How to Set a Manufacturing Line for Fingerprint Faking

Vashek Matyáš (credits to Agáta Kružíková & CRoCS)
matyas@mail.muni.cz
CRoCS, Faculty of Informatics, Masaryk University

CRoCS
Centre for Research on Cryptography and Security

Agenda

- **Lessons learned from an earlier project**
- Fingerprint as the authentication method of choice
- Our fingerprint forgery workbench
- Results of our effort
- Limitations and resources

Back then… (in 2018-2020) in a project…

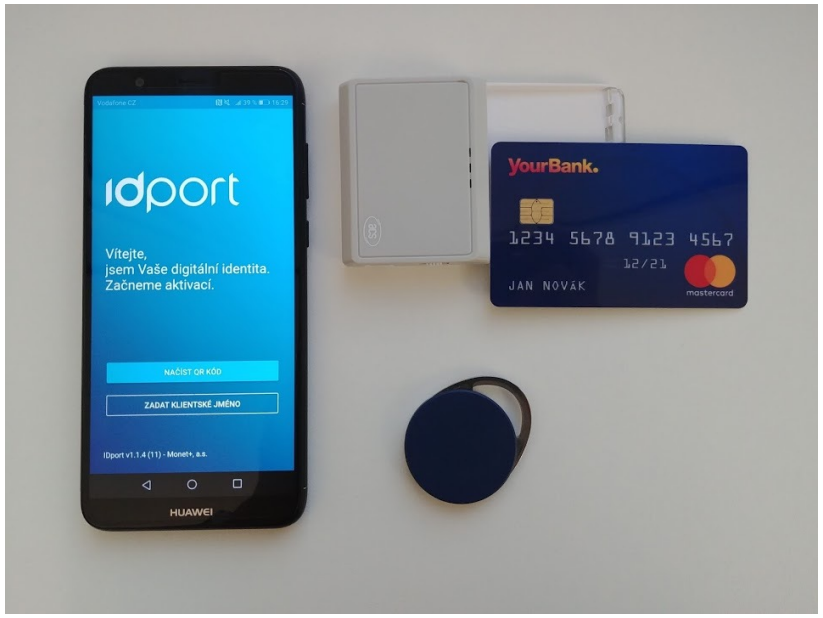
- ***Innovation and adaptation of authentication technologies for secure digital environment***

- Sponsor: Technology Agency of Czech Republic

- Cooperation between:
  - Centre for Research and Applied Cryptography
  - Interdisciplinary Research Team on Internet and Society
  - MONET+/AHEAD iTec

Investigated Authentication Methods

A. Numeric PIN code (6 digits)
B. Fingerprint
C. Hardware NFC token
D. Payment card with smartcard reader



Study Procedure

- Informed consent 
- Study description
- Demographic questionnaire 
- Getting familiar with the test smartphone 
- Scenario description 
- Fulfilment of the tasks 
- Questionnaires and interviews based on the fulfilled tasks 
- Recordings of the screens – for time measurement

Scenario Description

1. IDport – application of digital identity recommended by participant bank
2. IDport app activation
3. Login to m-banking
4. Payment of a bill

(Pre)testing

- Iterative process (“Nach der Schlacht ist jeder General”)

- 4 rounds
  - Each round just with few participants (up to ten)
  - Different authentication methods
  - Enhancements in the instructions and animations

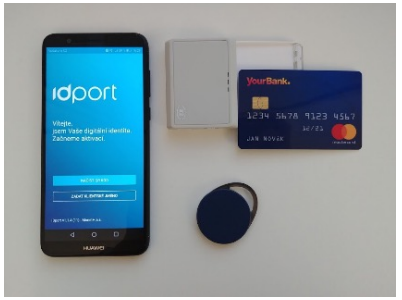
Sample Description & Data Collection

  - Smartphone users (Android OS)
- *Adults (N=250)*
  - Age: 26-54, median = 38
  - Representative sample from professional agency
  - 54% women, 69% full time job
- *The Ageing (N=250)*
  - Age: 55+, median = 61
  - Convenient sample, data collection organised by us
  - No education or work experience in IT
  - 61% women, 51% full-time job, 41% on pension

