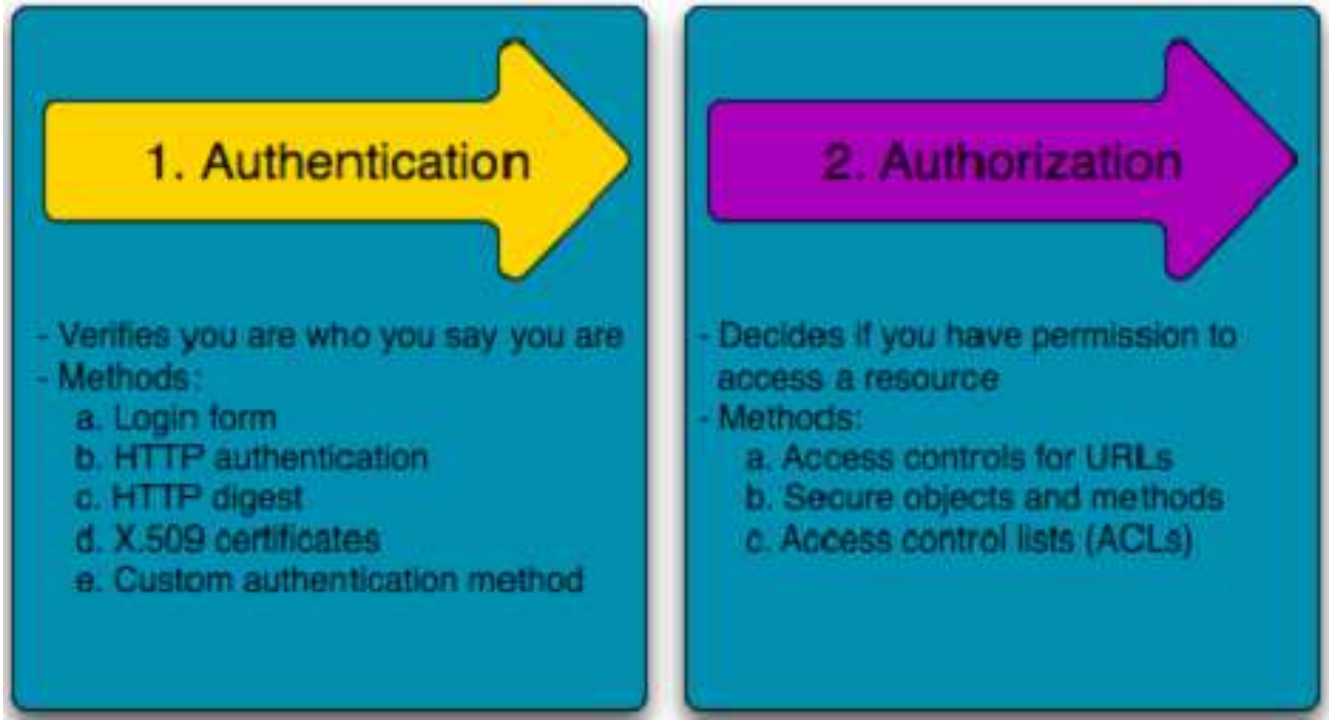
Lesson 4.

