Chapter 10. Authentication of People

User Authentication can be achieved using:
- What you **know**: e.g., password.
- What you **have**: e.g., a Physical key.
- What you **are**: e.g., Biometrics such as voice/face/eye/fingerprint.

**Passwords**

*Problems:*
- Eavesdropping.
- Read stored file.
- Easy to *guess* on-line.
- Easy to *crack* off-line.
- Users may *write it down*.

**On-Line Password Guessing**

*Odd cases:*
Some banks set passwords as the last 4 digits of SSN.
Some driver’s licenses use SSN as the license number.
When you write a check at a store, the clerk usually writes your driver's license number on the check. Thus the clerk may get all the information for your bank account!.

*Helpful Tips:*
- Set limit on the **number of trials**.
- Process incorrect passwords *slowly*
- *Report* to users of unsuccessful attempts.
- Assign users an easy to *pronounce* strings as passwords.
- Do not let users choose *easy-to-guess* passwords.
- Force users to *change* passwords frequently and prevent them from using old ones.
Off-Line Password Guessing
Obtaining a hash of a password h, an attacker can guess the password w and checks to see if \( h = \text{MD}(w) \).
If someone obtains a file F containing the hashes of many passwords, e.g., /etc/passwd, he can perform a dictionary attack:

```plaintext
for each word w in dictionary D do
    compute \( h = \text{MD}(w) \)
    for each e in F do
        if e = h then w as a password
    done
done
```

The number of performed hashes is: \(|D|\)
Storing a random number s (salt) with \( e = \text{MD}(w|s) \) makes it harder for a dictionary attack: (What is stored is a salt and the hash of \((w|s)\) or \(<s,e>\))

```plaintext
for each entry <s, e> in F do
    for each word w in the dictionary D do
        compute \( h = MD(w|s) \)
        if e = h then w as a password
    done
done
```

How long should a password be?
- To protect against on-line attack a short password is fine.
  E.g., ATM systems have 4 digits (10,000 different PIDs), it is OK since you only have 3 guesses before rejecting your card.
- To protect against off-line attack:
  64 bits of randomness makes the number of trials \(2^{64}\)
  which is considered computationally hard:
    - In decimal this is about 20 digits to remember.
    - If we select random characters (from a 64 chars of upper case, lower case, digits, punctuations) we need 11 characters.
    - If we generate pronounceable passwords (case-insensitive and every third char is one of the 6 vowels) we need 16 characters.
    - If we allow humans generated passwords, we need 32 characters.
Eavesdropping

- **Low tech:** e.g., watch someone type a password.
  
  *Protection:* use *shift/control* chars, and don't display the typed chars.

- **High-Tech:** e.g., wire-tapping, software-based keystroke logging.
  
  *Protection:* use *one-time password* list (use new one each time) & *numbered list of passwords* (system asks for one at random).

Passwords & Careless Users

**Professor:**

*Q:* "Are there any advantages of passwords over biometric devices?"

**Student:**

*A:* "When you want to let someone use your account, with password you just give it them, while with a biometric device you have to go with them until they are logged in!".

Users should be educated of the importance of security.

**General Tips:**

- Do not exchange passwords using email.
- Use different passwords on different systems or accounts.
- Change your password frequently.
- Abort Login Trojan Horses (e.g., type Alt-Ctrl-Del).

**Initial Password Distribution:**

*One popular scheme:* generate a *pre-expired* random password and hand it to the user. It must be changed as part of the first login process.

**Authentication Tokens:**

Physical devices that a person carries around and uses in authentication. People tend to be less willing to "loan" a token to a friend than to share a password.

**Example:** *Cryptographic calculator,* encrypt current time and display the result. The user types this number in place of a password. The computer do the same (takes into consideration that clocks drift).

**Physical Access:**

The location from which access is requested can be part of the authentication process. For Example, many bank transactions can only be initiated at teller's terminals inside the bank.
Biometrics:
Measure physical characteristics and match them against a profile.

Examples:
- Retinal scanner.
- Fingerprint readers.
- Face recognition.
- Iris scanner.
- Voiceprints.
- Keystroke timing.
- Signatures.