Swipe Your Fingerprints!

How Biometric Authentication Simplifies Payment, Access and Identity Fraud

Julian Fietkau, Starbug, Jean-Pierre Seifert
Security in Telecommunications - Technische Universität Berlin

Introduction

- A Norwegian tech company challenging the status quo of identification
- Build **smart cards** secured by your **fingerprint** instead of a secret PIN
- **Match-on-card Principle**: Fingerprint data stored and processed only on the card
- Already started to integrate their **Platform** into multiple Products

Access Control
(available)

Payment
(under test)

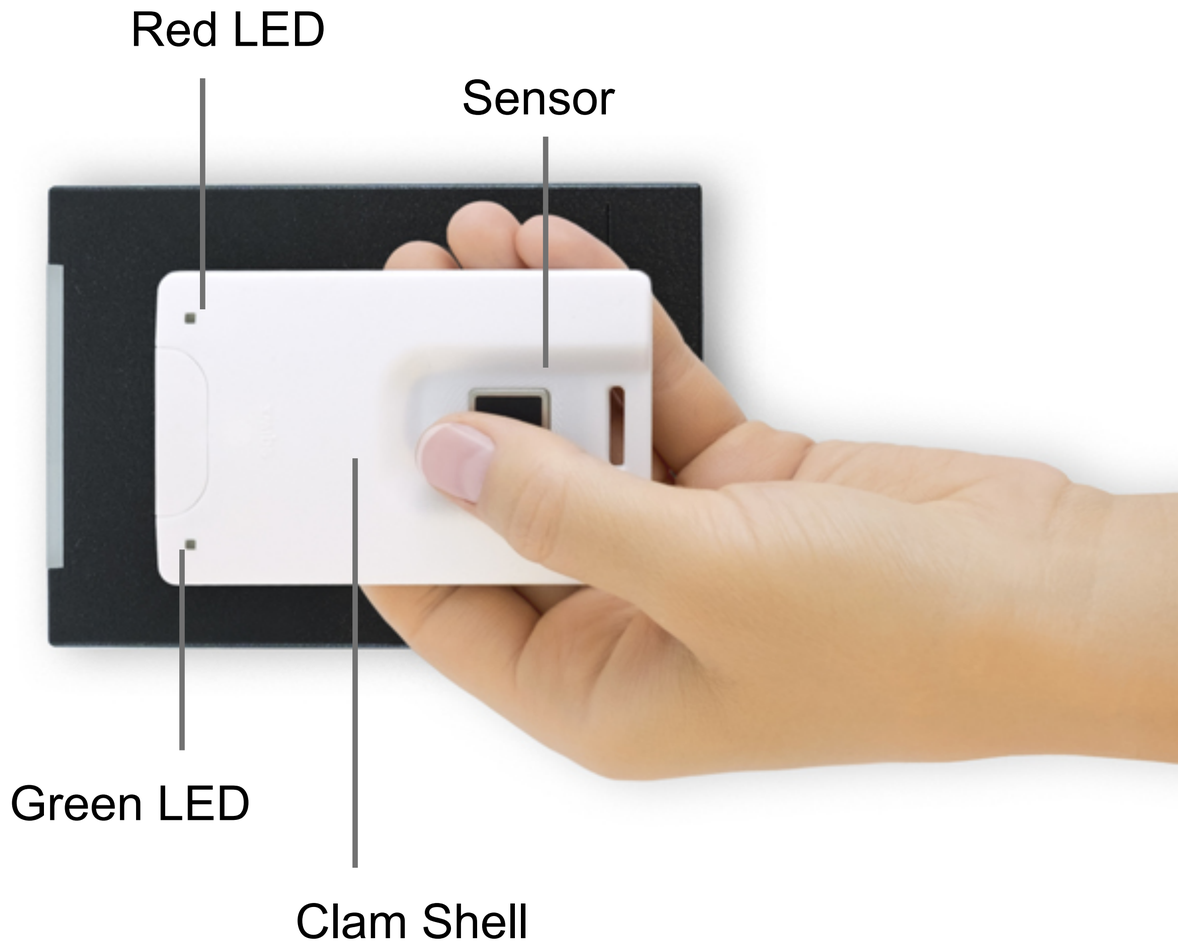
ID card
(not available)

Access Control Demo Kit

- Get it from the online-shop ~ $200
- Programmable NFC tag
- Match-on-card platform