Usability and Security Perception

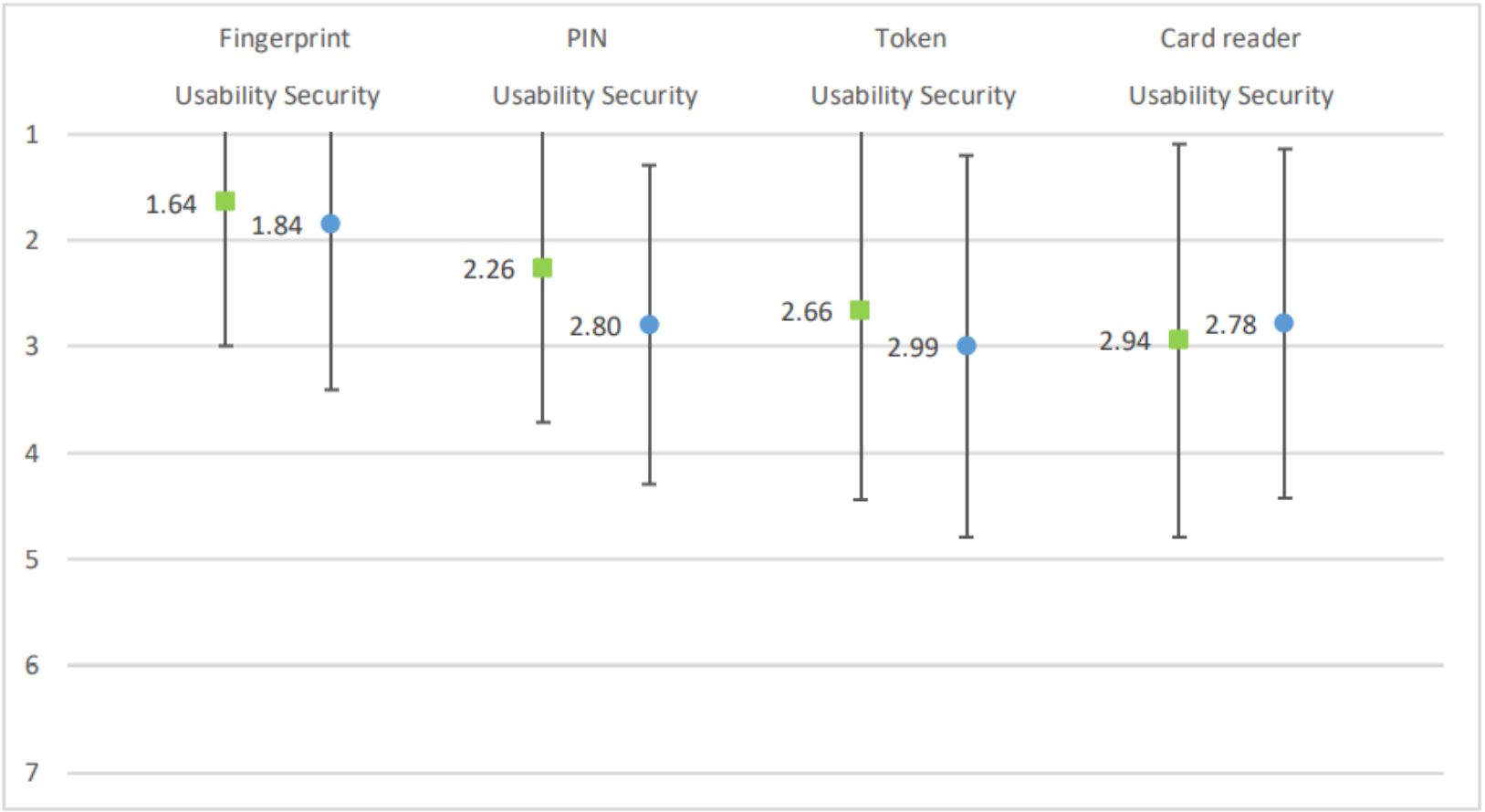
- RQ1: How do users evaluate selected authentication methods according to their perceived usability and security?
- Vote
  1. What method would be perceived as the best one for you?
  2. What method was perceived as the best one?
  3. Did participants perceive any differences for four tested methods?
  4. Did participants perceive all methods rather positive or rather negative?

