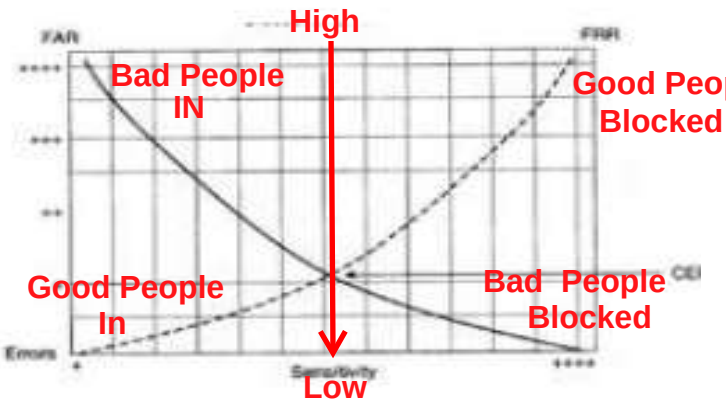
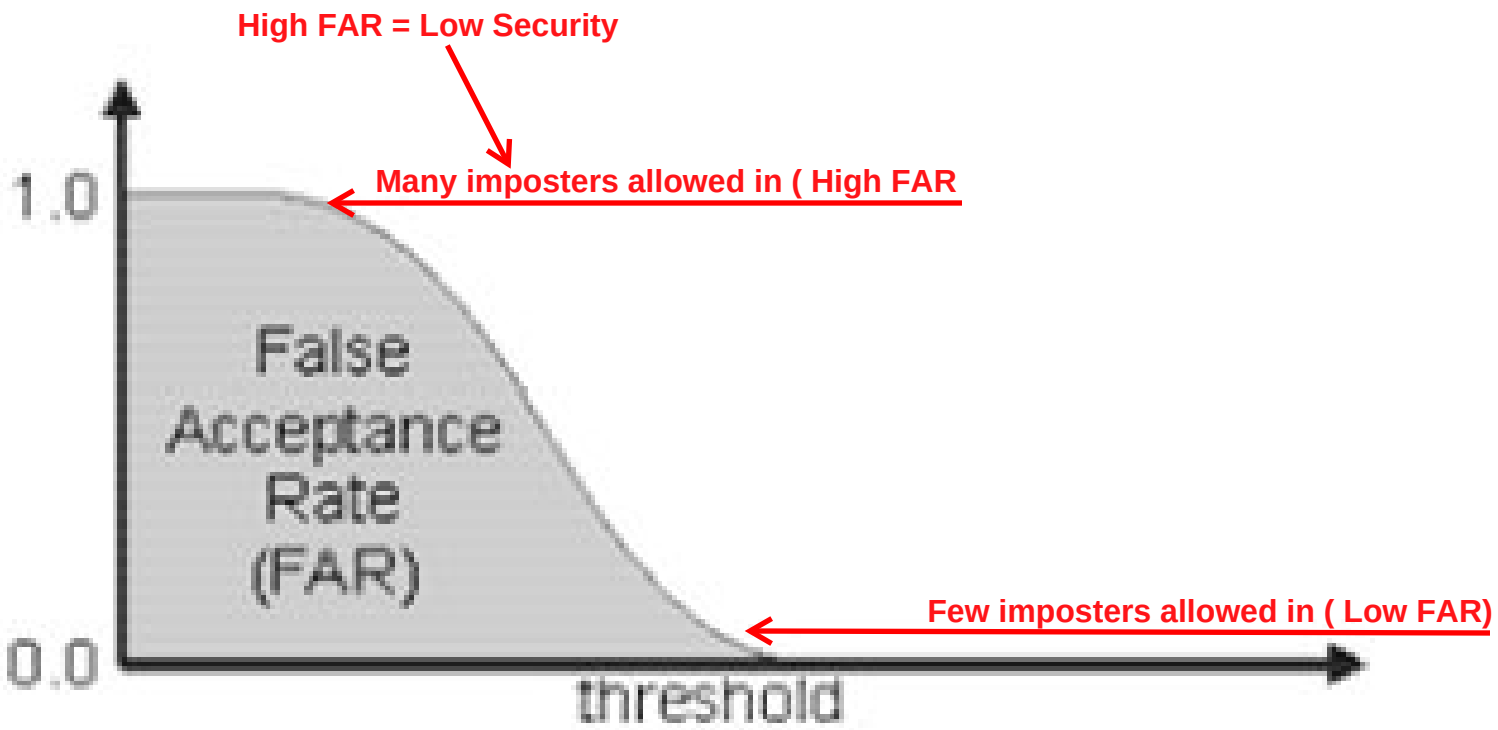
Biometrics

