Authentication

By

Hafez Barghouthi

Authentication: First some examples

- Passwords and PIN codes
- Passport with picture of face
- Faces of friends and family
- Voice on phone
- Email address
- Blind date with red rose

Authentication: Definition

- Authentication:
  - By authentication we mean verifying a claimed identity
- Identification:
  - By identification we mean establishing an identity

Authentication: Authentication vs identification

- Authentication (also called verification)
  - Identity is provided
  - Is he really who he claims to be?
  - One-to-one verification
- Identification
  - No identity is provided
  - Who is he?
  - One-to-many

Authentication: Focus of course

- Authentication, not identification
- Machine, not human
- Authentication systems
  - Enrollment
  - Authentication

Authentication: Parties involved

- There are in general 3 parties involved in an authentication process:
  - The authenticator (or user).
  - The verifier.
  - The attacker.

Authentication: Authentication Factors

- Currently we have 3 authentication factors:
  - Know: something only you remember
  - Have: something only you possess
  - Are: some biometric property

Authentication: Know - 1

- Basis:
  - Remembering a secret or recognition of a hidden item
- Open sesami

Authentication: Know - 2

- Examples:
  - Passwords, pass phrases, pass faces, PIN-codes

Authentication: Know - 3

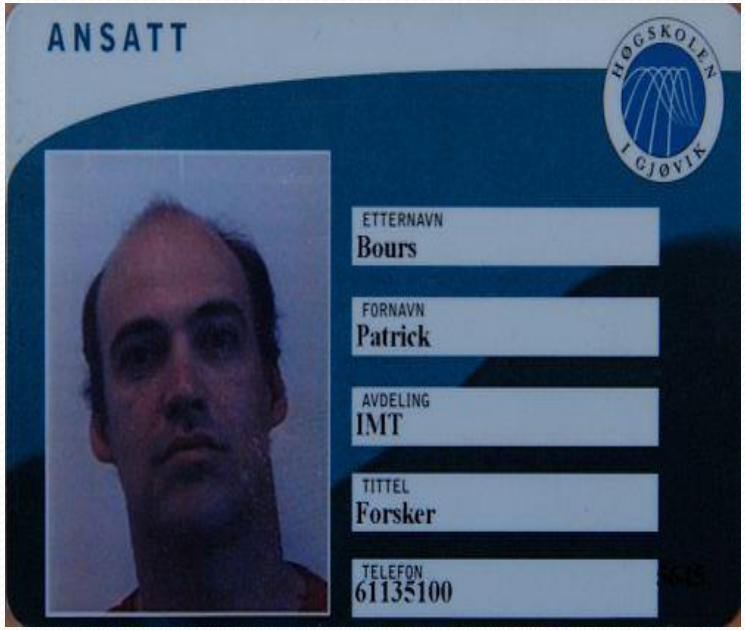
- Advantages:
  - Cheap and easy to implement, portable, widely available
- Disadvantages:
  - Sniffing attacks, easy to guess or hard to remember, easy to share, cost of handling forgotten passwords

