

# Biometrics 1

## Intro & fingerprints



**PV181 Laboratory of security and applied cryptography**  
**Seminar 9, 15. 11. 2017**

Vlasta Šťavová, [vlasta.stavova@mail.muni.cz](mailto:vlasta.stavova@mail.muni.cz)  
Martin Ukrop, [mukrop@mail.muni.cz](mailto:mukrop@mail.muni.cz)

**CRCS**  
Centre for Research on  
Cryptography and Security

# Lecture structure

## Seminar 1

1. Introduction
2. Fingerprints
3. Hands-on:
  - Generate fingerprints
  - Fake fingerprints
4. Homework:
  - Fake fingerprints

## Seminar 2

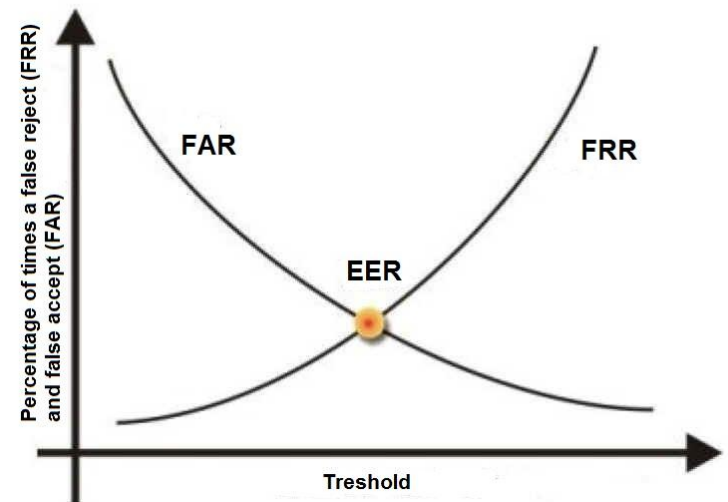
1. Face recognition
2. Hands-on:
  - Face matching
  - Fake fingerprints validation
3. Homework:
  - Age estimation

## Motivation on biometrics



# 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)



## Basic criteria for biometrics

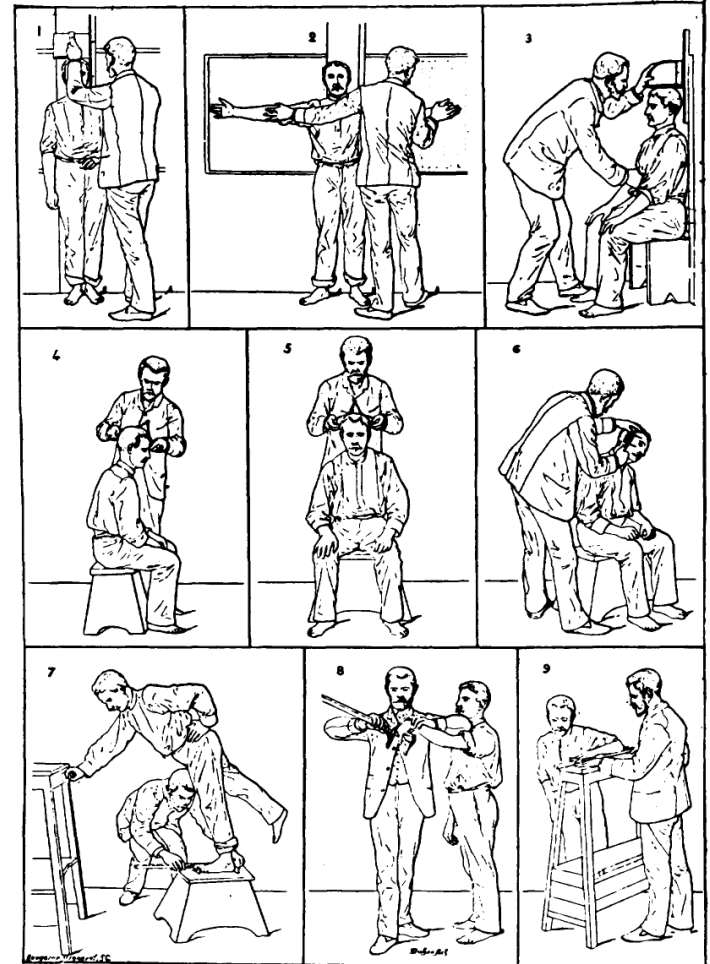
- **Uniqueness** (sufficiently different across population)
- **Universality** (everybody has it)
- **Permanence** (invariant in the period of time)
- **Collectability** (possible to measure and digitalize it)
- **Performance** (recognition accuracy should good)
- **Acceptability** (individuals should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