A. Numeric PIN code (6 digits)
B. Fingerprint
C. Hardware NFC token
D. Payment card with smartcard reader



Method Evaluation

Method evaluation: We show mean scores and their confidence interval (with +/-1 standard deviation) for perceived usability and perceived security of each authentication method (1-best, 7-worst)



Usability and Security Predictors

- Possible predictors
  - Prior experience in banking: PIN and fingerprint
  - Smartphone usage self-efficacy
  - Smartphone security behaviour – self-developed
  - Knowledge of secure smartphone behaviour
- RQ2: What demographic characteristics and other factors are associated with the evaluation of these authentication methods?
- Vote
  - What factors predict perceived *usability*?
  - What factors predict perceived *security*?

Methods Perceptions

- Methods:
  A. Numeric PIN code (6 digits)
  B. Fingerprint
  C. Hardware NFC token
  D. Payment card with smartcard reader

- All methods perceived as rather positive
  – Fingerprint was rated as best in usability and security
- No uniformed predictor for usability and security perception across all tested methods

Time as Predictor: End-Users

- **Satisfaction with the time** spent on the authentication task is more important for a positive perception of the authentication methods than the **task completion time**

Limitations

- Android users can be more security and technology aware
- Convenience sampling – not representative
- Previous experience only for PIN and fingerprint
- Hypothetical scenario – not real and no long-term use
- Two separate apps – activation and usage

Agenda

- Lessons learned from an earlier project
- **Fingerprint as the authentication method of choice**
- Our fingerprint forgery workbench
- Results of our effort
- Limitations and resources

Biometrics have their issues…

- Biometrics are not secret
- Unknowingly sharing biometric data increases security risks
  - For example, challenges on social media can make it easier for attackers to obtain data
- Biometric sensors operate with a certain degree of error—they are never 100% reliable

Fingerprint forgery around for ages…

- Tsutomu Matsumoto 2002 – “gummybear attack”

- Attacks with latent fingerprints utilized both legally and illegally

- And more…

Fingerprint forgery from a photo

Other studies*

- Photo of latent fingerprints

*E.g., Goicoechea-Telleria, I., Garcia-Peral, A., Husseis, A., & Sanchez-Reillo, R. (2018). *Presentation Attack Detection Evaluation on Mobile Devices: Simplest Approach for Capturing and Lifting a Latent Fingerprint. 2018 International Carnahan Conference on Security Technology (ICCST).*

Our study

- Photo of a finger

Photo from the internet: https://www.pexels.com/photo/close-up-of-human-hand-327533/