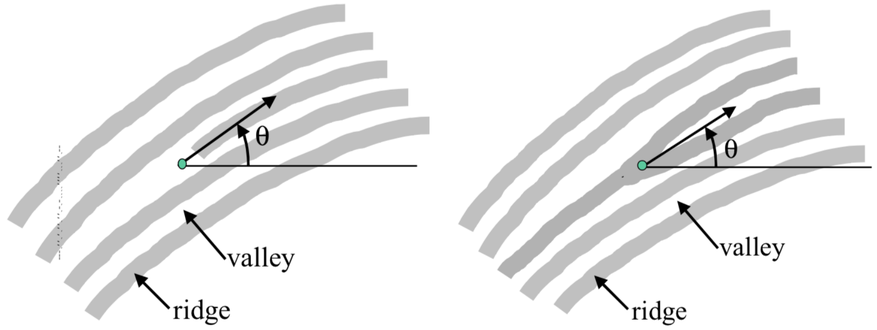
- Easy to use
- Much faster than PIN
- Nothing to remember

- **How secure is this?**



Introduction - How Fingerprint Authentication Works?

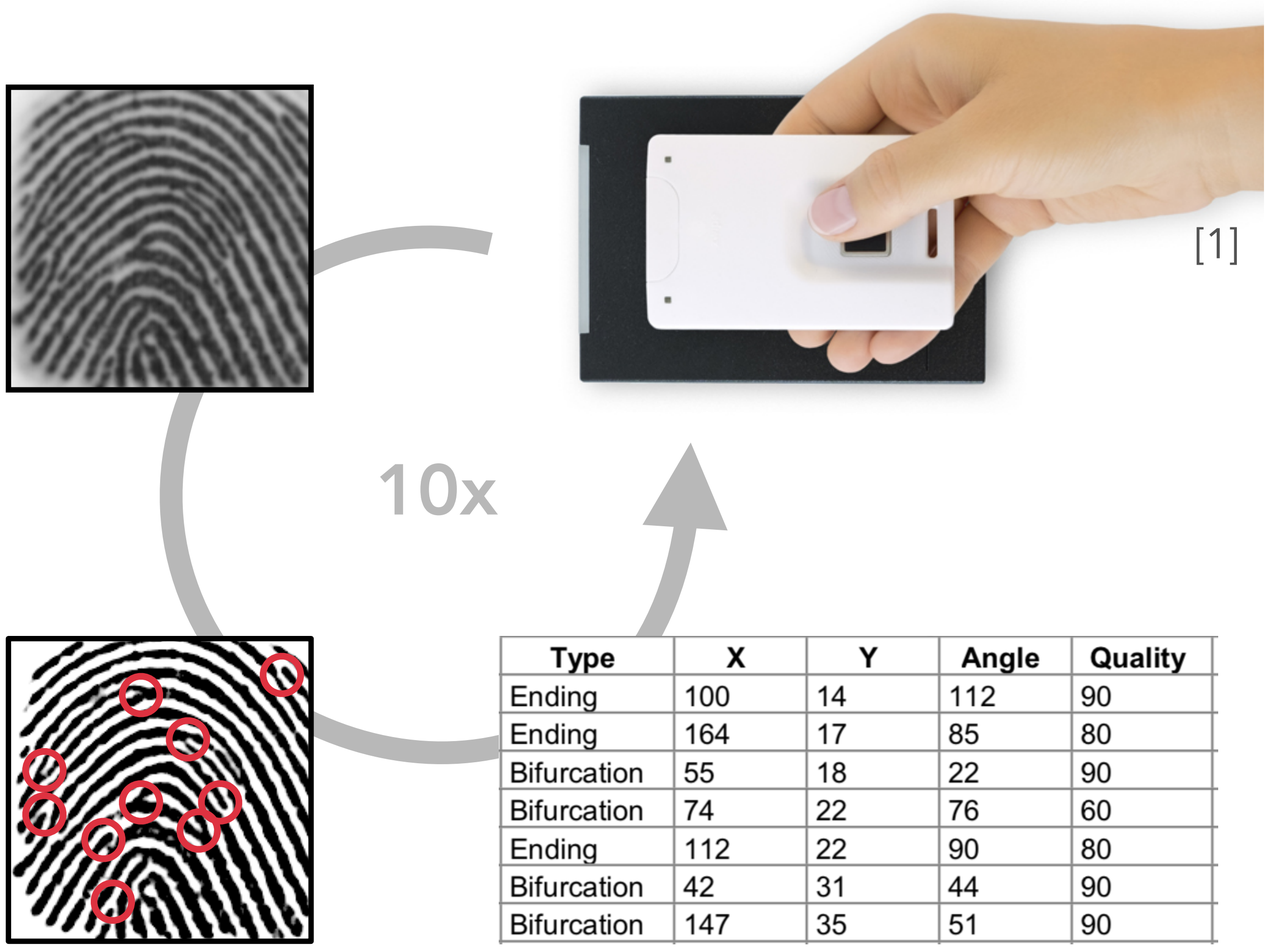
- Skin is formed by ridges and valleys
- **Unique for everyone** and hence can be used to identify a human
- **Minutiae-based Matching:** Special sections are called **minutiae** ridge end, ridge bifurcation, …



