Password Based Authentication

Information Security (CSC-407)

Fall 2024 (BSE-7A & 7B)

User Authentication

- **User authentication** is the basis for most types of ***access control*** and ***user accountability***.
- **User authentication** encompasses two functions:

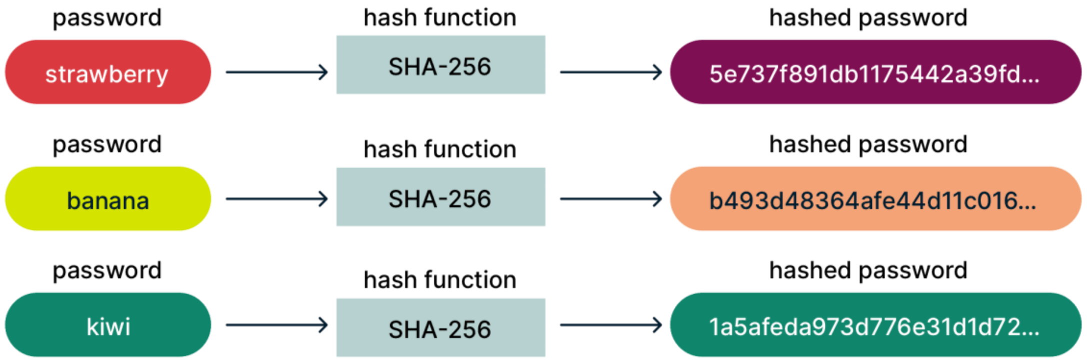
1. The user **identifies** himself/herself to the system by a credential, such as **user ID**.
2. The system **verifies** the user by exchange of **authentication information**.

User Authentication (Cont.)

- **User ID** could be known to system administrators and other users ***(e.g. e-mail)***.
- A typical authentication associated with **user ID** is a **password**, which is kept secret ***(known only to user and to the "system")***.
- Typically, the **password** is stored in **hashed** form on the server and this hash code ***may not be secret***.
- NIST (SP 800-171) provides a list of security requirements for **identification** and **authentication** services.

Passwords

- A typical authentication associated with **user ID** is a **password**.
- The **user ID** could be known to system administrators and other users *(e.g. e-mail),* but the **password** is kept secret ***(known only to the user).***
- Typically, the **password** is stored in **hashed** form on the server. However, this hash code ***may not be secret***.



NIST SP 800-171

NIST (SP 800-171) provides a list of security requirements for **identification** and **authentication** services.

Basic Security Requirements:

1. **Identify users** or processes acting on behalf of users or devices.
2. **Authenticate** IDs of users, processes, or devices, as a prerequisite to allowing access.

NIST SP 800-171 (Cont.)

Derived Security Requirements :

3. Use **multifactor authentication** for:
   - Local and network access to **privileged accounts**.
   - Network access to **non-privileged accounts**.
4. Employ **replay-resistant** authentication mechanisms for network access.
5. Prevent **reuse of IDs** for a defined period.
6. **Disable IDs** after a defined period of inactivity.
7. Enforce a **minimum password complexity** and **change of characters** when new passwords are created.

NIST SP 800-171 (Cont.)

Derived Security Requirements (Cont.):

8. **Prohibit password reuse** for a specified number of generations.
9. Allow **temporary password** use for system logons with an **immediate change** to a permanent password.
10. Store and transmit only **cryptographically-protected** passwords.