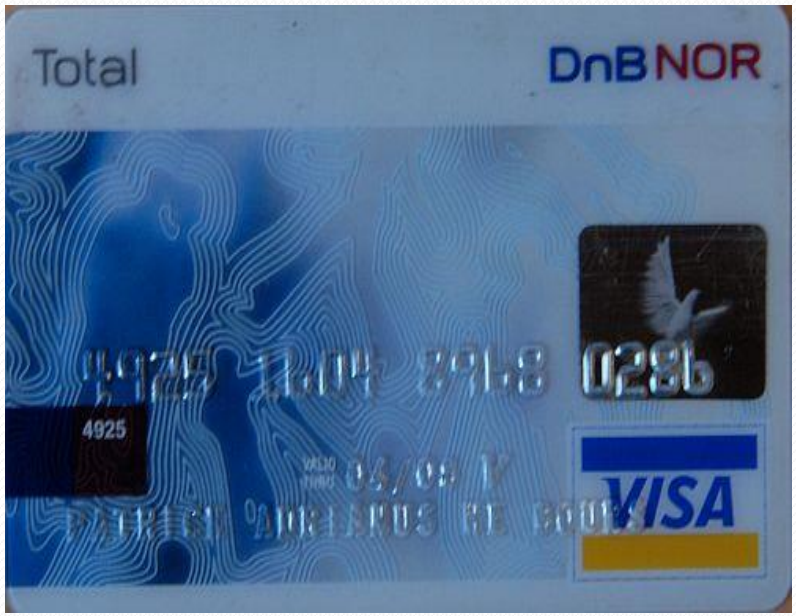
Authentication: Have - 1

- Basis:
  - Possession of some piece of hardware containing a secret

Authentication: Have - 2

- Examples:
  - Token (contact or contactless), smart card, mechanical key





Authentication: Have - 3

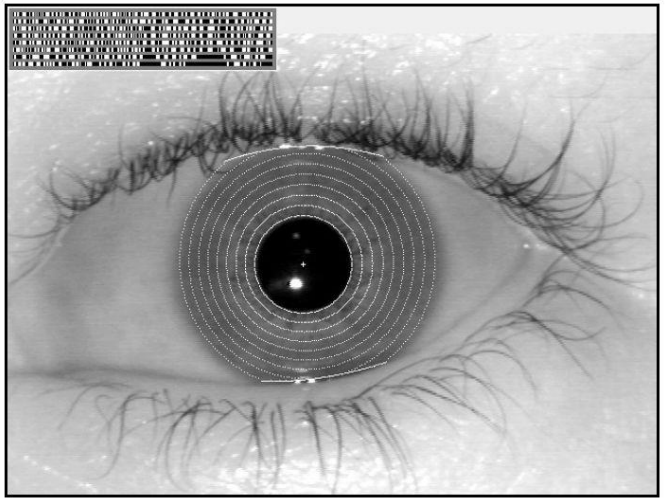
- Advantages:
  - Hard to abuse, easy to use
- Disadvantages:
  - Expensive, can be lost or stolen, hard to replace
- More information:
  - Often used with password or PIN-code (two-factor authentication)

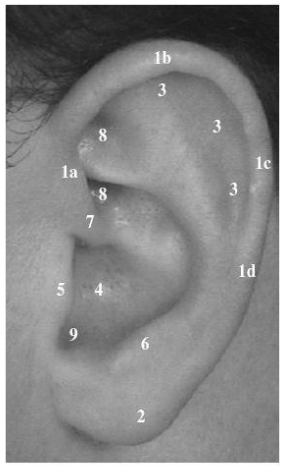
Authentication: Are - 1

- Basis:
  - Physiological (static) or behavioral (dynamic) biometrical properties

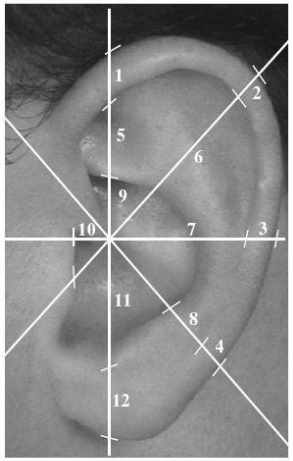
Authentication: Are - 2

- Physiological examples:
  - Fingerprint, face, retina, iris, DNA

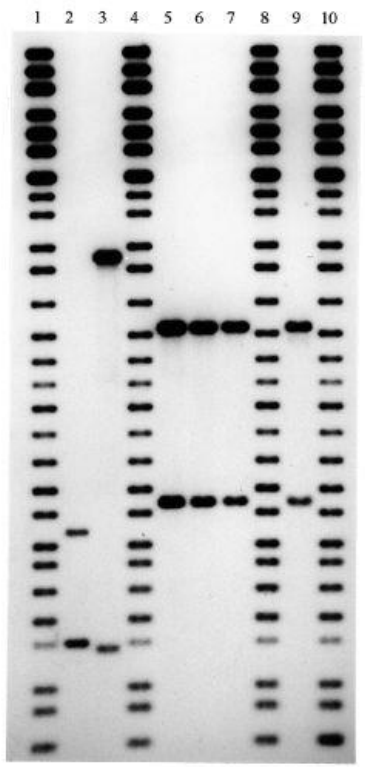




(a) Anatomy.

