Biometrics 1
Intro & fingerprints

PV181 Laboratory of security and applied cryptography
Seminar 20. 11. 2019

Agáta Kružíková, 409782@mail.muni.cz
Martin Ukrop, mukrop@mail.muni.cz

CROCS
Centre for Research on
Cryptography and Security

Lecture structure

Seminar 1

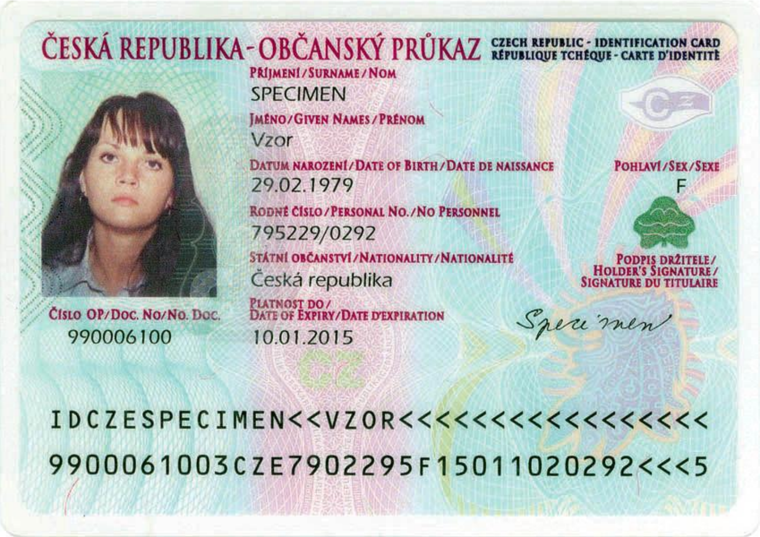
1. Introduction
2. Fingerprints
3. Seminar activity
   - Fake fingerprints
4. Homework
   - Report on selected biometric system

Seminar 2

1. Face recognition
2. Seminar activity
   - Face biometric SWOT analysis
3. Homework
   - Age estimation

Project Citizen K.

- 2010 “art” project by ZTOHOVEN
- 12 people had their Czech ID cards re-issued with morphed photographs
  - Similar haircut & style
  - Photos 50% themselves, 50% someone else
  - In 2010 you brought your own photo for the ID card



ČESKÁ REPUBLIKA - OBČANSKÝ PRŮKAZ
CZECH REPUBLIC - IDENTIFICATION CARD
RÉPUBLIQUE TCHÈQUE - CARTE D'IDENTITÉ

PŘIJMENÍ/SURNAME/NOM
SPECIMEN

JMÉNO/GIVEN NAMES/PRÉNOM
Vzor

DATUM NAROZENÍ/DATE OF BIRTH/DATE DE NAISSANCE
29.02.1979

POHLAVÍ/SEX/SEXE
F

RODNÉ ČÍSLO/PERSONAL NO./NO PERSONNEL
795229/0292

STÁTNÍ OBČANSTVÍ/NATIONALITY/NATIONALITÉ
Česká republika

PODPIS DRŽITELE/
HOLDER'S SIGNATURE/
SIGNATURE DU TITULAIRE

ČÍSLO OP/DOC. NO/NO. DOC.
990006100

PLATNOST DO/
DATE OF EXPIRY/DATE D'EXPIRATION
10.01.2015

Specimen

```
IDCZESPECIMEN<<VZOR<<<<<<<<<<<<<<<<<
9900061003CZE7902295F15011020292<<<5
```

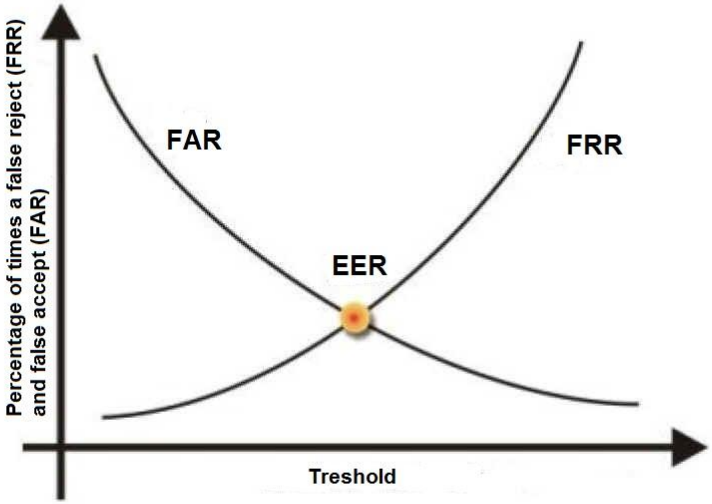
- Using someone else’s identity for several months
  - Wedding, gun licence, pilot licence, bank operations, out-of-Schengen travel, elections, ...

