Solutions: Sheet 6

1. Authentication Factors

(a) Name and briefly explain the three classes of authentication techniques.

- **Knowledge:** Knowledge-based authentication aims at proving a user's authenticity based on knowledge of private information about the them. It is used to prove that the person providing the identity information is the owner of the identity. (e.g Passwords, PINs, Cryptographic Keys)
- **Possession:** Possession-based authentication aims to prove a person's identity using items that the user carries, usually a hardware device such as a security token or a phone. (e.g smart card, USB token, Sim card)
- **Inherence:** Inherence-based authentication aims to verify the identity of a person based on the unique biological characteristics of a person. (e.g fingerprint, iris, face, voice, dna tests)

(b) Research and explain the following terms, describe how they are used to authenticate users:

- token, e.g.,
  - **ID token (e.g., RSA SecurID):** RSA SecurID is a security token which is assigned to a computer and which generates an code/key for authentication which changes after a fixed time period. For syncronisation with the computer the inner clock is used. The key is generated almost randomly.
  - **Universal 2-Factor (U2F):** U2F is simplifies the two-factor authentication by using USBs or NFC (near-field communication) devices. It furthermore strengths the seucrity using smart chip technology. The devices for authentication use encryption and private keys to protect the user.

2. **smart card:** A smart card is a microcontroller that is used to generate, store and process cryptographic keys. A user receives a smart card for authentication and connects it to the computer for authentication. If the data stored on the microcontroller can be verified by the computer, the user is authenticated. Keys are compared. chip in smartcard can to full calculation. (all calculation done on smartcard not on computer)
3. **biometrics:** Biometric authentication uses a biologically unique identifiers of a user to authenticate them. Software creates data from given biological information. information from the unique characteristics are used to identify (key).
   1. Register information (taking samples) of biological information (stored in database)
   2. Measured and extract features
   3. extract freatures compared with stored information
   4. looking for matches

(c) Name two strengths and two weaknesses that a biometric authentication process has compared to a 2-factor authentication based on knowledge and possession.

- **Strength:**
  - 2-factor authentication requires an extra device (No loss possible)
  - Fast authentication (just need to let characteristic scan)
  - Make sure only people suppose to access can really access (cannot share it)
- **Weakness:**
  - Results of biometric security can have *false accepts* and *false rejects*
  - Information about real identity of person are stored, while 2FA don't store information that can be used to identify users (privacy issue)
  - Key cannot be changed/ Limited amount of biometric features
  - Lot of computing power

2. Passwords

(a) Name and explain four requirements that affect the security of password-based methods.

- Don't store password in plain text
- store them in hash form
- store them with a salt
- Should have minimum standards (complexity)
- Weak passwords can be guessed
- Sometimes passwords are transmitted in clear text
- Passwords need to be remembered

(b) Compile the main advantage and disadvantage of one-time passwords (e.g., based on an ID token) compared to ordinary passwords and compare them.

Advantage:

- not knowledge based
- only used once

Disadvantage:

- An extra device is required

3. Challenge-Response Protocols

(a) Describe the process of password-based challenge-response authentication.

1. First both Parties (Alice, Bob) agree on a secret key
2. Alice want to confirm her identitdy to Bob
3. Bob creates a random challenge and sends it to Alice (random value)

4. Alice compute the anwser/encrypts the challenge using the shared the secret key and sends the solution to Bob
5. Bob computes the anwser as well and compares it with the receive result of Alice. If the anwser is the same alice confirmed her identity.

Example challenge: Security questions

(b) Compare the security level of authentication based on a challenge-response with the transmission of the password itself via an encrypted or unencrypted connection.

- **unencrypted connection:** challenge-response add security (uncritical to send challenge unencrypted)
    - Mallory won't help himself by knowing the *challenge* and *reponse* $\longrightarrow$ cannot recover shared secret key from it
- **encrypted connetion:** doesn't matter