Biometric-Based Authentication

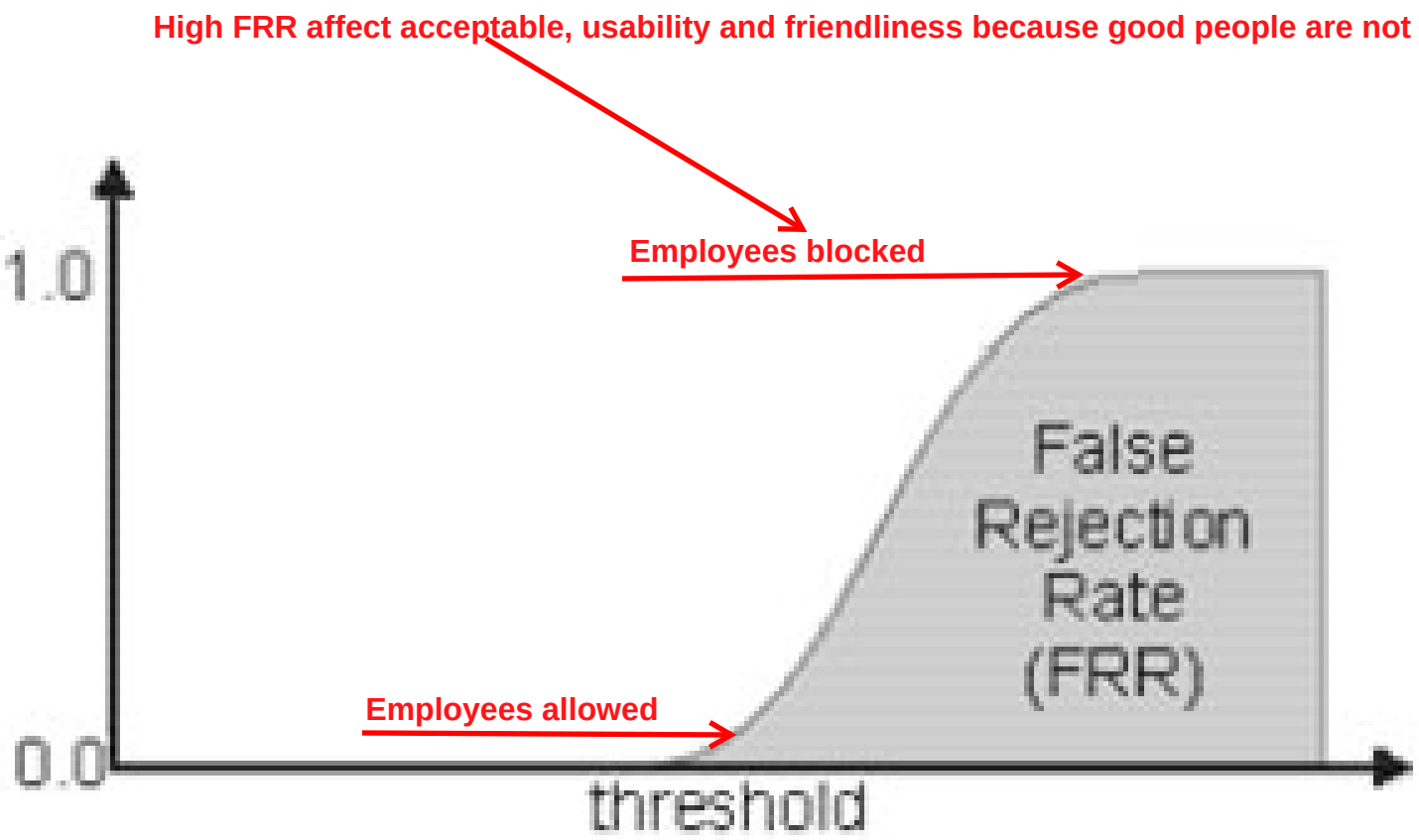
- False Rejection Rate (FRR)
  - When the system rejects an authorized individual
- False Acceptance Rate (FAR)
  - When the system accepts an intruder who should be rejected
- Crossover Error Rate (CER)
  - Metric used to compare biometric systems When false rejection rate equals false acceptance rate



Biometric FAR - The Imposter chart



Biometric FRR – The Nuisance Chart



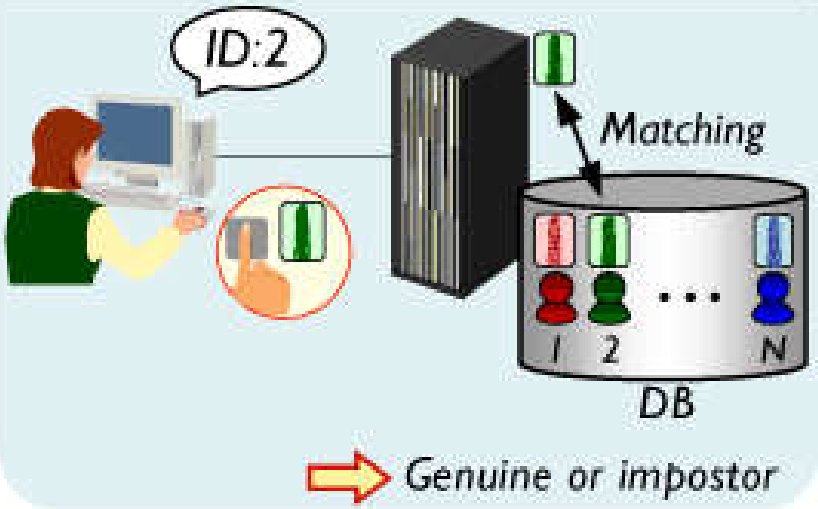
Biometrics

- 2 Categories of Biometrics
  - **Physiological** – Static biometrics:
    - measurement of a **part of a person's anatomy**.
    - example, fingerprints and iris patterns, as well as facial features, hand geometry and retinal blood vessels
  - **Behavioral** – Dynamic biometrics:
    - measurement of a **person action performed**.,
      - . For example, voice (speaker verification)

Authentication vs Identification

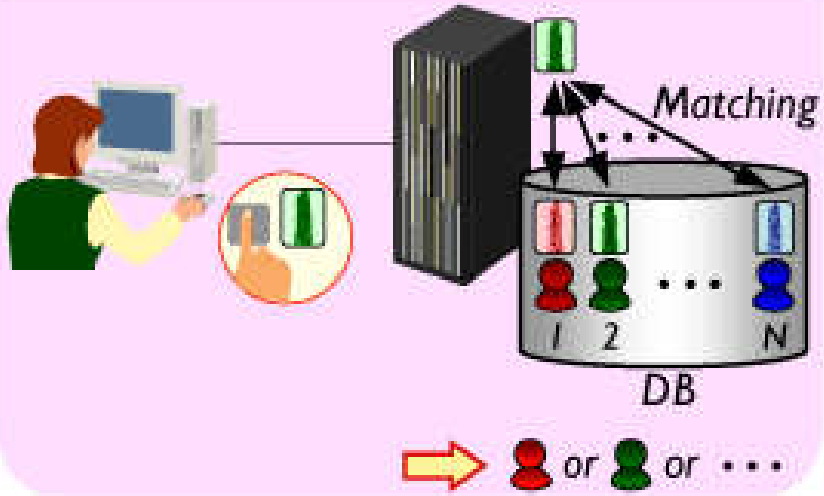
Biometric verification
(1:1 authentication)

The user presents his/her ID (or card) and the biometric data, which is matched against the enrolled biometric data corresponding to the ID (or on the card).



Biometric identification
(1:N authentication)

The user only presents his/her biometric data, which is matched against all the biometric data in the database.
(Convenience: high)



Kerberos

- **Kerberos weakness:**
- The KDC is a single point of failure.
- The secret keys are temporarily stored on user's workstations, in memory, etc.
- Session keys are decrypted and reside on user's workstations.
- Vulnerable to password guessing.

Kerberos Weakness

- Does not protect network traffic unless encryption is enabled.
- When a user changes password, the KDC database needs to be updated with a new corresponding secret key.
- Replay attacks can be used against Kerberos

Comparison Between Biometric

Biometric Technology	Accuracy	Cost	Device Required	Social Acceptability
DNA	High	High	Test Equipment	Low
Iris recognition	High	High	Camera	Medium -Low
Retina scan	High	High	Camera	Low
Facial recognition	Medium - Low	Medium	Camera	High
Voice recognition	Medium	Medium	Microphone, telephone	High
Hand geometry	Medium - Low	Low	Scanner	High
Finger print	**High**	**Medium**	**Scanner**	**Medium**
Signature recognition	Low	Medium	Optic pen, touch panel	High

One Time Passwords

- **Synchronous –** Token device synchronizes (shares same secret key) with authentication server via a time-based or event-based synchronization.
- **Asynchronous –** Uses a *challenge-response* scheme to communication with the authentication server.