# Biometrics – introduction – discussion

- Physiological
  - Face
  - Fingerprint
  - Palm geometry
  - Hand vein pattern
  - Eye iris
  - Eye retina
  - Ear shape
  - DNA
- Behavioral
  - Keystrokes
  - Signature dynamics
  - Voice
  - Walking dynamics

# 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



# Mugshots



BUDDSDJ\_10



CAUGHMANMD\_3



CLYMANN\_1



DELAROSAJ\_2



CHEWEYSR\_22



CLARKJ\_6



DELOACHAM\_1

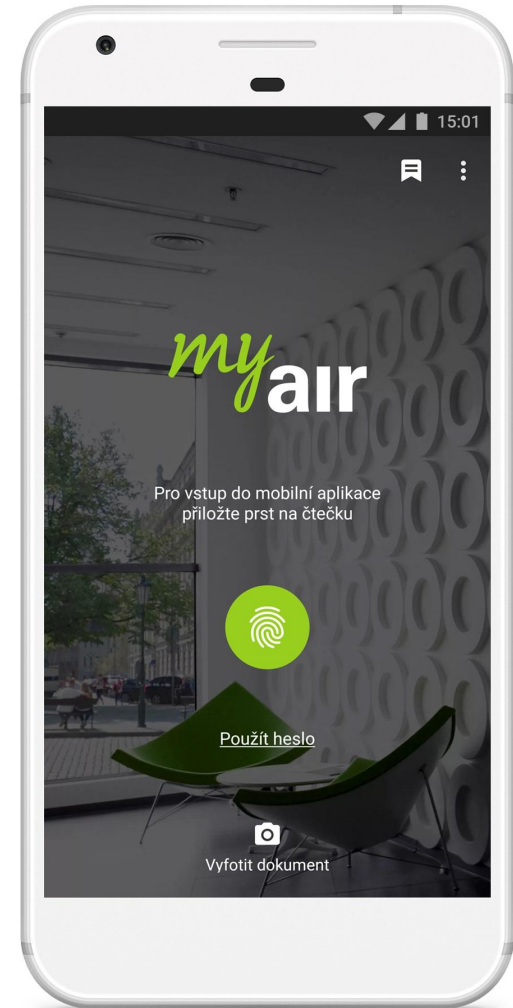


GILLEYNK\_1



## Biometrics now (optimistic)

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



## Biometrics now (pesimistic)

- 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 as liveness testing.
  - Being introduced in 12 EU countries
  - Supported by Alibaba e-shop
- *“Selfies to kill off passwords ‘in five years’”*  
says MasterCard.

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

# Biometrics in the future (combined?)



## Biometrics – basic problem?

**Biometrics are  
not secret!**

And cannot be changed...

## It's not so easy (math everywhere!)

- Image quality checking
- Feature detection and extraction
- Storage format (irreversibility!)
- Feature comparison (performance)
- Matching (accuracy, threshold)
- Liveness detection