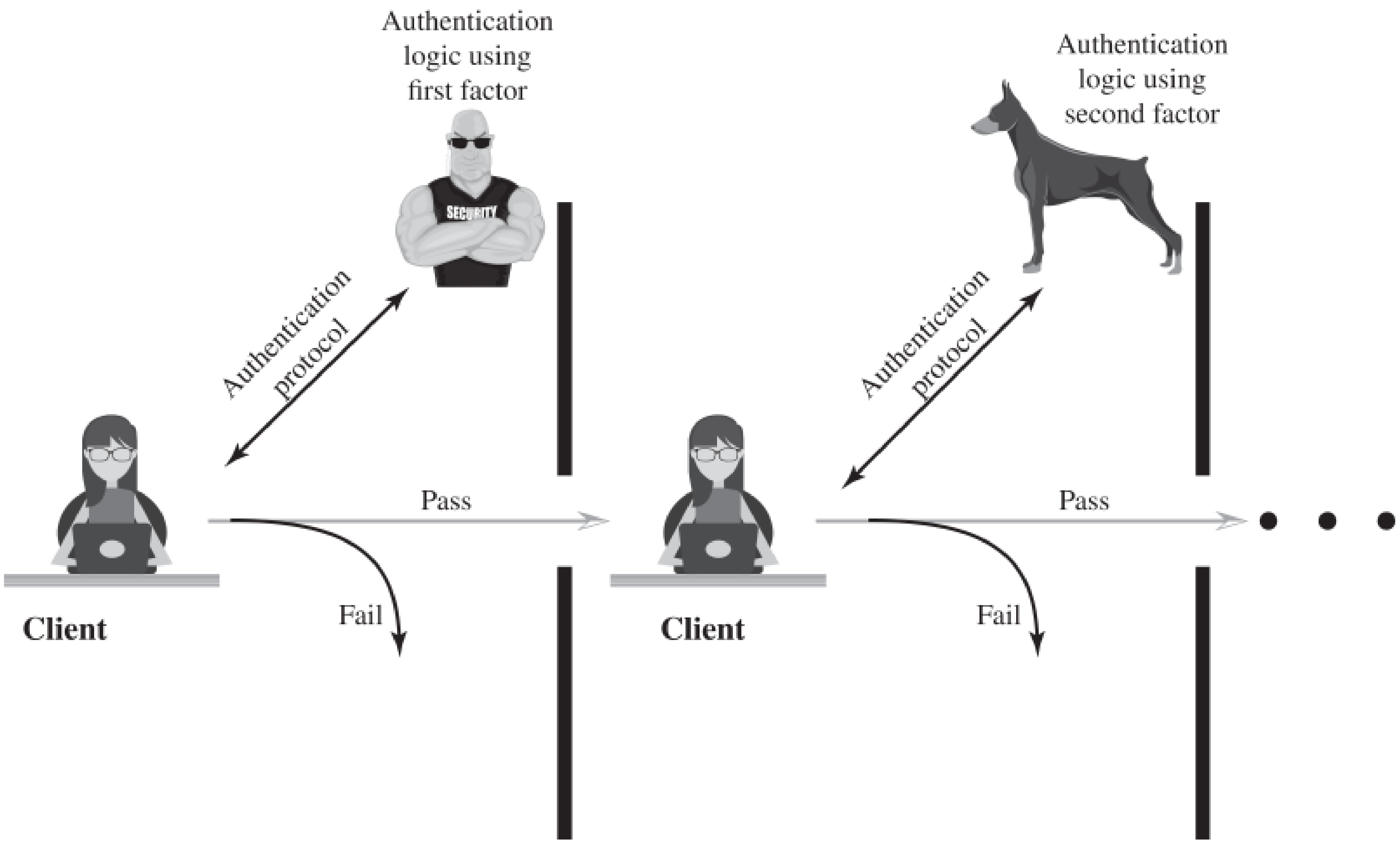
Means of Authentication

- There are four general means of authenticating a user's ID:
  - **Something the individual knows:** E.g. password, PIN or answers to a prearranged set of questions.
  - **Something the individual possesses:** E.g. smart cards. This type of authenticator is referred to as a **token**.
  - **Something the individual is (static biometrics):** E.g. recognition by finger-print, retina and face.
  - **Something the individual does (dynamic biometrics):** E.g. recognition by voice pattern, handwriting characteristics and typing rhythm.

Multifactor Authentication

- **Multifactor authentication** refers to the use of more than one of the **authentication means**.
- The strength of authentication systems is largely determined by the **number of factors** incorporated by the system.
- Implementations that use two factors are considered to be stronger than those that use only one factor.
- Systems that incorporate three factors are stronger than systems that only incorporate two of the factors, and so on.

Multifactor Authentication (Cont.)



The Password System

- Virtually all multiuser systems, network servers, E-commerce websites and other similar services require that a user provide not only a **user ID** but also a **password**.
- The system compares the password to a previously stored password for a user ID, maintained in a ***system password file,*** **e.g. Security Accounts Manager (SAM) in Windows OS**.
- The password serves to **authenticate** user ID of the individual logging on to the system.

The Password System (Cont.)

The ID provides security in the following ways:

- Determines whether the user is **authorized** to gain access to a system or not.
- Used as an **index** for searching the relevant password.
- Determines the **privileges** accorded to the user, E.g.:
  - ***Administrator or super-user***
  - ***Guest accounts***

Common Attack Scenarios

Common attack Scenarios against Passwords:

1. **Specific account attack:**
   - The attacker targets a **specific account** and submits password guesses until the correct password is discovered.
   - **Countermeasure:** account lockout mechanism, which locks out access to the account after a number of failed login attempts. Typical practice is **five access attempts**.

Common Attack Scenarios (Cont.)

Common attack Scenarios (Cont.):

2. Popular password attack:

- Use **popular passwords** and try against a range of user IDs.
- Users have tendency to choose a password that is easily remembered, which unfortunately makes it easy to guess.
- **Countermeasure:** policies to inhibit the selection by users of common passwords.

Common Attack Scenarios (Cont.)

Common attack Scenarios (Cont.):

3. **Offline dictionary attack:**

- Attacker obtains **system password file** and compares the **password hashes against hashes of commonly used passwords**.
- If match is found, the attacker can gain access by that ID/password combination.
- **Countermeasure:** prevent unauthorized access to **password file** through **access controls**. However, incidents show that determined hackers can frequently bypass such controls, hence gaining access to file!

Password Cracking Approaches

Often the following approaches are adopted:

1. Develop a large dictionary of possible passwords and try each against the **password file**.
2. A **rainbow table**, i.e. a huge **pre-computed hash table**.
3. Attacks using a combination of **brute-force** and **dictionary techniques**. E.g. **John the Ripper**.
4. Sophisticated **password generation algorithms**.
5. Using **Machine Learning** with large datasets of leaked passwords as training data.

Examples of Password Selection

Examples for Password Selection:

- Passwords that contain **only letters**: **POTHMYDE**
- Passwords that contain **letters and numbers**: **meet123**
- Passwords that contain only **letters and special characters**: **bob@&ba**
- Passwords that contain **letters, special characters, and numbers**: **ap1@52**
- Passwords that contain **only numbers**: **23698217**
- Passwords that contain **only special characters**: **&*#@!(%)**

Examples of Password Selection (Cont.)

- Passwords that contain only **special characters and numbers**: **123@$45**
- Passwords that contain only **uppercase and lowercase letters**, such as: **RuNnEr**
- Passwords that contain more than 20 characters comprising a phrase: such as **Hardtocrackveryeasily**
- Passwords that contain shortcut codes or acronyms, such as **L8r_L8rNot2day** (i.e., later, later, not today)

Examples of Password Selection (Cont.)

- Passwords that contain frequently used words, such as **ABT2_uz_AMZ!** (i.e., about to use Amazon!)
- Passwords that contain the first letters of words of a long sentence, such as:
  - **TffcievwMi16wiwdm5g** (i.e., the first foreign country I ever visited was Mexico in 2016 when I was doing my 5th grade)
  - **Mrrh247** (munna ro raha he 247)

Thank You!