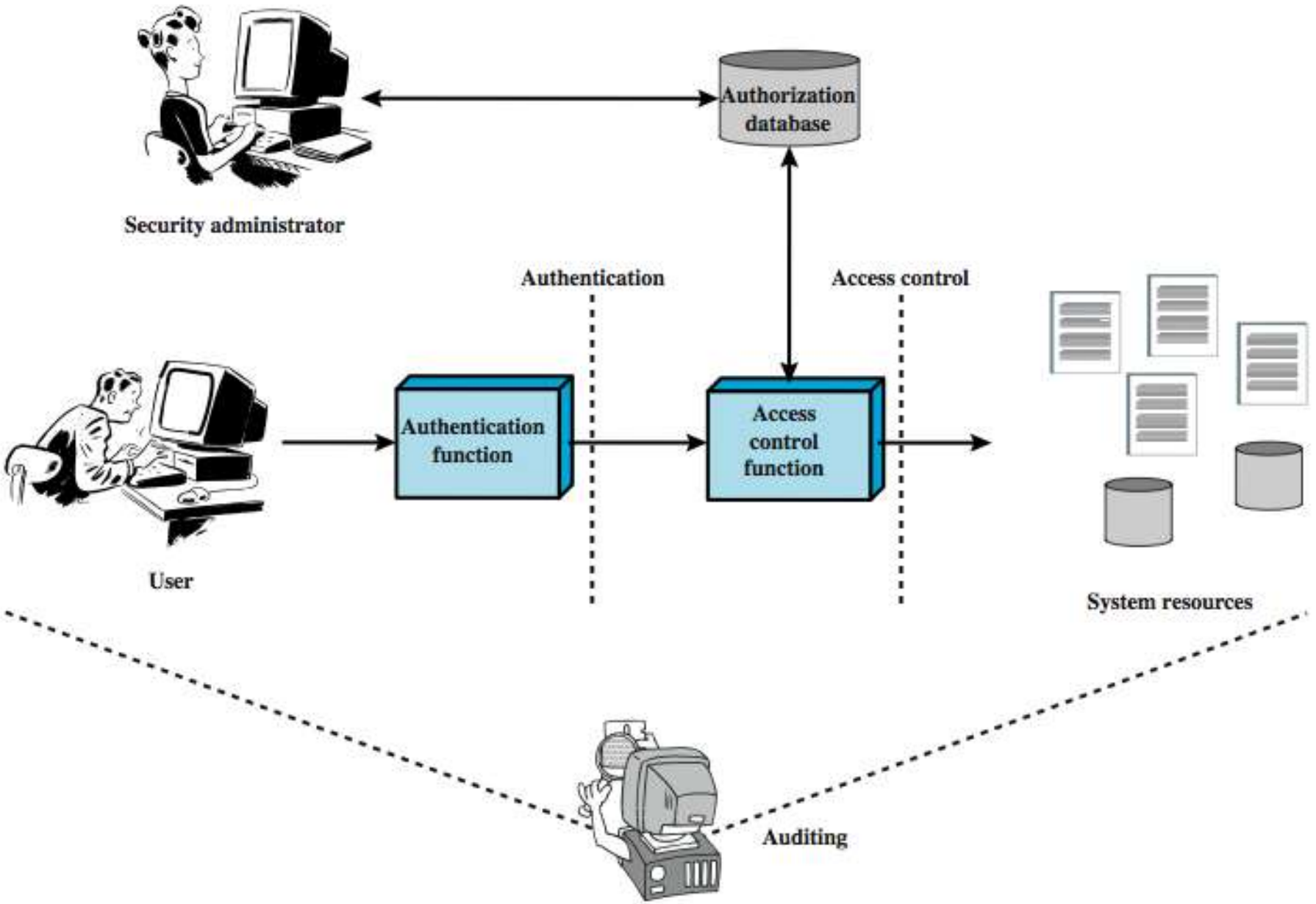
Authentication



Outline

1. Introduction
2. Authentication factors
3. One Time Password (OTP)
4. Single-Sign-On (SSO)
5. Labs
6. Summary

Introduction



Introduction

Authentication is about validating your credentials such as Username/User ID and password to verify your identity.

Introduction

- Strong authentication is important

  To be properly authenticated, the subject is usually required to provide a second piece to the credential set (i.e., password, passphrase, key, PIN, token etc.

Authentication factors

Authentication factors determine the many different elements the system uses to verify one's identity before granting the individual access to anything.

- something you know
- Something you have
- Something you are

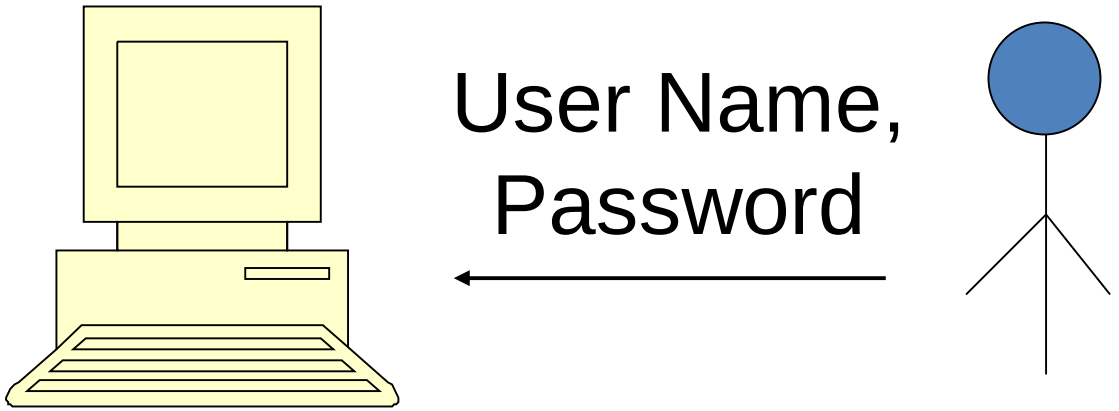
Authentication factors

- Based on the security level, authentication factors can vary from one of the following:
  - **Single- Factor Authentication**
  - **Two- Factor Authentication (2FA)**
  - **Multi- Factor Authentication (MFA)**