# 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?

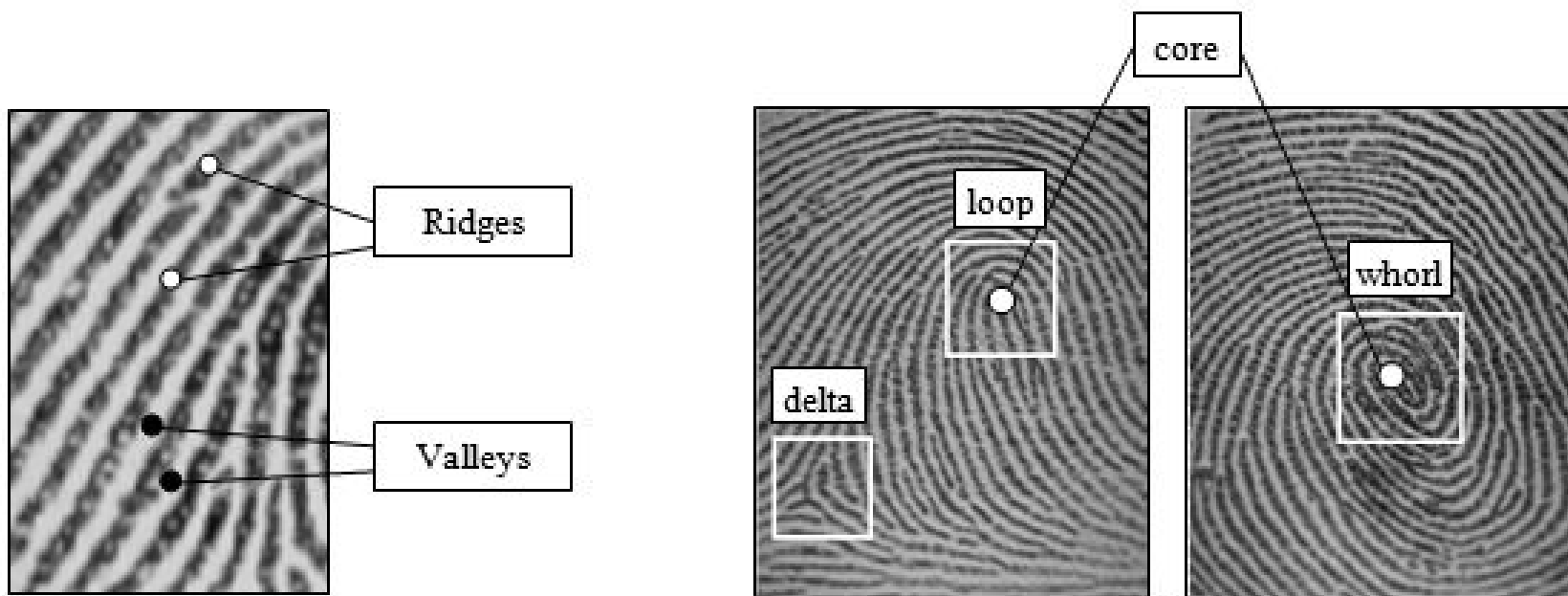
Would you use biometric authentication

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

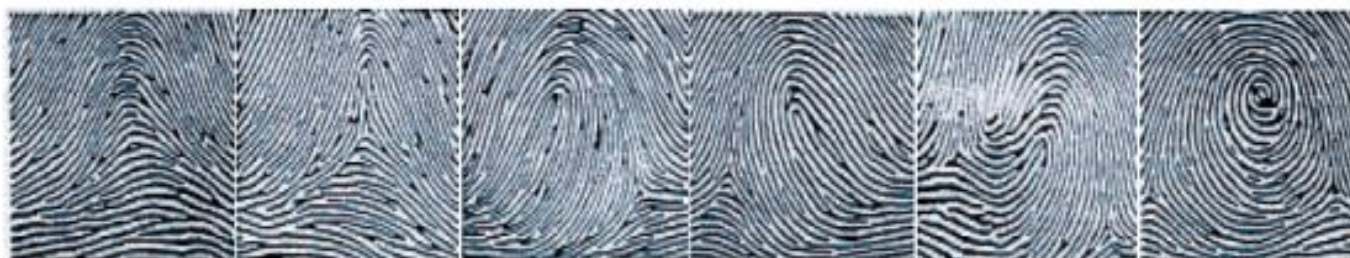
# Fingerprints

Theory, technology, news, ...

