

Authentication of People

- what you know (passwords)
- what you have (keys)
- what you are (biometric devices)
- where you are (physical)

Passwords

- initial password distribution (students)
- limit password guessing \implies denial-of-service
- make pronounceable, add punctuation, numbers
- need 64 bits of secret:
 - 20 random digits
 - letters, digits, punctuation: 11 characters
 - pronounceable: 4 bits/character \implies 16 characters
 - own password: 2 bits/character \implies 32 characters

Trojan Horses

- limit appearance (border, characters, interrupts)
- show failed attempts at next successful login
- prevent login by user programs

Initial Passwords

- need to meet root
- ATM PIN entry
- pre-expired passwords
- difficulty: can't change passwords (locks, Windows'95)

Authenticating Tokens

- magnetic cards, memory cards (European phone cards)
- smart cards: challenge/response
- cryptographic calculator: typing, display encrypted time

Biometrics – Accuracy

False acceptance rate (FAR): The percentage of unauthorised persons accepted in error.

False rejection rate (FRR): The percentage of authorised persons who are incorrectly denied acceptance.

- one-try
- three-try
- remove “unstable” population
- can adversary select impostors?
- identical twins, family members vs. random impostor
- fraud: with or without cooperation of Alice?

Fingerprints

False rejection rate: 1 to 5 % (three tries).

False acceptance rate: 0.01 - 0.0001 % (three tries).

Vulnerability: Dummy fingers and dead fingers

Ease of use: Easy to use, but “suspect”

Suitable: Not for people with damaged fingerprints due to daily handling of rough material.

Speed: 2 seconds

Storage: 800–1203 bytes

Stability: change for children

Hand Geometry

False rejection rate: 0.2 % (one-try)

False acceptance rate: 0.2 % (one-try)

Vulnerability: difficult without cooperation

Suitable: rheumatic hands

Speed: < 3 seconds

Storage: 9 bytes

Stability: change for children, weight gain

Use: Kennedy Airport

Retinal Scans

retinal vascular pattern

False rejection rate: 12.4 % (one-try), 0.4 % (three-try);

False acceptance rate: 0

Vulnerability: None; false eyes, contact lenses and eye transplants

Ease of use: difficult, socially unacceptable

Suitable: everyone with eyes

Speed: 1.5 seconds;

Storage: 40 bytes

Stability: very stable; changed by some diseases/injuries

Voice Recognition

- single phrase \Rightarrow tape recorder
- changing phrases \Rightarrow unreliable
- background noise
- colds
- use with public phone

Signature

- shape and dynamics
- some signatures easily faked, some variable
- signing surface properties

Other Biometrics

- keystroke timing \Rightarrow network?
- hand veins
- finger geometry
- facial recognition \Rightarrow perspective

Recognizing Machines

Detect differences even if “output signal” is the same:

- reflective multi-faceted surfaces (ICBMs);
- magnetic particles on credit card;
- RF spectrum for phones