Introduction - Minutiae-based Matching

Enrollment

1. **Capture** the fingerprint
2. Preprocess and **identify minutiae**
3. Create a mathematical description "**biometric template**"
4. **Store it securely**
   - On the card or externally



[1]

Type	X	Y	Angle	Quality
Ending	100	14	112	90
Ending	164	17	85	80
Bifurcation	55	18	22	90
Bifurcation	74	22	76	60
Ending	112	22	90	80
Bifurcation	42	31	44	90
Bifurcation	147	35	51	90

Verification

1. Create a fresh template

2. **Compare fresh and stored one**
   - Complex pattern matching process, suffering from a lot of noise

Variations of the same finger:
Pressure, Rotation, Dryness, Cuts, …

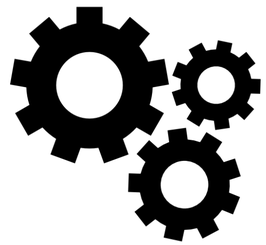
Similarities of different fingers:
Everyone has either loop, whorl or arch fingerprint (58.5%, 35%, 6.5%) [3]

Fresh Template

Type	X	Y	Angle	Quality
Ending	100	14	112	90
Ending	164	17	85	80
Bifurcation	55	18	22	90
Bifurcation	74	22	76	60
Ending	112	22	90	80

Stored Template

Type	X	Y	Angle	Quality
Ending	100	14	112	90
Ending	164	17	85	80
Bifurcation	55	18	22	90
Bifurcation	74	22	76	60
Ending	112	22	90	80
Bifurcation	42	31	44	90
Bifurcation	147	35	51	90



= 876
Similarity Score

Score >= Threshold ?

ACCEPT **or** **REJECT**

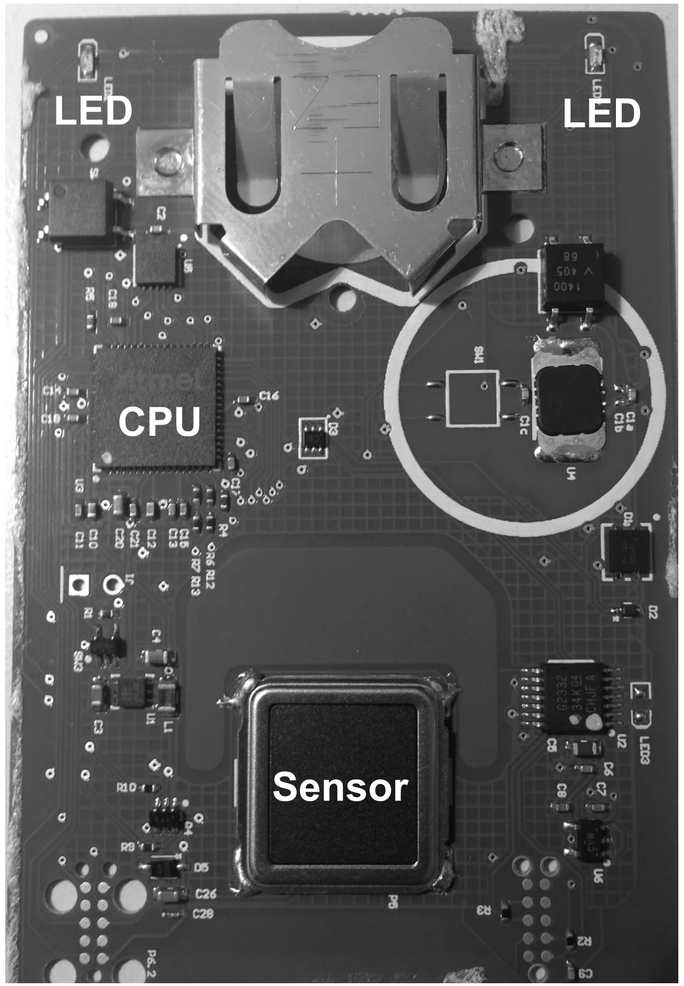
Analysis - Hardware

- Remove the cover
- Identify components
  - **CPU & Sensor**
  - NFC, Batterie, LEDs
- All components are connected with wires