# Fingerprint characteristics



### LEVEL 1 FEATURES



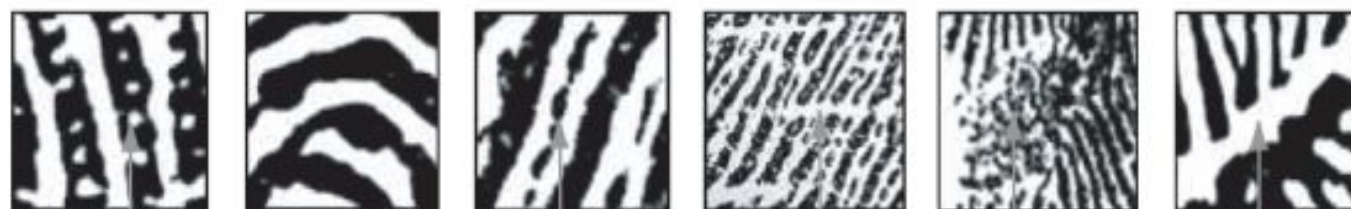
ARCH    TENTED ARCH    LEFT LOOP    RIGHT LOOP    DOUBLE LOOP    WHORL

### 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



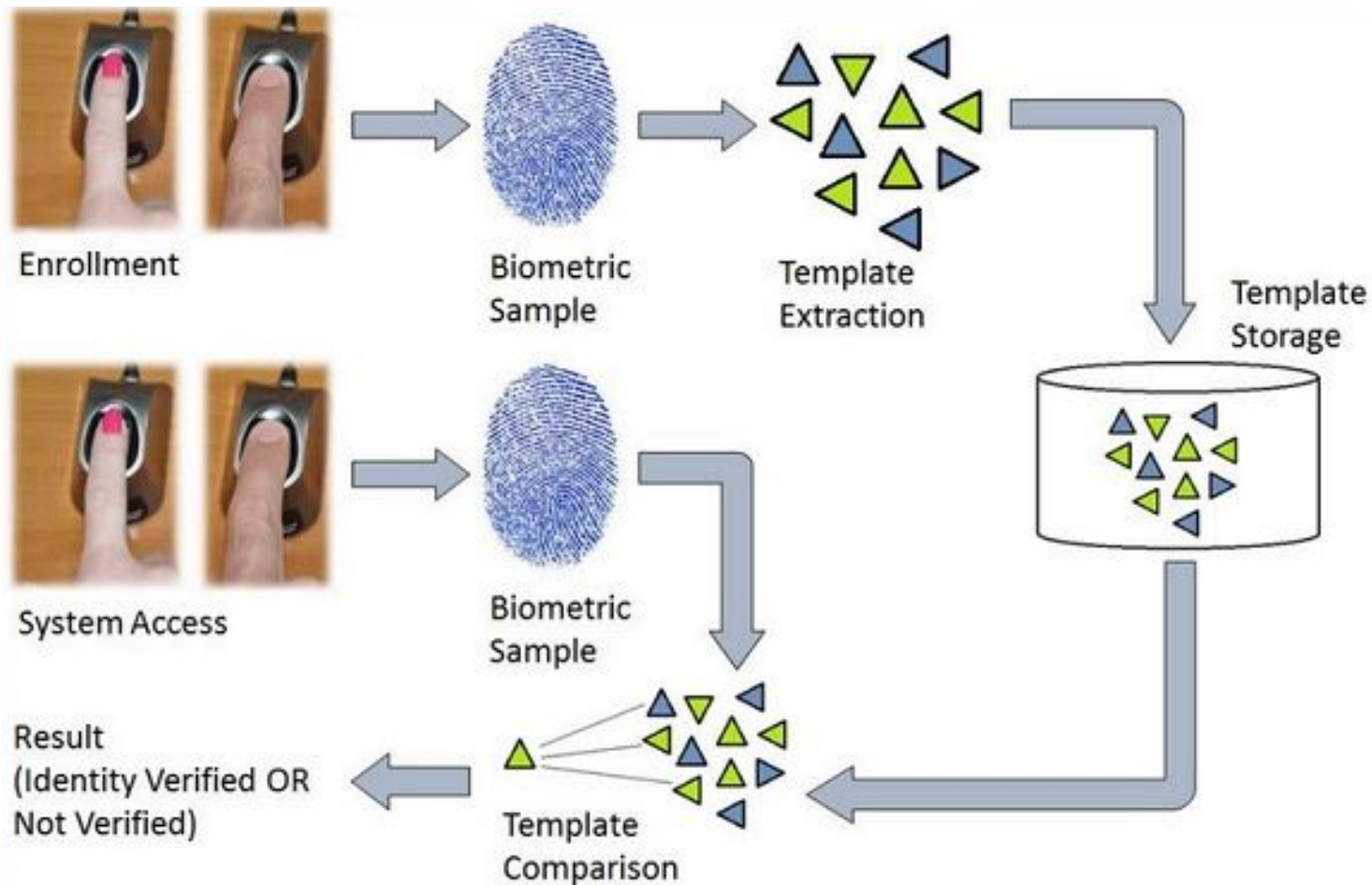
Minutia Points



Minutia Map



# Fingerprint authentication



# Fingerprint classification

Different approaches:

- based on singular points
- structure-based
- frequency-based