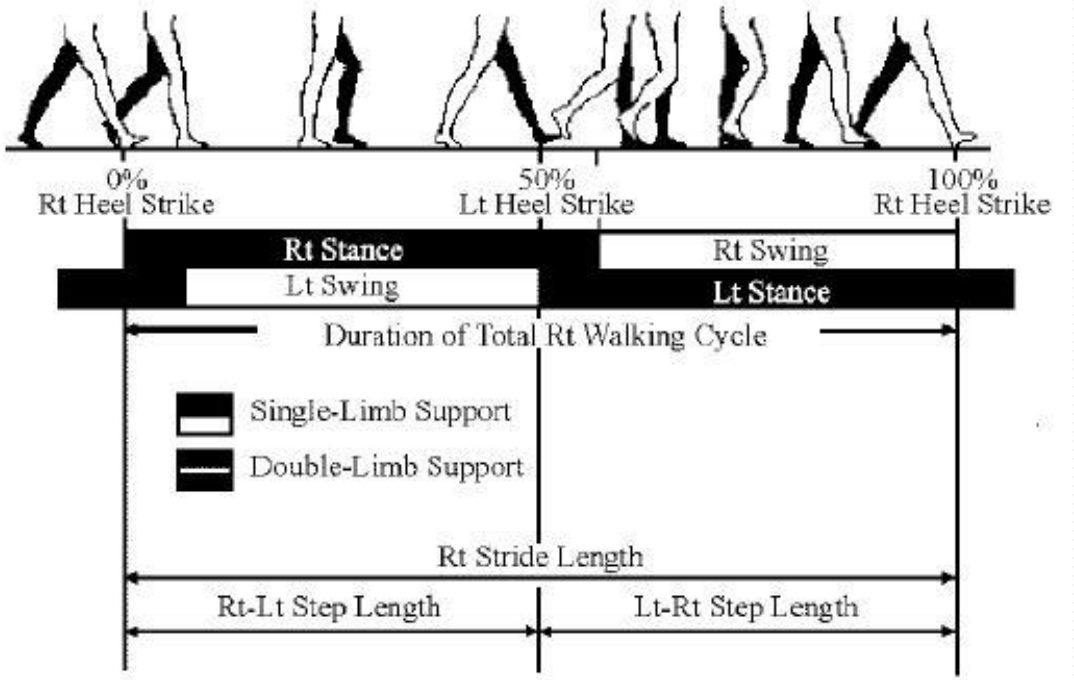


(b) Measurements.



Authentication: Are - 3

- Behavioral examples:
  - Voice, signature, keystroke, gait



Authentication: Are - 4

- Advantages:
  - Easy to use, portable
- Disadvantages:
  - Expensive, replay attacks may be possible, privacy issues, characteristics can (in general) not be changed, characteristics can be injured, intrusive

Authentication: Biometrics

- Fingerprint
- Face
- Hand
- Iris
- Retina

- Voice
- Signature
- Gait
- Keystroke dynamics

- Thermo gram
- Vascular patterns
- Ears
- Odor

- DNA

- Footprint
- Others…

Authentication: Other factors

- Somewhere you are
  - Authenticating a geographical location
  - Uses GPS satellites (global position system)
- Something you think (pass-thoughts)
  - Humans brain waves are identical
  - Can maybe used for verification
- Any others???

Authentication: Multiple authentication factors

- Two factor authentication:
  - Know and have (bank card and PIN code)
  - Have and are (token with fingerprint reader incorporated)
  - Know and are (fingerprint and PIN code)
  - Are and are (two biometrical features, e.g. finger and iris or 2 different fingers)

Authentication: Best authentication?

- Dependent on side conditions
  - Phone based banking: PIN or voice
  - Computer access: password or token
  - Computer access: finger or face
  - High security buildings: iris
  - Parking lot access: wireless token