Identification, authentication, authorization

1 Access Control

Access to the resources:

- Claim the identity
- Verify the credentials
- Check permissions
- Grant access

2 Identification

Subject - An active entity within a system (physical person, script, etc)
Principal - An entity that can be granted access (represented by a username, userid, pin etc)

The subject identifies itself to the system as a principal

3 Authentication

The system verifies the identity of the user

Object - Resource that some principals may access or use

The system checks that the principal has the permissions to access an object

4 Credentials

- What do you know? Passwords, PINs
- What do you have? Authentication key, passport, ticket, mobile phone
- Who you are? Biometrics

5 Passwords

Common Security Guidelines:

- Adopt long passphrases
- Avoid easy to guess passwords
- Use combination of a-z, A-Z, 0-9 and symbols
- Do not write down passwords
- Avoid using the same password for multiple services

However - when internet users log on to as many as 25 password-protected sites per day, remembering a different and secure password for each one is very difficult.
Passwords should be stored in a password manager so you only have to remember one secure password

6 Authentication Keys

Authentication keys (e.g. SSH keys)

- Similar to passwords, but
- RSA-based keys
- Subject create private/public key
- Share the public key with services
- Per device RSA key

Advantages:

- Public key leak are inconsequential
- Compromised device access can be revoked

7 Security Keys

Authentication keys weakness: Compromised client

Solution: Physical security keys:

- Static password token (not recommended)
- Asynchronous tokens (one-time passwords)
- Challenge-response tokens

8 Biometrics

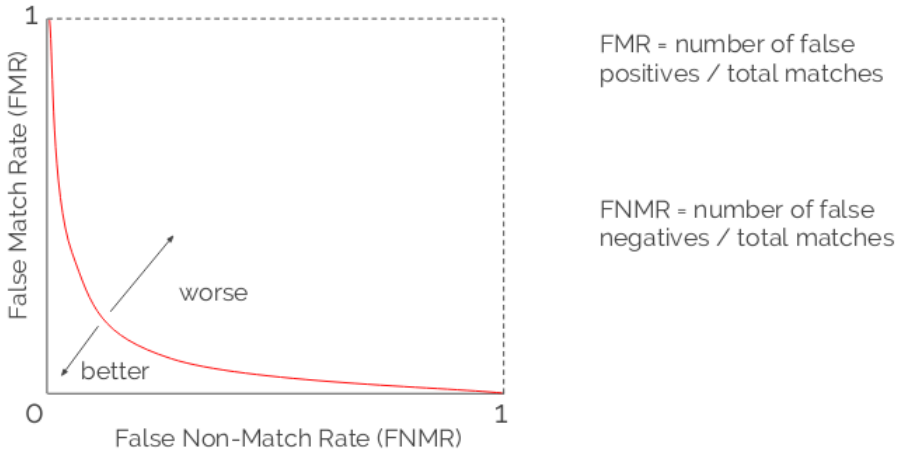
Advantages:

- Non-repudiation: a way to guarantee that an individual who accesses a certain facility cannot later deny using it

Disadvantages:

- Uncertainty: Compromise between false-positive and false-negatives

Receiver Operating Characteristic (ROC) curve



Performance policy

- Prefer low FMR. E.g. automatic border control. Refer to human on negative result
- Prefer now FNMR. E.g. suspect recognition on CCTV. Refer to human on positive result

9 Two-factor authentication

Two-factor authentication.

Combine two authentication factors from:

- What you know: password, pin
- What you have: mobile phone, authentication key

10 Zero-Knowledge Password Proof

Objective: Do not reveal anything in the client/server communications about the password.
Otherwise we are vulnerable to replay attacks.

Most common ZKPP approach: Challenge-response auth:

- Serer generate unique challenge value: nonce
- Server send nonce to the client
- Client computer response = hash(nonce + password)
- Client send response back to server
- Server compare the response with hash(nonce+stored password)