- mathematical models
- machine learning methods
- hybrid models
- ...

# Fingerprint readers

- Various sensor types
  - optical, capacitive, thermal, ...
- Smartphone readers
  - Partial scanning (fewer unique features)
  - Liveness still an issue
- iPhoneX
  - Only Face ID (no more the Touch ID)



## News: TAPS

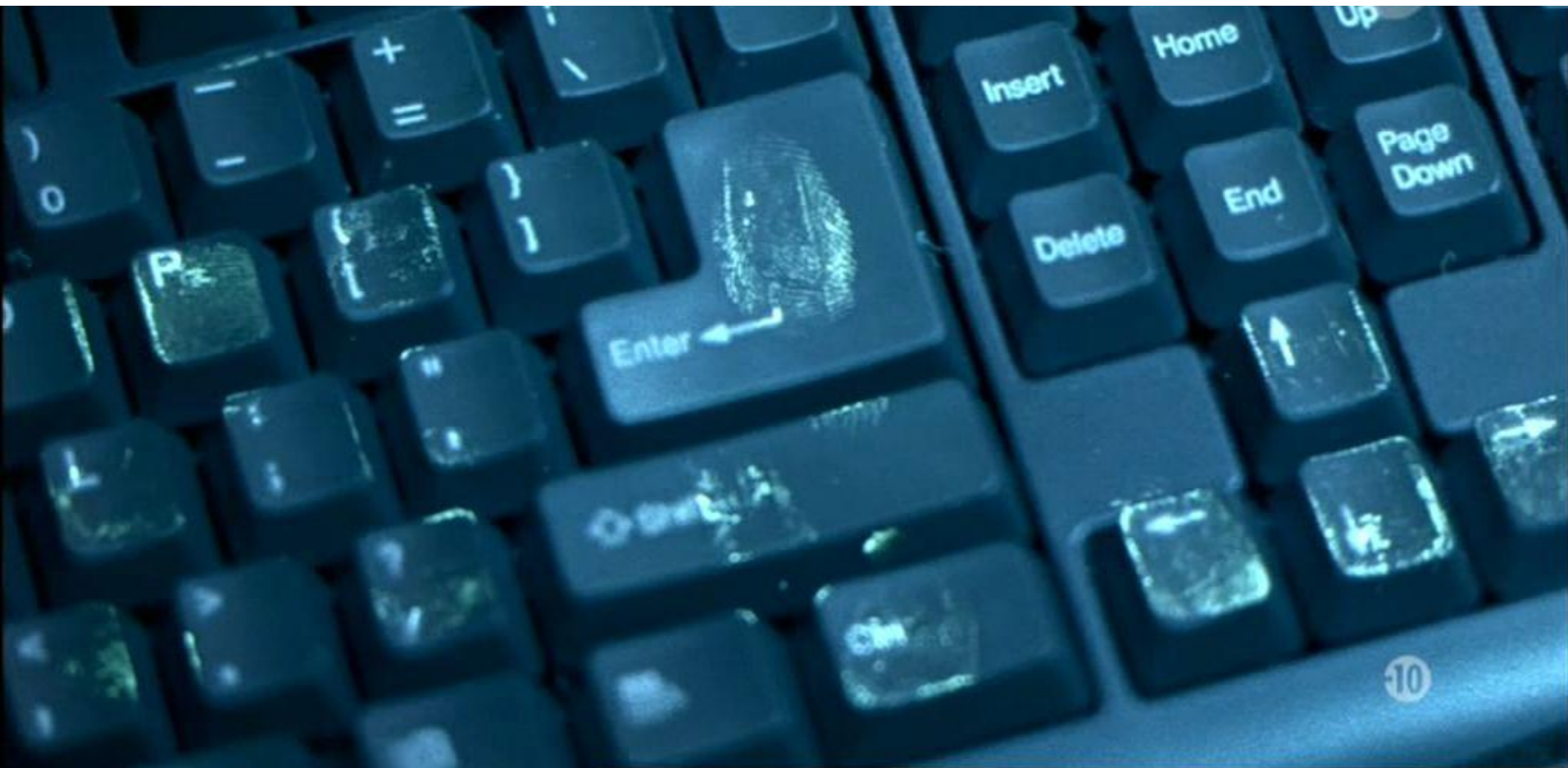
- [Touchscreen Sticker with TouchID](#) (KickStarter)
- *Something I have instead of something I am*