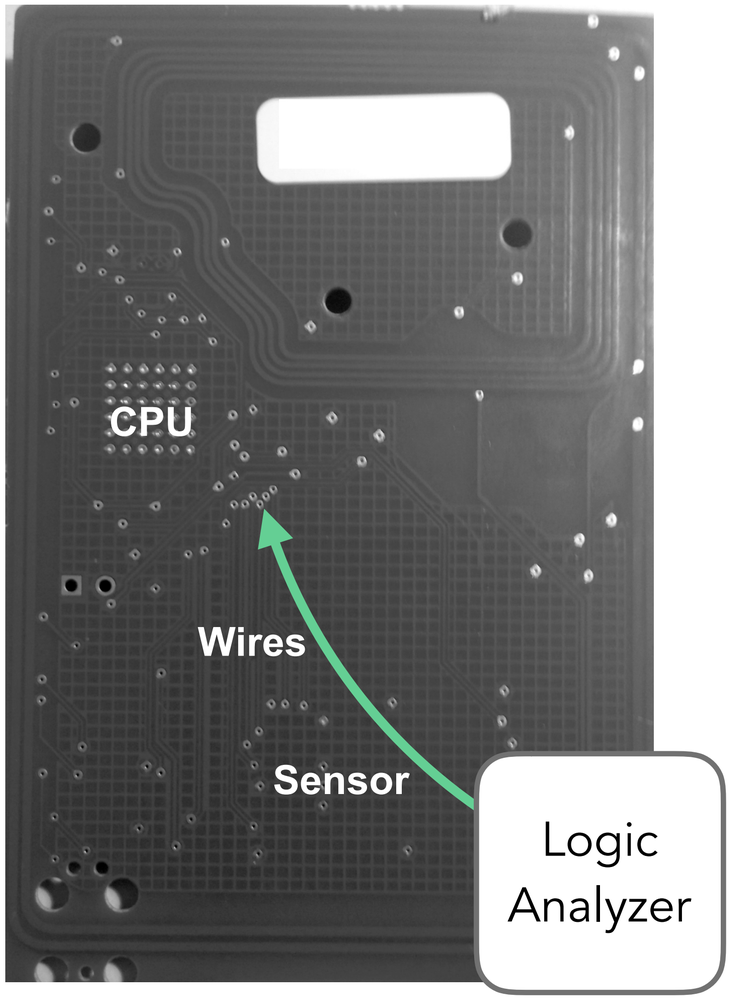
What do they send?

