**Chapter 13: Managing Identity and Authentication**

Identification is the process of a subject claiming, or professing, an identity.

Authentication verifies the subject’s identity by comparing one or more factors against a database of valid identities, such as user accounts.

Identification and authentication occur together as a single two-step process.

Authorization indicates who is trusted to perform specific operations. If the action is allowed, the subject is authorized; if disallowed, the subject is not authorized.

Authentication Factors Overview

* Something You Know (type 1)- password, pin, etc
* Something You Have (type 2) - OTP on mobile, hardware token, etc
* Something You Are (type 3) - fingerprint, retina pattern, etc

In addition to the three primary authentication factors, attributes are sometimes used for additional authentication. These include the following:

* Somewhere You Are - location
* Context-Aware Authentication - kind of device, etc

Password recommendations are changing, and so far, there isn’t a consensus that everyone is following.

NIST Password Recommendations

* **Passwords must be hashed**
* **Passwords should not expire** - expiring passwords regularly doesn't add much value
* **Users should not be required to use special characters** - it often challenges users’ memory, and they wrote these passwords down
* Users should be able to copy and paste passwords - makes it easier to use password manager. When copy and paste is restricted, users must retype the password and typically default to easier passwords.
* Users should be able to use all characters - By allowing spaces, users can create longer passwords that are easier to remember.
* Password length should be at least eight characters and as many as 64 characters.
* Password systems should screen passwords - Before accepting a password, password systems should check them against a list of commonly used passwords.

The PCI DSS (version 3.2.1) has the following requirements, which differ from NIST SP 800-63B:

* Passwords must expire at least every 90 days.
* Passwords must be at least seven characters long.

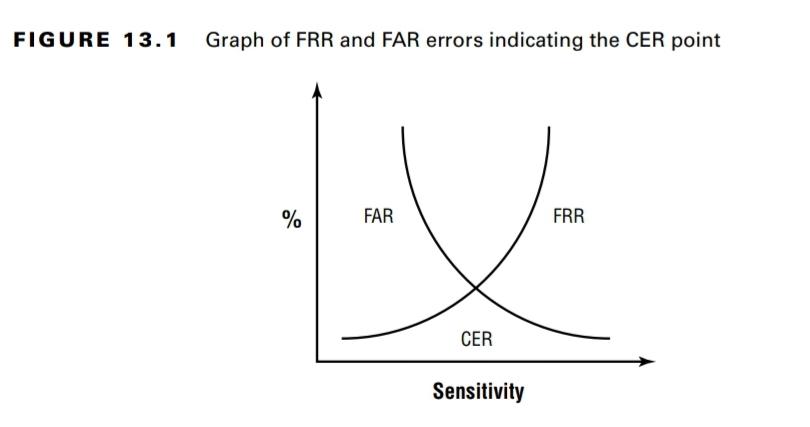
Biometric Factor Error Ratings

**False Rejection Rate (FRR)** - Rejected, but it was false rejection

**False Acceptance Rate (FAR)** - Accepted, but it was false acceptance

The point where the FRR and FAR percentages are equal is the crossover error rate (CER), and the CER is used as a standard assessment value to compare the accuracy of different biometric devices. Devices with lower CERs are more accurate than devices with higher CERs

Increasing the sensitivity of biometric devices makes it do more thorough pattern matching and therefore rejection rate also increases.



Credential management systems provide storage space for usernames and passwords. As an example, many web browsers can remember usernames and passwords for any site that a user has visited.

A periodic account access review can discover when users have more privileges than they need and could have been used to discover that this employee had permissions from several positions.