Photo © 2016 TAPS Kickstarter campaign



# 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

# Seminar task

Exploring possible defects in fingerprint reading

# Fingerprint generation

- Explore imperfections of fingerprint images
  - What can happen when touching the reader?
- Use SFinGe (*Synthetic Fingerprint Generator*)
  - By [Biometric System Laboratory, University of Bologna](#)
- Pre-installed on CRoCS PCs



# Fingerprint reader

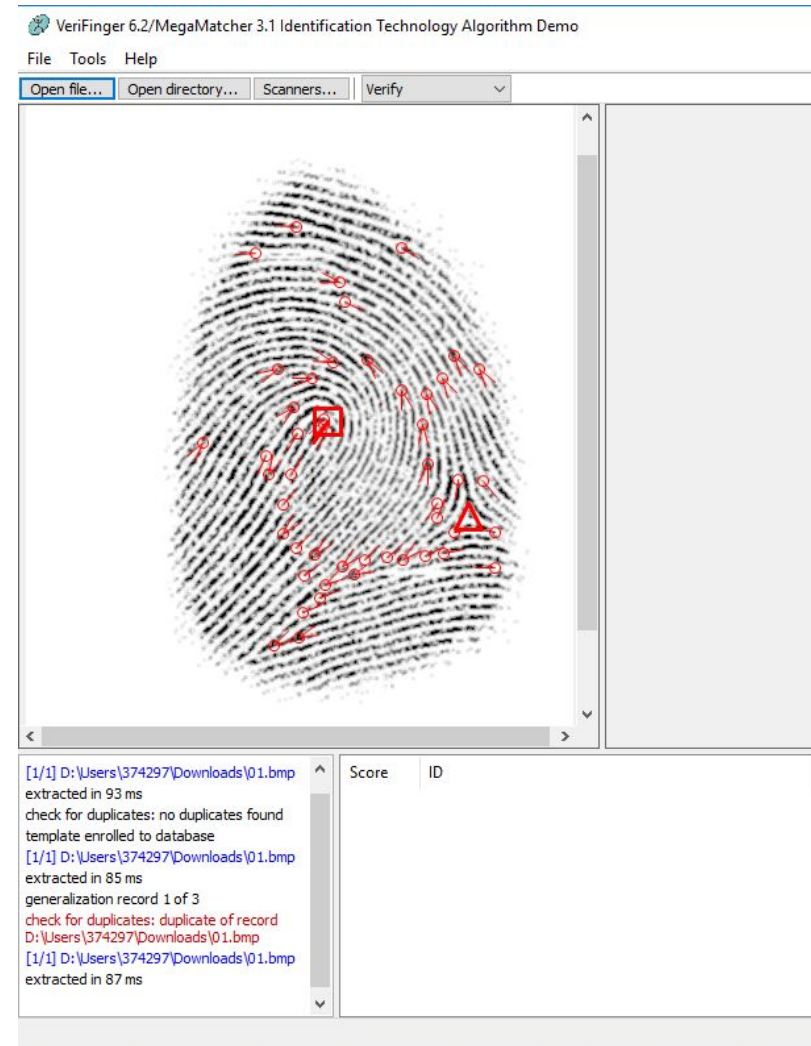
- Try the real reader
  - Optical, 500 ppi
  - “Infrared filter to improve ambient light rejection.”
  - No liveness detection :-/





# Compare fingerprints

- Explore fingerprint matching
  - Edit images with GIMP (What does it take not to match the image?)
  - Work with generated and/or your fingers
  - SFinGe: Screenshot and readjust the finger
- Software here:  
C:\ProgramFiles\Neurotechnology\FingersAlgorithmDemo3.1\FingersAlgorithmDemo.exe



# Homework

Creating fake fingerprints





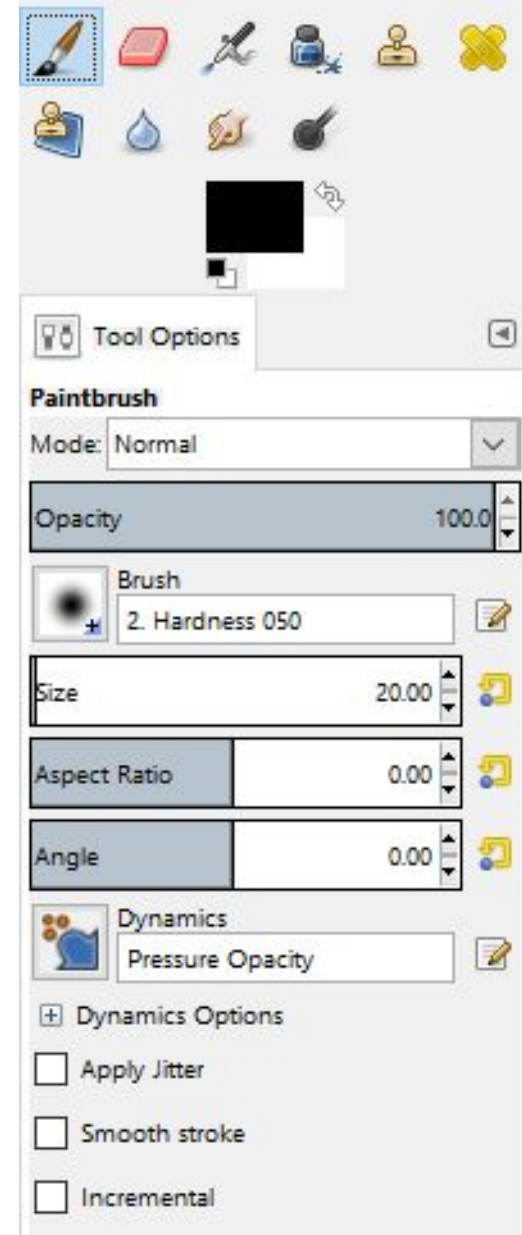
# Creating fake fingerprints I.

1. Create visible fingerprint
  - Imprint onto photographic paper
  - Make ridges visible using carbon powder
2. Scan the fingerprint
  - Come to the scanner [Vlasta]
3. Clean the image
  - Create B/W image with clear papillary ridges
  - **Invert colors**



# GIMP basics

- Colors > Levels/Curves
  - Adjust the contrast
- Paintbrush
  - Clean the surroundings
- Image > Mode
  - Convert to B/W (not grayscale!)
- Crop as necessary
- Others as you see fit...
- You may want single-window mode
  - Windows > Single-Window Mode



## Creating fake fingerprints II.

4. Print fingerprint on transparent foil
  - Upload cleaned PNG file to IS (HW vault)
  - We'll print it for you on foil [Martin]
  
5. Cover in glue
  - Idea: The glue will form a copy of your finger
  - **Make a THIN layer**



## Creating fake fingerprints III.

*(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
  - Enroll the tested finger
  - Use a different finger + fake fingerprint for verification