PS: Czech documentary can be legally streamed for 60 Kč

Biometrics – introduction

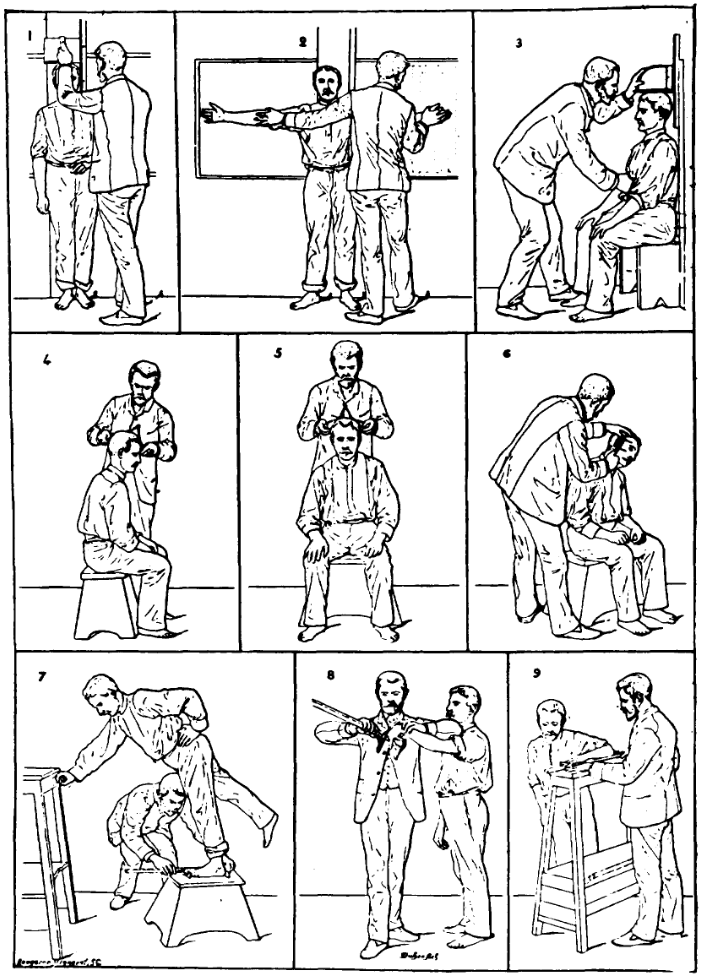
- Authentication based on:
  - something I know (e.g. password)
  - something I have (e.g. access card)
  - **something I am (e.g. fingerprint)**

- Never 100% match
  - FAR (false acceptance rate)
  - FRR (false rejection rate)



The beginning of anthropometry

- The Bertillon system (1882)
- 5–9 stable body features
  - Head length & breath
  - Middle finger & foot length
  - Cubit length
- Categorization
  - small/medium/large
  - In total: 243 bins

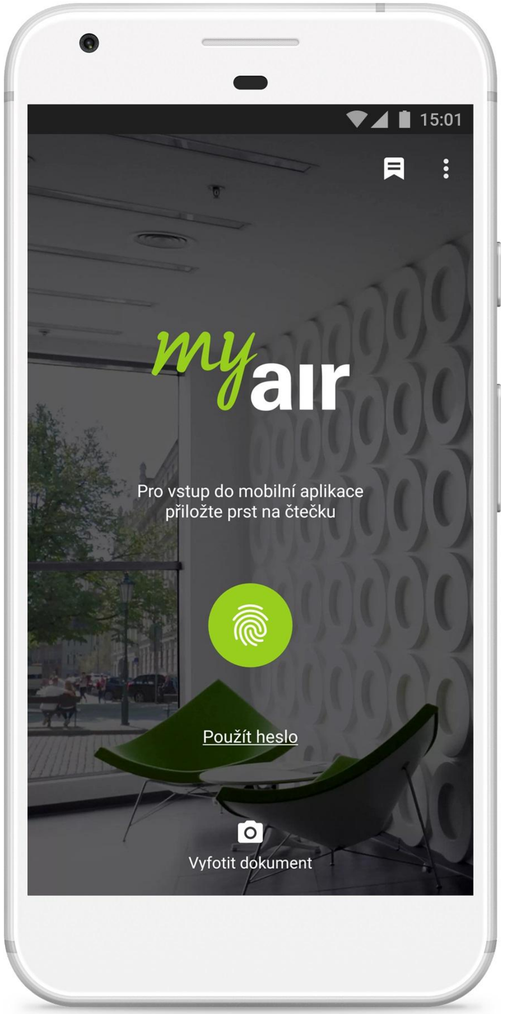


Basic criteria for biometrics

- Uniqueness (sufficiently different across population)
- Universality (everybody has it)
- Permanence (invariant in the period of time)
- Collectability (possible to measure and digitalize it)
- Performance (recognition accuracy should good)
- Acceptability (individuals should be OK to present it)
- Circumvention (hard to fake)

Biometrics now (optimistic)

- Smartphones
  - Fingerprints, face
- Passports
  - Fingerprints, face
- Contract signing
  - Signature
- Nuclear power plants :-)
  - Dukovany use hand geometry



Biometrics now (pessimistic)

- Fingerprint reader EULA:

  The biometric (fingerprint reader) feature in this device ***is NOT a security feature*** *and is intended to be used* ***for convenience only****. It should not be used to access corporate networks or protect sensitive data, such as financial information.*

- Other problems
  - Unencrypted transfer, liveness detection, ...