Something you know
(Knowledge-based)

- Passwords are the most common form of authentication
- PIN

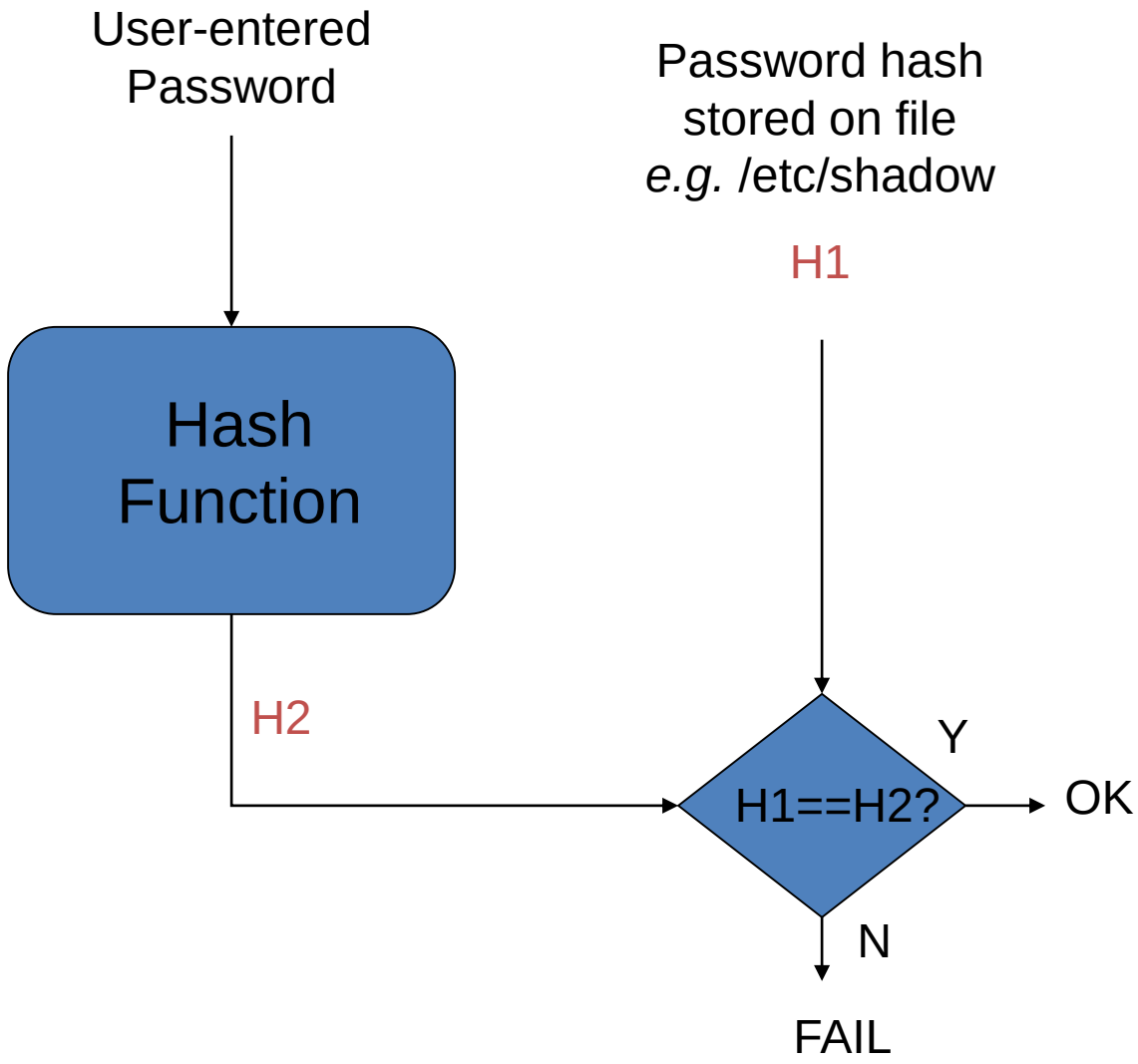
Simple Password Authentication



/etc/shadow

Something you know

Password Verification



Something you know

"Passwords are one of the biggest practical problems facing security engineers today."