Photo processing

- Fingerprint forgery simulation seminar

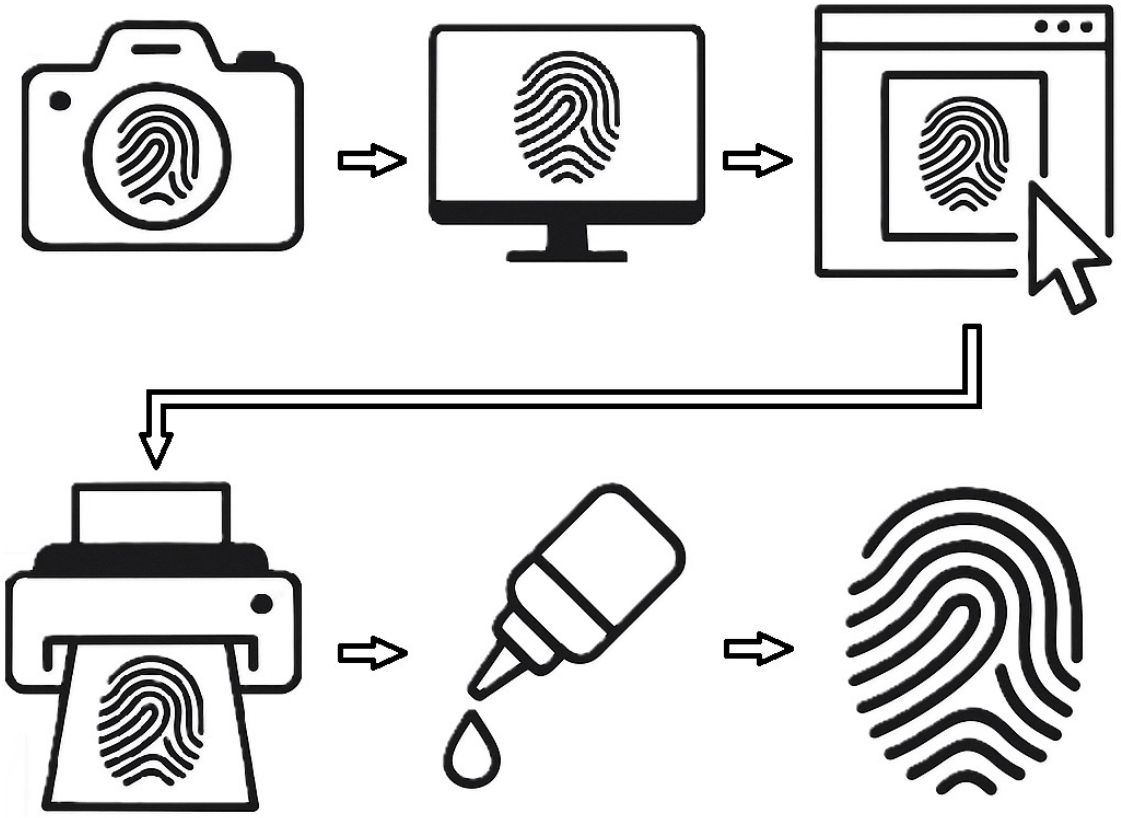
Example photo from a thumb (left) and result of our software processing (right)

Source: https://www.pexels.com/photo/close-up-of-human-hand-327533/

Agenda

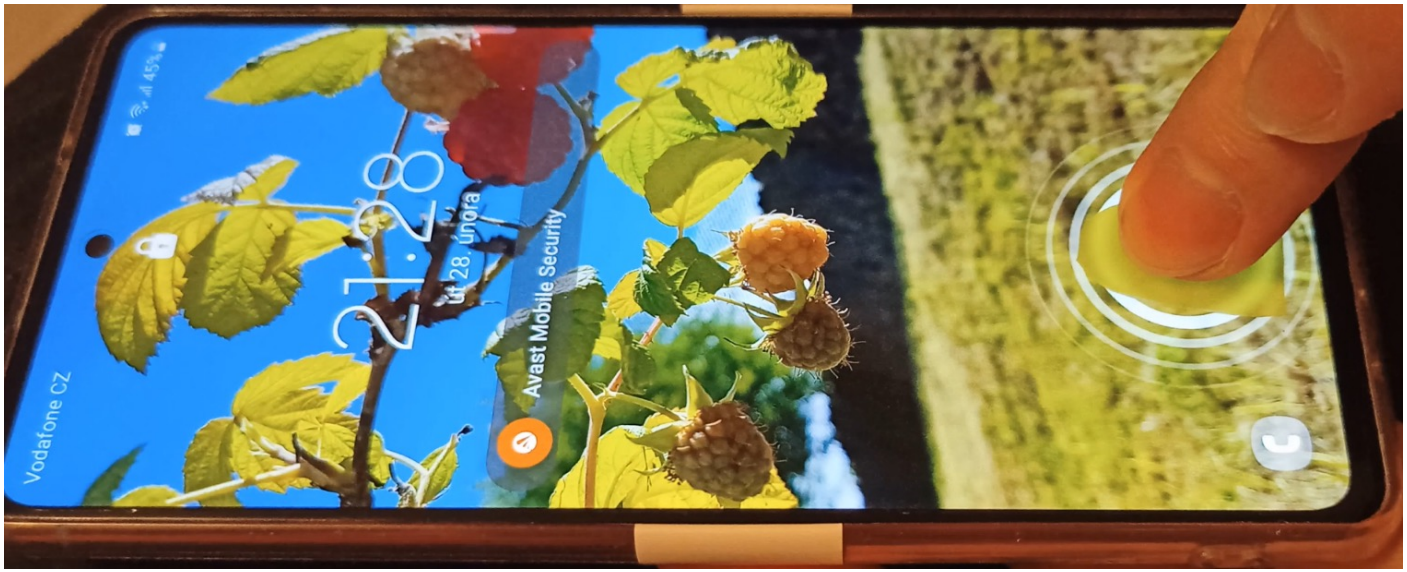
- Lessons learned from an earlier project
- Fingerprint as the authentication method of choice
- **Our fingerprint forgery workbench**
- Results of our effort
- Limitations and resources