Biometrics soon (maybe?)

- MasterCard’s Identity Check Mobile
  - Prove holder’s identity by fingerprint/selfie
  - Blinking/nodding as liveness testing
  - Being introduced in 12 EU countries
  - Supported by Alibaba e-shop
- *“Selfies to kill off passwords ‘in five years’”* says MasterCard in 2015.
- Still not broadly used.

http://newsroom.mastercard.com/eu/press-releases/mastercard-makes-fingerprint-and-selfie-payment-technology-a-reality/

Less-used biometrics: Physiological

- Cardiac signature (for Pentagon)
  - Laser-based system
  - Identifying people at a distance 200m and more
- Hand vein pattern
- Ear shape
- DNA
- Crazy ideas:
  - Scent/odor
  - Bum detection

Less-used biometrics: Behavioral

- Keystrokes
- Signature dynamics
- Voice
  - used by Česká spořitelna
- Walking dynamics
  - tried by police in China
- Indoor movements
  - more than two WiFI devices
  - possible future: monitor emotions and behavior patterns

Biometrics in the future (combined?)

Biometrics – basic problem?

Biometrics are not secret!

And cannot be changed...

Authentication types

Verification

- One to one.
- Determines if person is who he claims to be.

Identification

- One to many.
- Search entire database.
- Determine identity of person.

What could go wrong?

Commercial vs. forensic use

Commercial

- Low precision
- Enrollment can be repeated
- Only extracted characteristics saved
- Fast and automatic

Forensic

- High precision
- Enrollment just once
- Full biometric data saved
- Slower, expert interventions may be necessary

How much do you trust biometrics?

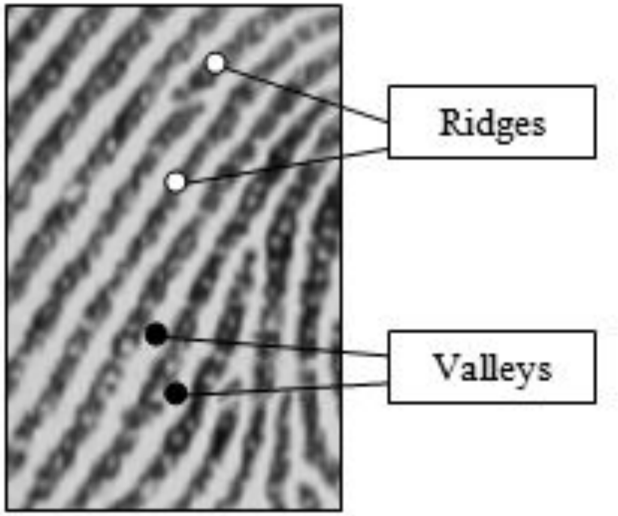
Would you use biometric authentication

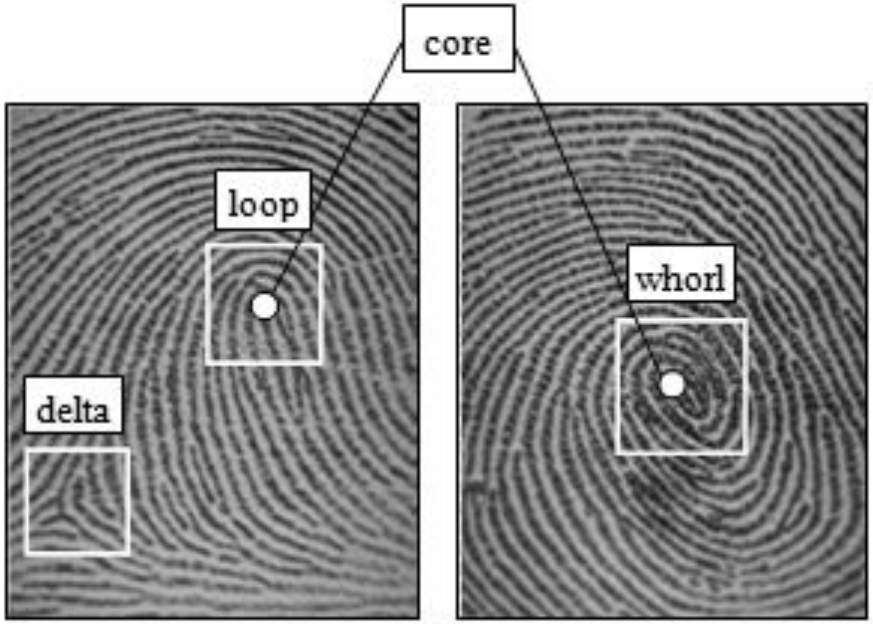
- … to access the library?
- … to log in to your work computer?
- … to do money transactions?
- … to secure the Declaration of Independence?