Problems:

- Easy to share (intentionally or not)
- Easy to forget
- Often easy to guess
- Too many passwords to remember

Password vulnerabilities

- Access the password file
- Brute force attacks
- Directory attacks
- Social engineering

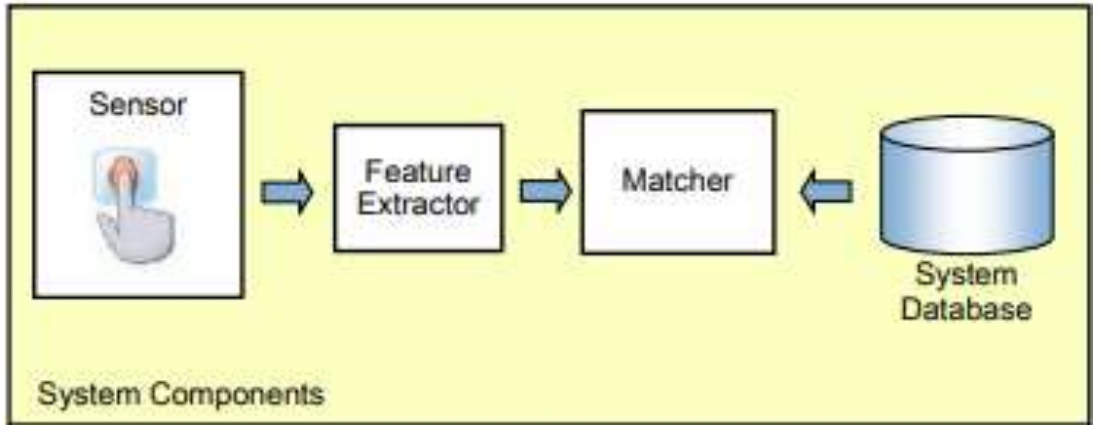
- Complex password policy
  - Forcing users to pick stronger passwords

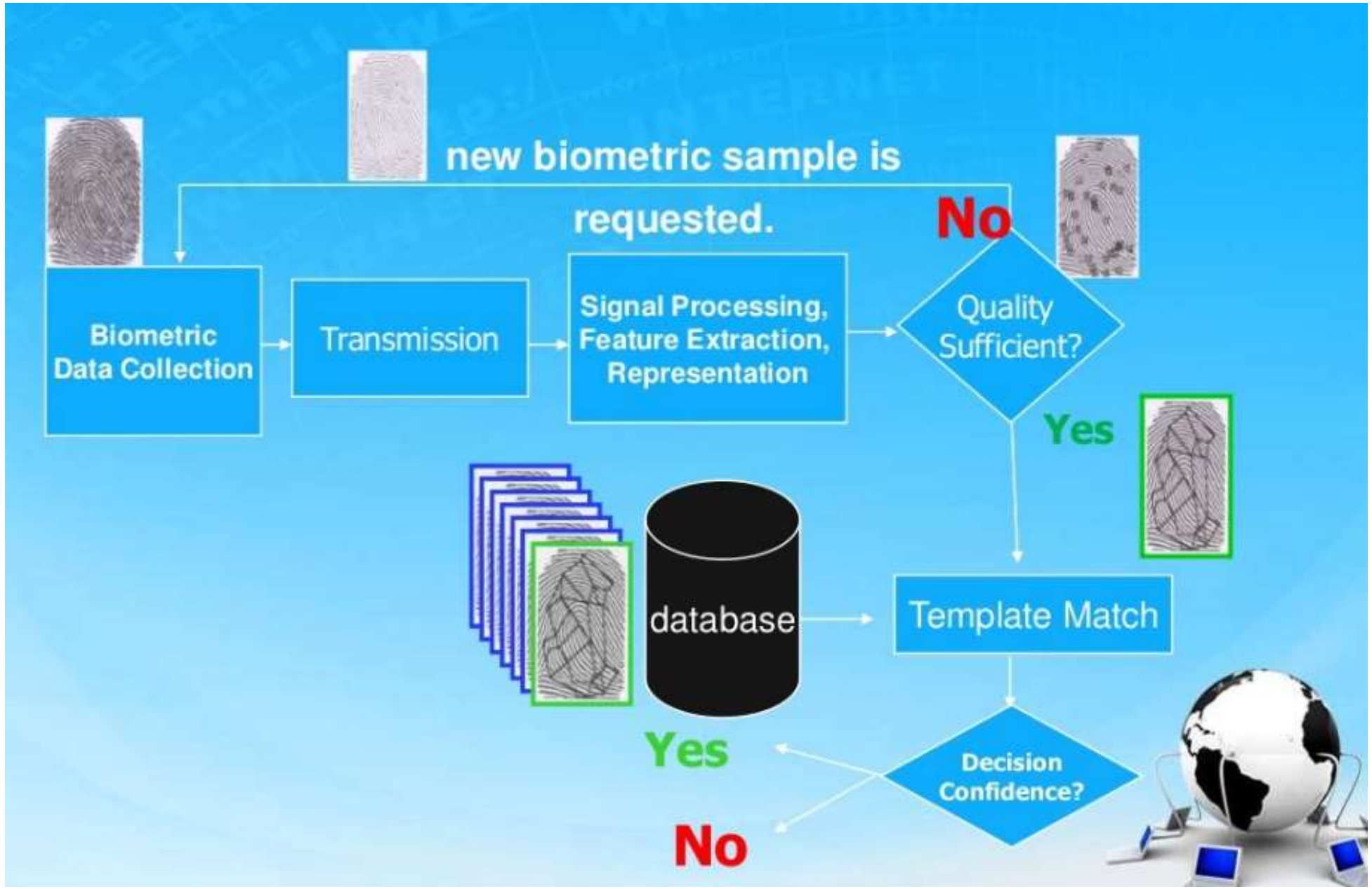
Strategies for strong passwords

- Proactive password checking
  - Users select a potential password which is tested
  - Weak passwords are not accepted
- Reactive password checking
  - SysAdmin periodically runs password cracking tools to detect weak passwords that must be replaced
- Computer-generated passwords
  - Random passwords are strong but difficult to remember

Something you are/do
(Inherence-based)

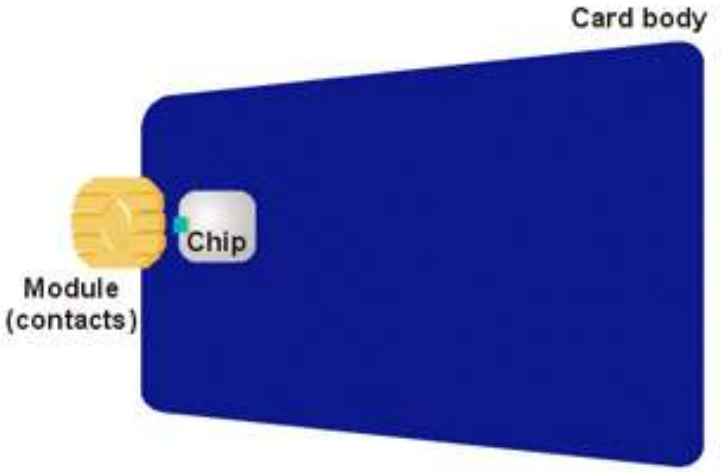
- Biometric - **"You are your key"**
- Examples:
  - Fingerprint
  - Handwritten signature
  - Facial recognition
  - Speech recognition
  - Iris
  - Voice
  - …




new biometric sample is requested.
No
Biometric Data Collection
Transmission
Signal Processing, Feature Extraction, Representation
Quality Sufficient?
Yes
database
Template Match
Yes
Decision Confidence?
No

Something you have
(Ownership-based)

- **E-Token**: store credentials such as passwords, digital signatures and certificates, and private keys
- **RFID**: Integrated circuit(s) with an antenna that can respond to an RF signal with identity information
- **Smart card**
- **Digital Certificates** (used by Websites to authenticate themselves to customers)

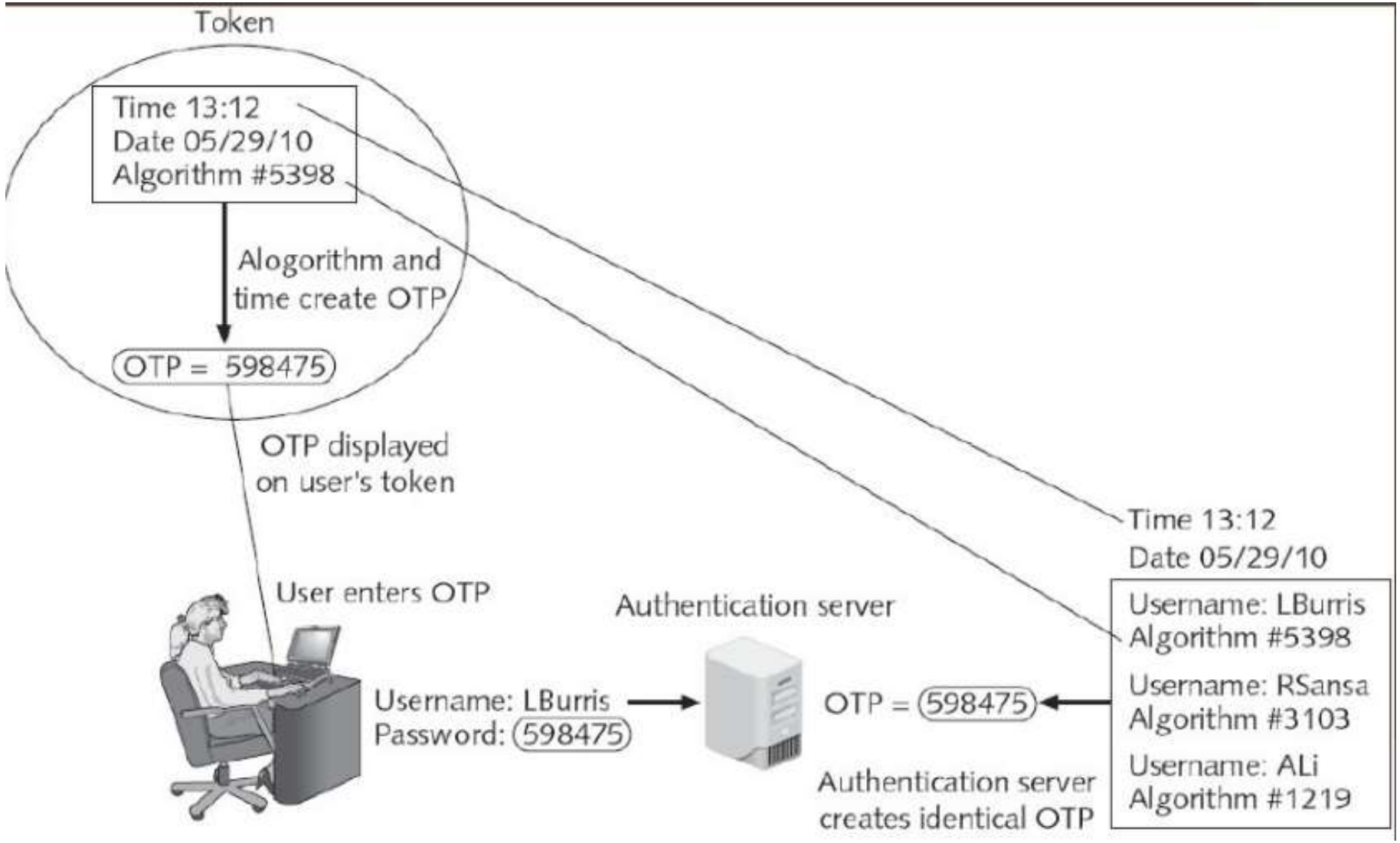


Source: Gemplus - All About Smart Cards

One Time Password

- Dynamic password that change frequently
- Systems using OTPs generate a unique password on demand that is not reusable

Time-synchronized OTP



Challenge-based OTP

- Authentication server displays a challenge (a random number) to the user
- User then enters the challenge number into the token (executes a special algorithm to generate a password)
- Because the authentication server has the same algorithm, it can also generate the password and compare it against that entered by the user.

Single Sign On

- Multiple applications, each requires login
- Provide users with the ability to login only once for usability
- Automatically propagate login to all applications

Single Sign On

- Advantages
  - Unified mechanism
  - One login/password to remember
  - New applications reuse code
- Disadvantages
  - Can weaken security

Implementing authentication

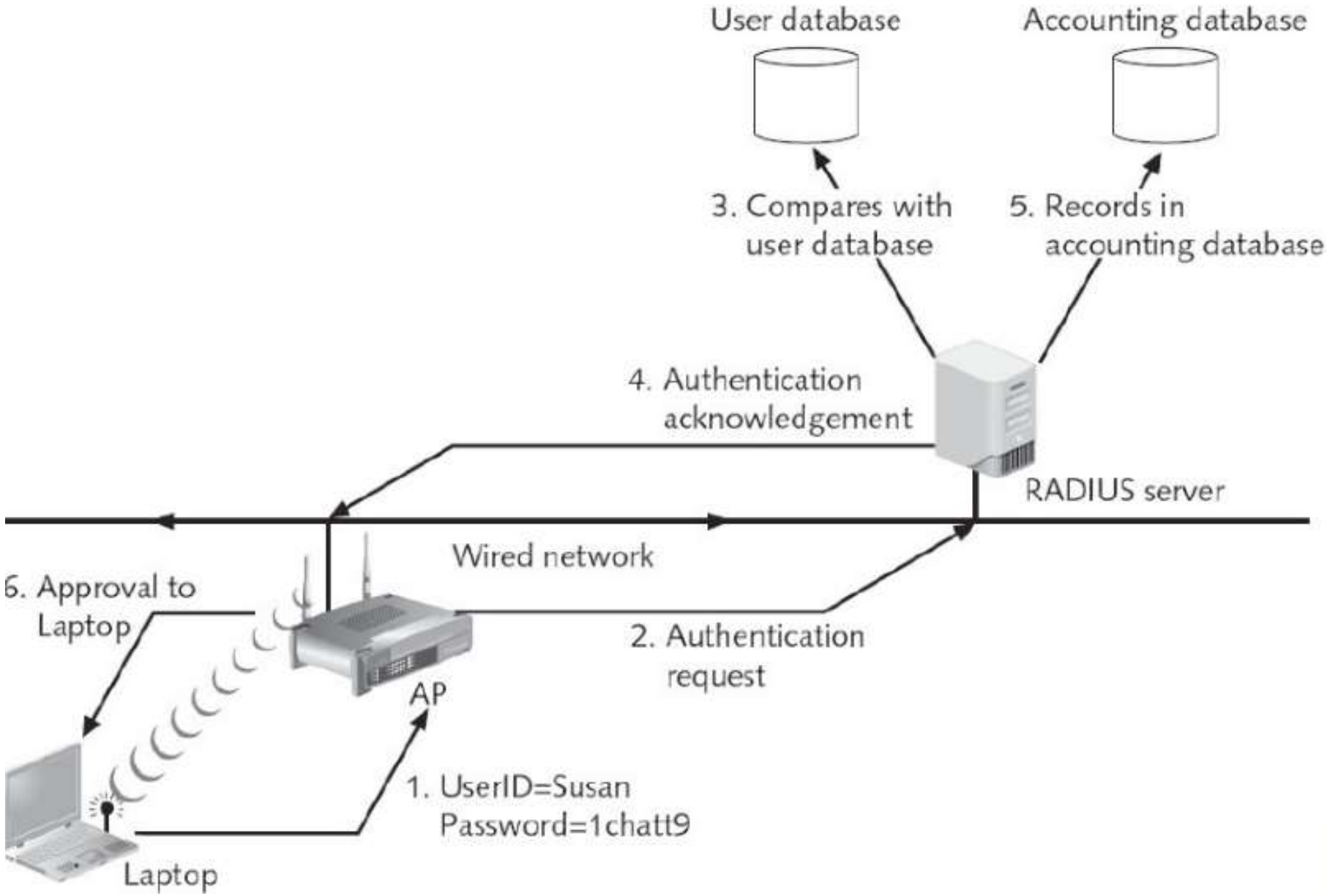
- Local authentication
- Network authentication

Authentication Server

- Radius
- Kerberos
- TACACS+
- LDAP

RADIUS

- Wired and Wireless LANs
- Radius clients: server, switch, AP
- Radius server authenticates and authorized the radius client requests


User database
Accounting database
3. Compares with user database
5. Records in accounting database
4. Authentication acknowledgement
RADIUS server
Wired network
6. Approval to Laptop
2. Authentication request
AP
1. UserID=Susan Password=1chatt9
Laptop

Lab

1. **Password policies**

   Create an account and test some functionalities:

   – Minimum the password length

   – Strong password

   – Account lockout threshold

2. **WiFi User authentication (WiFi)**

   – WPA2

   – RADIUS server

Lab. Password Policies

Ubuntu

- A strong password should contain:
  - Upper case letters
  - Lower case letters
  - Digits
  - Symbols
- we will use the pwquality module of PAM

```
$ sudo apt install libpam-pwquality
```

