stored
  - Verifier compares value sent from client with its own calculation of r and the client’s stored password:
    - \( f(r, h(storedPassword)) \)
  - If they match, client is authenticated
  - Claimant and Verifier do not have to be synchronized
  - Verifier does not have to keep track of values sent

**Authentication Security Issues**
- Client attacks
- Host attacks
● Eavesdropping
● Replay
● Trojan horse
● Denial-of-service
  ○ If an attack is launched against companies that offer authentication services such as Google, Facebook, or Twitter, then many people would be barred from authentication

Chapter 4 - Access Control
● Access control: prevention of unauthorized use of a resource
  ○ Includes prevention of using resource in an unauthorized manner
● Example: Allow someone read-only access to file, then that person should not be able to write to file
● Control physical access to devices and resources
● Most important aspect of computer security

Authorization and Access Control
● Must first specify who can access resource
● Then specify what they can do with the resource
● Questions to consider:
  ○ Who can change the access?
  ○ How is authorization enforced?
    ■ Cryptography is one way

Access Control Principles
● Security admin:
  ○ Creates the authorization database
    ■ Database runs users into an access control function to determine what access each user has
● User:
  ○ Password goes into an authentication function
    ■ If authenticated, we check the user’s access rights and allow access to valid resources
● Auditing is necessary to find use of resources in an unauthorized manner

Access Control Policies (ACP)
● Discretionary ACP
● Mandatory ACP
● Role-based ACP

Socrative Questions
● How secure is 2 factor authentication by phone?
- Good as long as the phone is secure

- What are the most commonly targeted resources by attackers?
  - Data files

- Is it possible to have user access control for processes without requiring user input?
  - I think question was directly referring to the pop-up windows that Windows 10 has when you need admin privilege.

- What is the difference between challenge-response and using a password salt?
  - A salt increases the space an attacker would have to search to find the password. A challenge-response model can use salting when hashing the password, and is a more robust way to authenticate then just using a password.

- If biometrics change during age wouldn't it be a good idea to store a new biometrics login data every time, so this growing database will be used for next authentication?
  - Because it changes so slowly, it is generally not necessary or convenient because of data storage limitations.

- Why were enforcement agents assumed secure until recently?
  - In a small system, the enforcement agent only verifies that a request matches the lookup table. It is a small program so finding malware is easy relatively easy. But as systems evolve and get more complex, we have to be careful that they are as secure as we think.

- Are challenge-response the same as asking `challenge questions` when you log into your bank’s website? If not, could you give an example of this that we might have experienced?
  - Challenge questions are not the same as challenge-response authentication. An example of challenge-response authentication is the tile picture that asks you to ‘select all the tiles with street signs’

- Should we put a limit on the number of resources protected by a single access control system?
  - No because all resources need some kind of protection.

- What is the default configuration of challenge response for the open SSH server?
  - Professor Ray did not want to go over this yet. We might go over it when we discuss SSH.