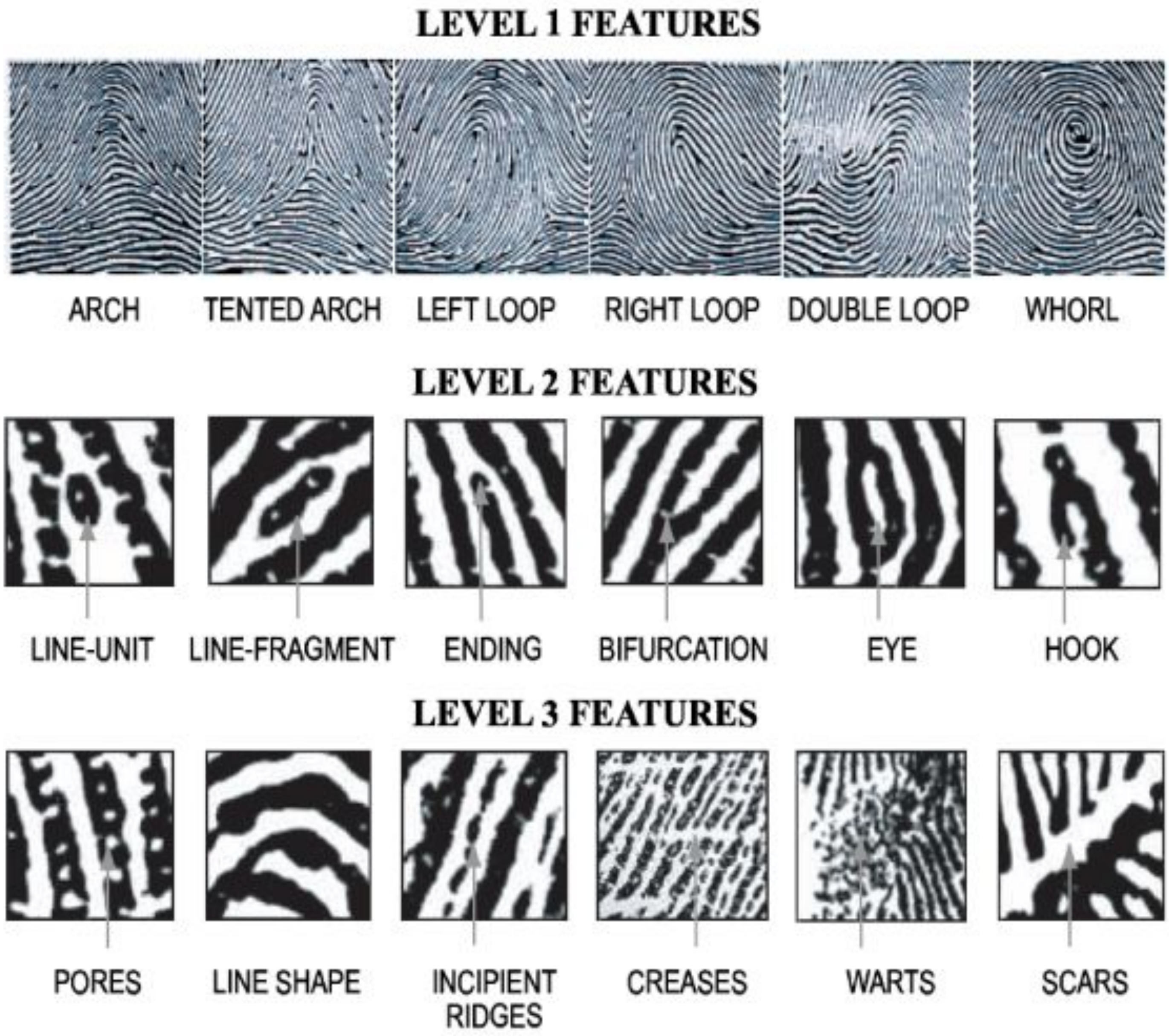
Fingerprints

Theory, technology, news, ...