Forgery process



Smartphone fingerprint readers

1. Unlocking with counterfeit
2. Registering a counterfeit as a new finger



Counterfeit processing

- Fingerprints scanned with external fingerprint reader (Futronic FS80H)
- Processed with NBIS (NIST Biometric Image Software) packages
  - Match score computed with BOZORTH3 algorithm

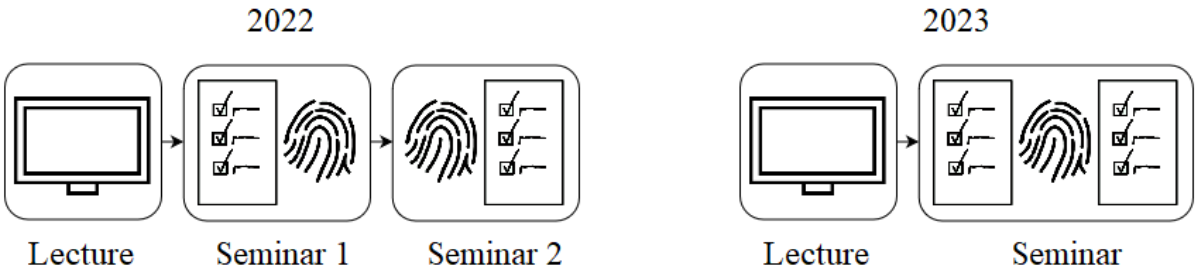
Source: futronic-tech.com

Sample

- Students of introductory IT security course
  - Spring 2022: 221 participants
  - Spring 2023: 149 participants
  - Spring 2024: only informal verification by 146 respondents

Study design

- Lecture
- Seminar 1
  - Questionnaire 1 → Theory → Creation an counterfeit from the photo → Applying glue into the mold
- Seminar 2
  - Peeling off the glue/silicone → Counterfeit processing → Questionnaire 2



Ethics

- No biometric data collected!
- Collected only self-reported data
  - E.g., opinions, experiences
- Participation purely voluntary
  - No advantages or disadvantages

Source: Sayeed, Md Shohel & Nasir, Ilham & Ong, Thian Song. (2016). An Efficient Multimodal Biometric Authentication Integrating Fingerprint and Face Features. American Journal of Applied Sciences. 13. 1221-1227. 10.3844/ajassp.2016.1221.1227

Agenda

- Lessons learned from an earlier project
- Fingerprint as the authentication method of choice
- Our fingerprint forgery workbench
- **Results of our effort**
- Limitations and resources

Results: counterfeit success

- NBIS
  - 19% → 76% of participants successful (58% in 2024)
- Unlocking smartphone
  - 1 (in 2022) → 4 (2023) → 7 (2024)
- Registering counterfeit into a smartphone
  - 26% → 11% → 16% of participants successful