- Now first copy “/etc/pam.d/common-password” file before configuring any changes.

```
$ sudo cp /etc/pam.d/common-password /etc/pam.d/common-password.backup
```

$sudo vi /etc/pam.d/common-password

($sudo vi /etc/security/pwquality.conf)

$sudo vi /etc/login.defs

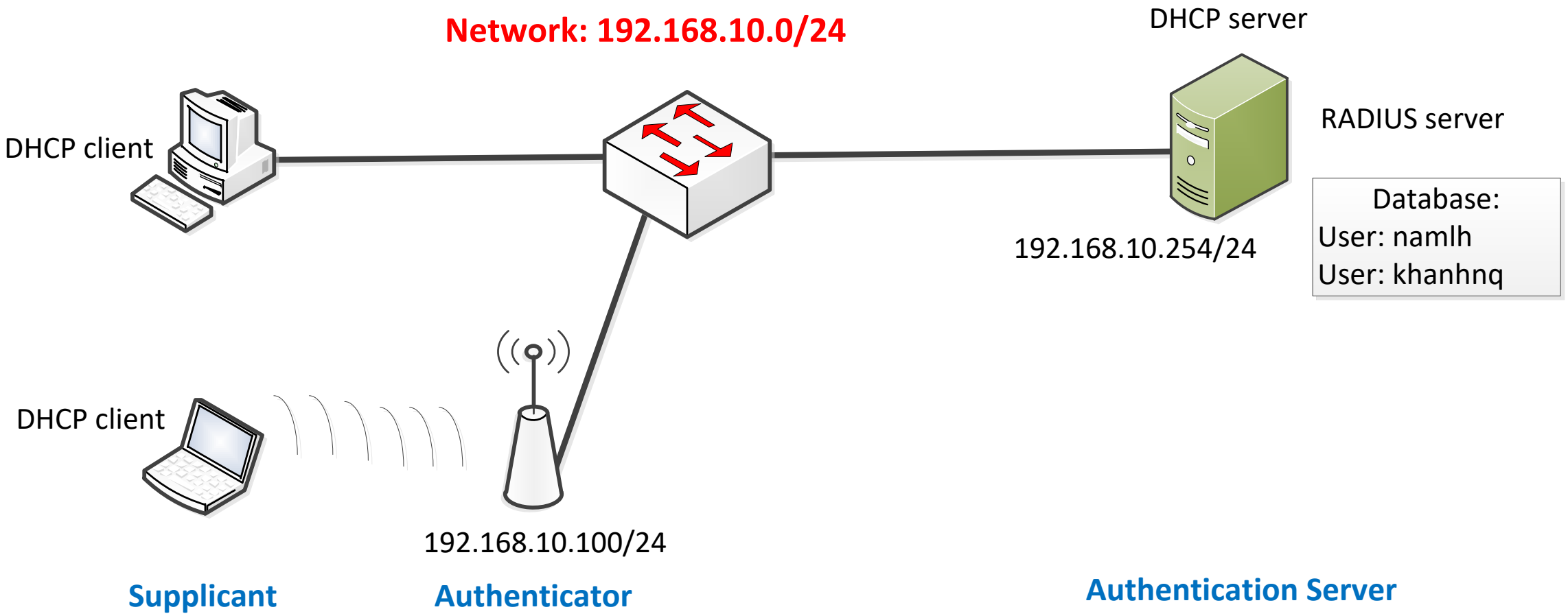
```
password   requisite pam_pwquality.so retry=4  minlen=9  difok=4   lcredit=-2 ucredit=2
 dcredit=-1 ocredit=-1 reject_username enforce_for_root
```

1. **retry**: No. of consecutive times a user can enter an incorrect password.
2. **minlen:** Minimum length of password
3. **difok:** No. of character that can be similar to the old password
4. **lcredit:** Min No. of lowercase letters
5. **ucredit:** Min No. of uppercase letters
6. **dcredit:** Min No. of digits
7. **ocredit:** Min No. of symbols
8. **reject_username:** Rejects the password containing the user name
9. **enforce_for_root:** Also enforce the policy for the root user

Verify the configuration

- $sudo reboot
- $sudo useradd namlh
- $sudo passwd namlh

Network topology



Summary

- Authentication is about validating your credentials such as Username/User ID and password to verify your identity
- Multiple factors:
  - Something you know
  - Something you have
  - Something you are
- Implementing authentication
  - Local
  - network