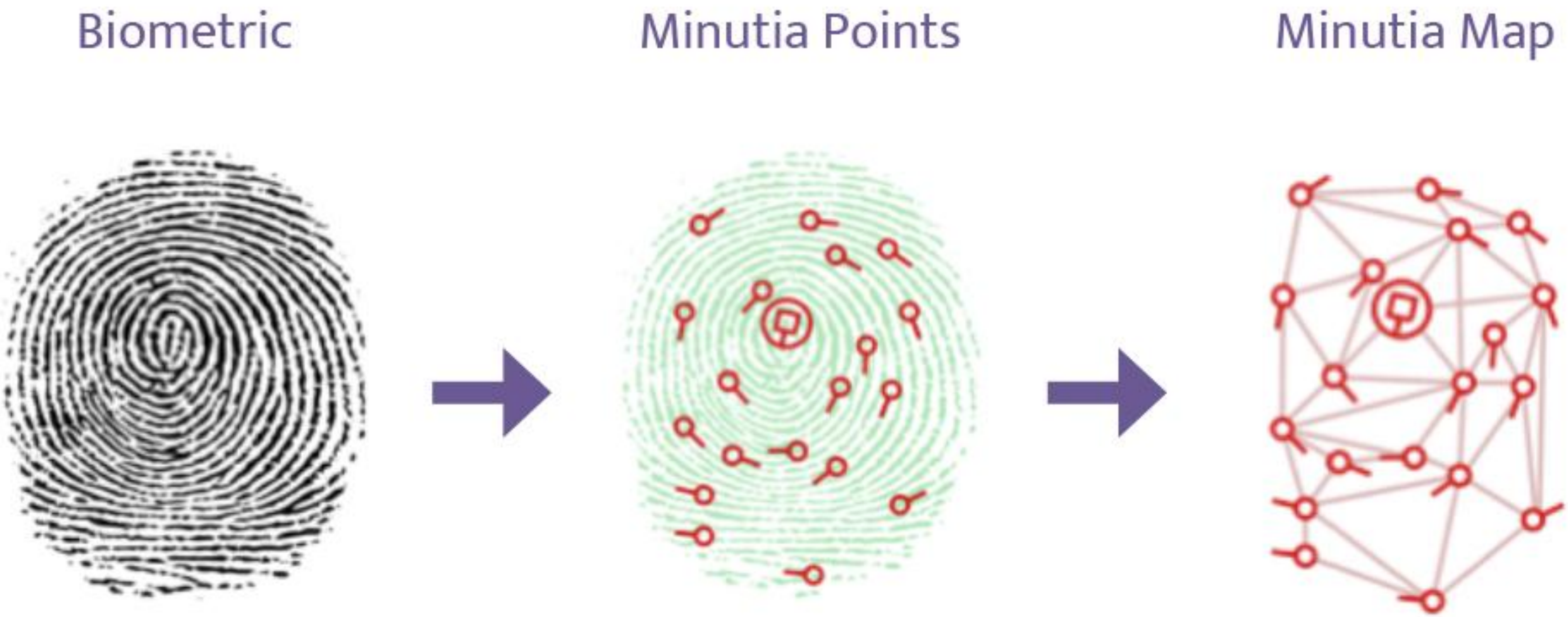
Fingerprint characteristics



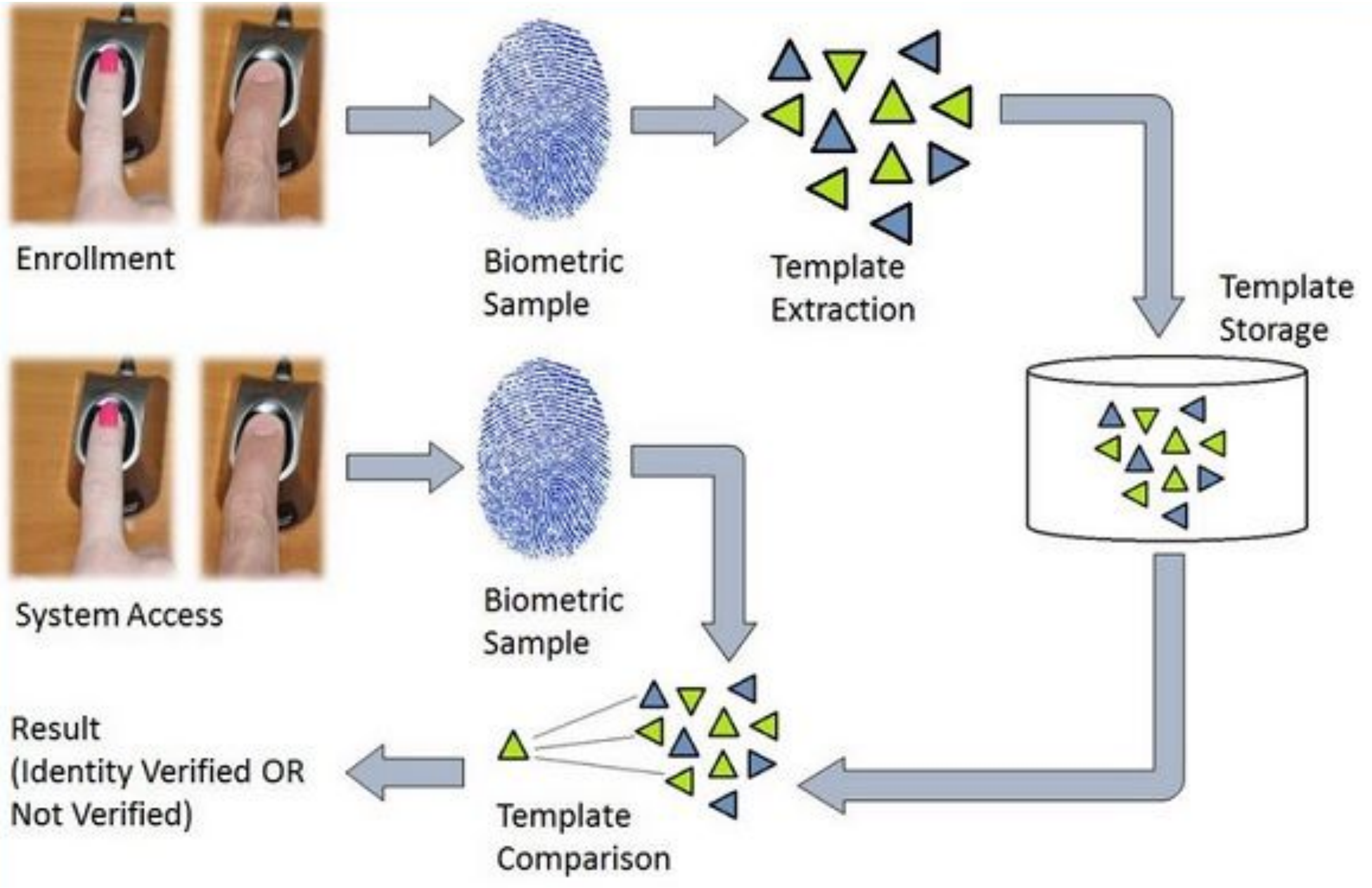



LEVEL 1 FEATURES
ARCH
TENTED ARCH
LEFT LOOP
RIGHT LOOP
DOUBLE LOOP
WHORL
LEVEL 2 FEATURES
LINE-UNIT
LINE-FRAGMENT
ENDING
BIFURCATION
EYE
HOOK
LEVEL 3 FEATURES
PORES
LINE SHAPE
INCIPIENT RIDGES
CREASES
WARTS
SCARS