Results: security perception

- Fingerprint authentication perceived as less secure after forgery simulation in the first run, but no change was observed in the second run
- Methods perception from the least to the most secure (measured only in the first run):

Swipe pattern
Face recognition
<
Fingerprint
PIN
<
Software token
Password
Hardware token

Results: perceived susceptibility

- The subjective perception of the risk of fingerprint attack
- Higher before the forgery simulation than after

Source: https://slate.com/technology/2019/08/how-criminals-might-use-stolen-fingerprints.html

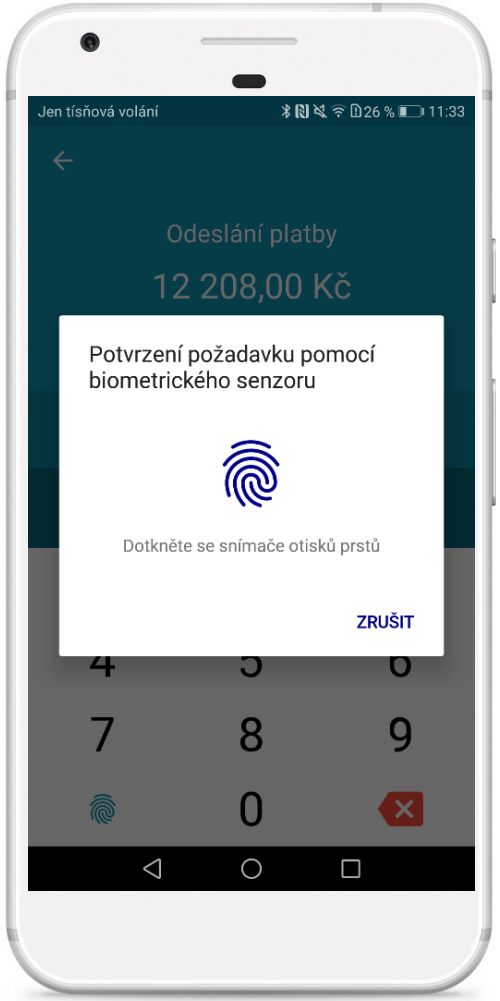
Results: forgery perception

- Fingerprint forgery perceived as
  - easier to learn
  - harder to perform (only in the first run)
  - attacker level as lower (only in the first run)

  after the simulation than before

Results: fingerprint authentication usage

- After simulation, willingness to use fingerprint authentication less often for:
  - Unlocking smartphone (only in the first run)
  - Login into mobile banking
  - Confirmation of transaction in mobile banking



Agenda

- Lessons learned from an earlier project
- Fingerprint as the authentication method of choice
- Our fingerprint forgery workbench
- Results of our effort
- **Limitations and resources**

Limitations

- Attacker and victim is the same person
  - Because of the ethics
  - But still very good simulation of real-life scenario
- Issues with photo quality
- Issues with size estimation in the first run

Resources

- Kruzikova, A., Di Campi, A., Cerny, T., Matyas, V. No Thumbs Up in Pictures! Experimental Fingerprint Forgery for Inexperienced Impostors. EEE ACCESS, 2024, vol. 12, No 131297.
- Kruzikova, A., Knapova, L., Smahel, D., Dedkova, L., Matyas, V. Usable and secure? User perception of four authentication methods for mobile banking, *Computers & Security*, Volume 115, 2022.
- Kružíková, A., Mužík, M. Knapová, L., Dědková, L., Šmahel, D., Matyáš, V. Two-Factor Authentication Time: How Time-Efficiency and Time-Satisfaction Are Associated with Perceived Security and Satisfaction., *Computers and Security*, Volume 138, 2024.

- Videos: (1) promotional/warning (YouTube) & (2) training the tutors

Summary

- Fingerprint first perceived as the most usable and secure method (of the four we tested).
- Students can make a reasonable counterfeit in ~ 60 mins.
- Mixed results about fingerprint security perception after forgery experience.

Thank you for your attention!

Article:

Video: