Safety of information systems

Lecturer: Roman Danel

Authentication, authorization, biometrics

Authentication = user access verification

Authorization = user rights verification

Authentication

- Password expiry
- Limited number of login attempts (password, PIN)
- "Strong" password - the minimum number of characters, required combination of numbers and characters, and avoid the use of known words
- No "blank" password
- The use of time intervals (automatic logout after a period of inactivity)

User Authentication Method

1. Ownership of an **object** - a card, bar code, keys
2. **Password**
3. Verification of physiological characteristics - **biometrics**

Authentication issues:

- Too many passwords to different systems
- Ambiguity of identity (somebody else under identical username in a different system)

Biometrics Verification

- Fingerprints
- The image of the retina and iris
- Face Detection, palms
- Voice recognition
- Hand geometry
- Face geometry
- Verification method according to eye movement (Gliwice, Poland)
- The surface topography of the cornea
- The structure of the veins on the wrist
- Dynamics of signature, typing
- The shape of the article finger and fist
- Dynamics of walk
- The acoustic characteristics of voice
- Verification by smell
- Verification according DNA sample

- Verification according to the shape and movement of the lips
- Identification by spectroscopy skin
- Biometric characteristics teeth
- Identification by plantogram (feet barefoot man)

Problems of biometrics method:

- Difficulty in measuring biometric information
- Verification that the user is alive (LIVENESS Test)
- Dependence of measurement on environment and physical condition of verified person

Errors of biometrics systems:

- **False Rejection Error** - authorized user is denied access to the system
- **False Acceptance Error** - unauthorized user is recognized as a legitimate one by biometric device
- **Failure to Enroll Rate** - indicates the proportion of subjects who failed in reading process of characteristics
- **False Match Rate (FMR)** - indicates the proportion of people who are incorrectly recognized as an accredited during the comparative process
- **False Identification Rate** - indicates the probability that within the process of identifying the biometric value (characteristic) is incorrectly assigned to any of reference sample
- **False Non-Match Rate (FNMR)** - indicates that authorized persons are incorrectly unrecognized during the matching process. In comparison with the FRR it is different - it does not include the rejection by the poor quality of the scanned image.
- **False Rejection Rate - FRR**

  $FRR = N_{FR} / N_{ELA}$ [%]

  $\mathrm{N_{FR}}$ - Number of False Rejection

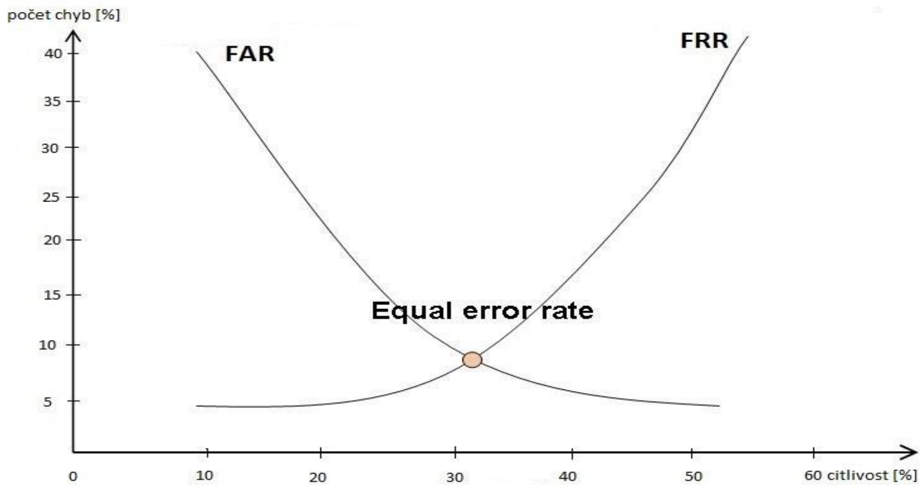
  $\mathrm{N_{ELA}}$ - Number of Enrolee Identification Attempts

- **False Acceptance Rate - FAR**

  $FAR = N_{FA} / N_{IIA}$ [%]

  NFA - Number of False Acceptance

  NIIA - Number of Impostor Identification Attempts



Authentizaton Aproach

- **User-centric** - verifies the user
  - **OpenID** - decentralized authentication protocol; allows users to be authenticated by co-operating sites using a third party service
  - **LiveID** – single sign-on web service developed and provided by Microsoft
  - **OpenAuth, Facebook Connect**
- **Institution-centric** - verifies the authorization role within the organization

  Shibboleth - Single Sign-On - It allows people to sign in using just one identity to various systems runs by federations of different organizations or institutions. The federations are often universities or public service organizations.

Kerberos - is a computer network authentication protocol that works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Kerberos builds on symmetric key cryptography and requires a trusted third party. Kerberos uses UDP port 88 by default.