Fingerprint minutiae


Biometric
Minutia Points
Minutia Map

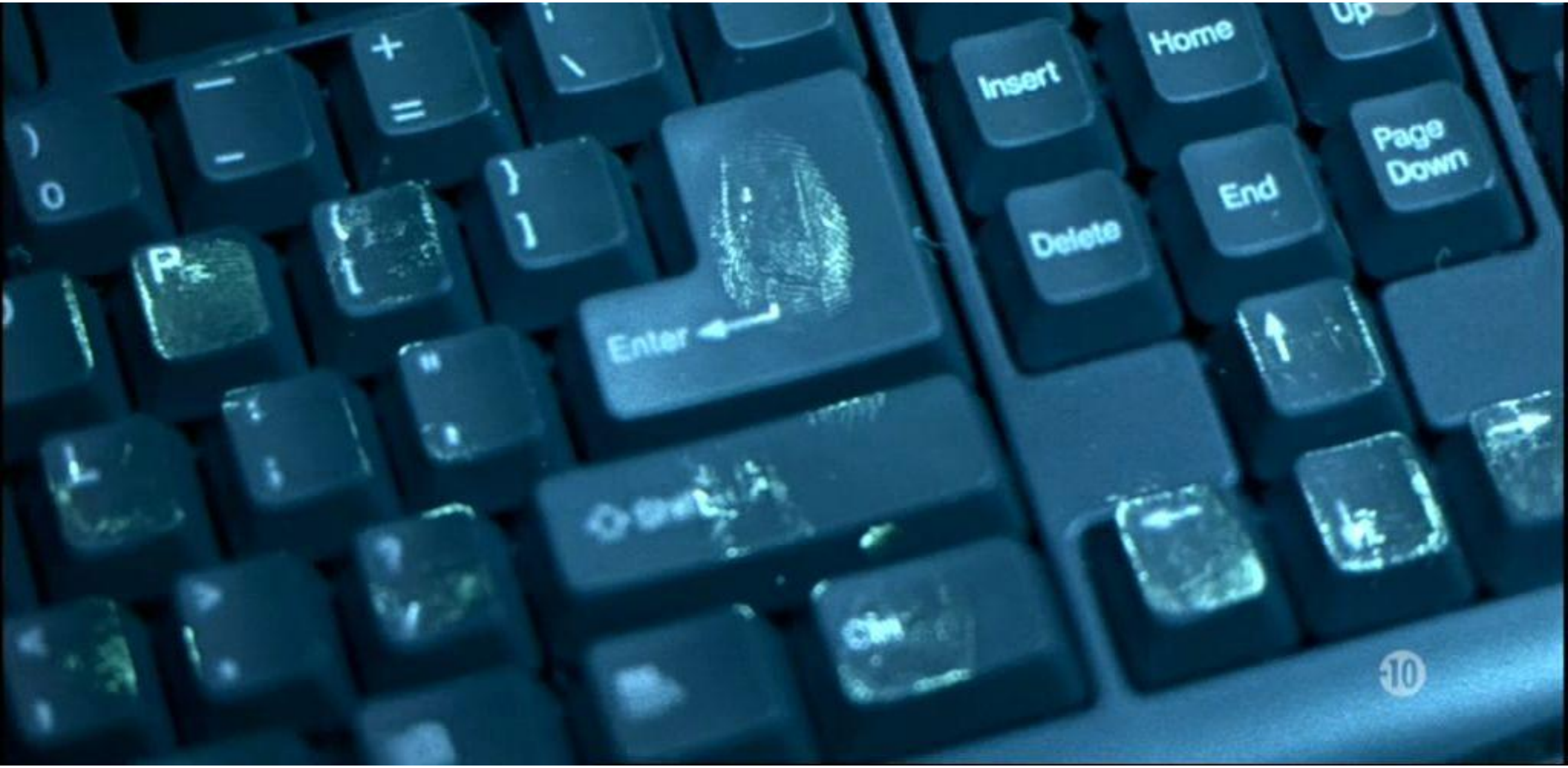
Fingerprint authentication



Fingerprint readers

- Various sensor types
  - Optical, capacitive, thermal, …
- Smartphone readers
  - Partial scanning (fewer unique features)
  - Liveness still an issue
- iPhone
  - In-screen fingerprint technology in the future?

Latent fingerprints



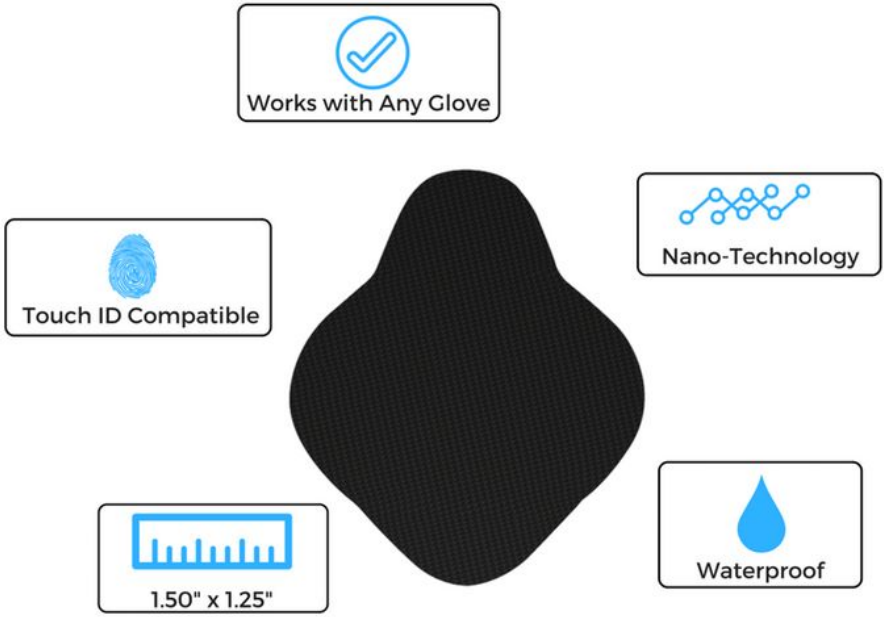
Attacks and liveness detection

- Attacks
  - Latent fingerprints, replay attacks, fake features, ...
- Liveness detection (!)
  - Testing the finger reaction to sensor stimuli
  - Temperature measurement
  - Skin resistance measurement
  - Pulse/blood flow measurement

News: TAPS

- Touchscreen Sticker with TouchID (KickStarter)
- “Biometric” authentication?

Photo © 2016 TAPS Kickstarter campaign



News: Fingerprint research in Brno (BUT)

- Cooperation with criminalists
- Fingerprint recognition with diseases
- Fingerprint generator: high quality, with diseases
- Fingerprint falsification: they hacked every system that exists
  - The best is spectral liveness control
- Research on foreigners
  - Only optical fingerprint reader recognises if the fingerprint is from Caucasian or African-American

Homework: Faking other biometrics

Write a short report (2+ pages) summarizing current usage and current faking techniques for a biometric system of your choice (but not fingerprint nor face).

- Deadline: 27. 11. 2019 8:00
- Up to 10 points awarded (see the scoring rubric)
- Submit a single PDF file to IS MUNI
  - File automatically prefixed by you name and UČO
- Cite all your references properly! (blogs, news, ...)
- Be concise using mostly your own words

Seminar task: Faking fingerprints

The task has several bottlenecks, so please adhere to the following:

I. Listen to the overview of the whole process.

II. Open the slides and follow the instructions.

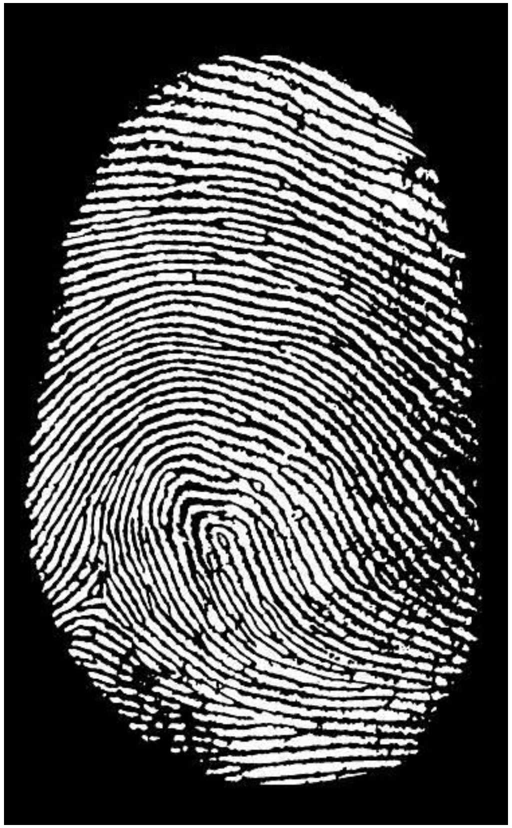
III. Consult us if you have not found it elsewhere.

Creating fake fingerprints I.

- Create visible fingerprint
  - Imprint finger
    onto photographic paper
  - Try multiple times
  - If you have dry fingers,
    touch some greasy place
    (e.g. behind your ears)
- Make ridges visible
  - Use brush & carbon powder
  - Handle the powder carefully

Creating fake fingerprints II.

- Scan the fingerprint
  - Have the photopaper scanned
  - Have it scanned
  - You can find it in the IS study materials
- Clean the image
  - Create **inverted 1-bit B/W image** With clear ridges (see right)
  - See GIMP basics later
  - Foil needs to have ridges when printed! (that’s why B/W)



Creating fake fingerprints III.

- Upload the **PNG(s)** image to IS folder
  - We'll print it for you on foil
- Cover in glue
  - The glue will form a copy of your finger
  - Cover a bigger area
    (it will shrink when drying)
  - Thin enough layer
    to dry out completely
  - Thick enough to hold
  - Avoid bubbles in glue

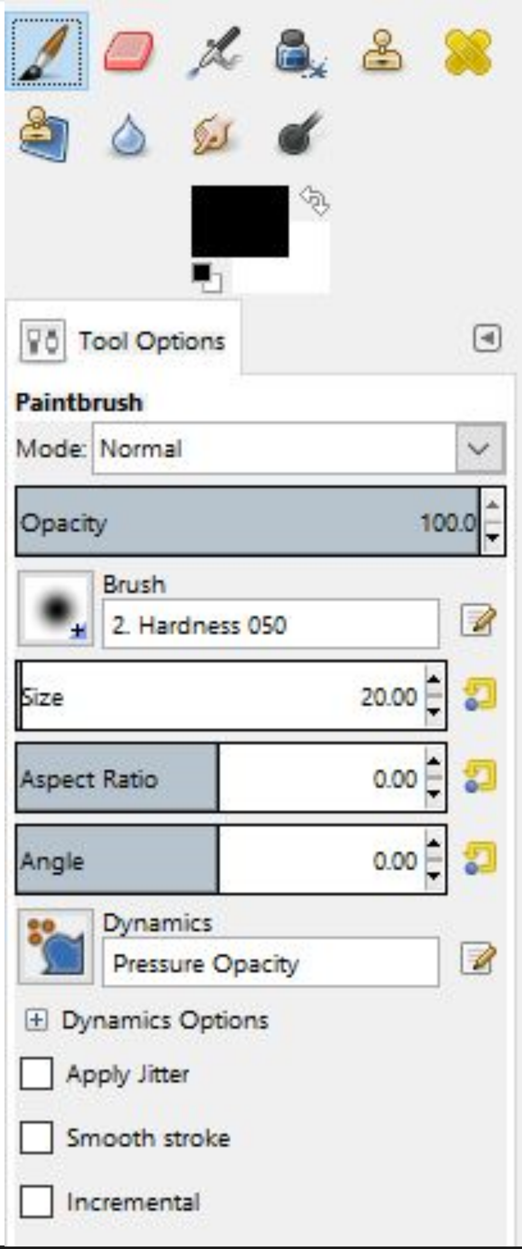
Creating fake fingerprints IV.

(next week, when the glue is dry)

- Peel the glue off the foil
  - Be extra careful!
  - Printing ink should peel off
- Try to verify the fingerprint on the reader
  - Read the finger and fake
  - Do visual comparison

GIMP basics

- Colors > Levels/Curves
  - Adjust the contrast
- Paintbrush
  - Clean the surroundings
- Image > Mode > Indexed
  - Convert to 1-bit B/W (not grayscale!)
- Crop as necessary
- Others as you see fit...



Tool Options

Paintbrush

Mode: Normal

Opacity 100.0

Brush 2. Hardness 050

Size 20.00

Aspect Ratio 0.00

Angle 0.00

Dynamics Pressure Opacity

Dynamics Options

□ Apply Jitter

□ Smooth stroke

□ Incremental