- Record the signals

Frontside



Backside



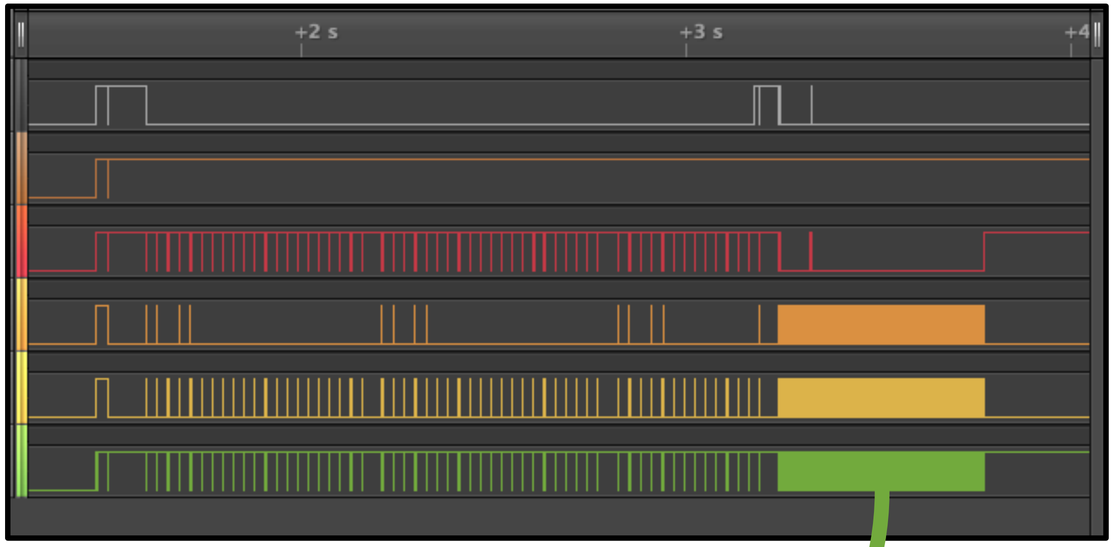
Analysis - Communication

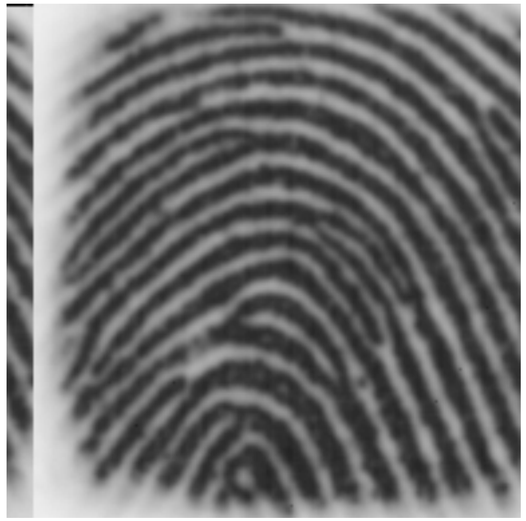
1. **Record of a valid authentication**

2. **Export payload**
   Serial Peripheral Interface (SPI)
   12 MHz clock, Mode 0
   CPU Master - Sensor Slave

3. **Visualise**
   Grayscale, each byte a pixel

- **Insecure on-device communication**

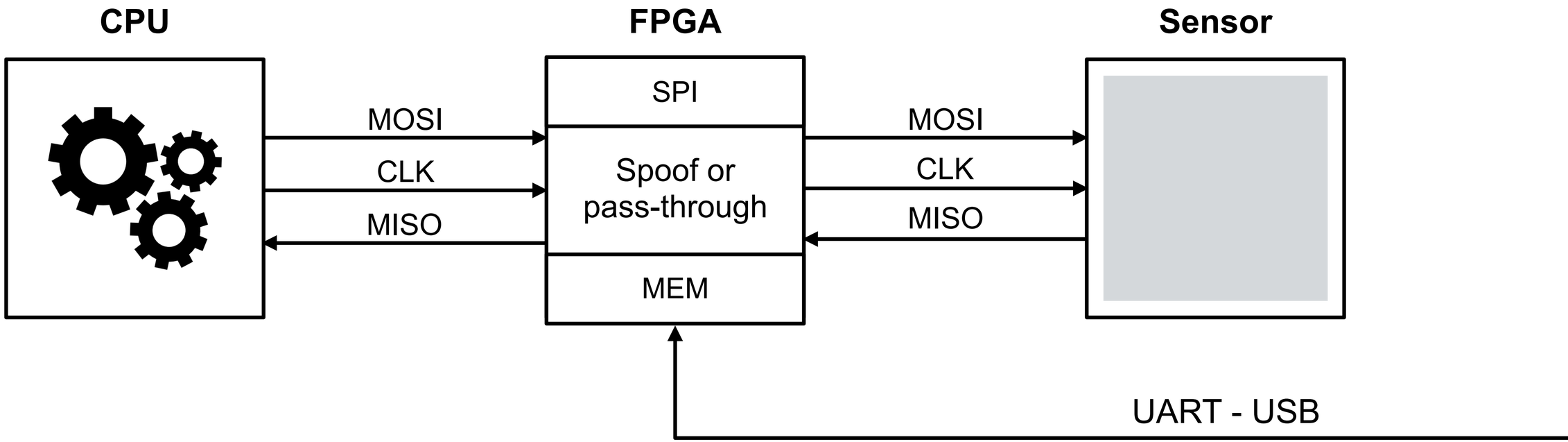




```
0002 0A00 0000 0A00
0808 0909 1212 1313
0055 4000 3F24 0000
0000 0000 5540 003F
2400 0200 0F1E 0003
0000 0000 0A01 ....
00FF 0000 0000 0A01
0000 000A 01.. ....
.... .... .... ....
```

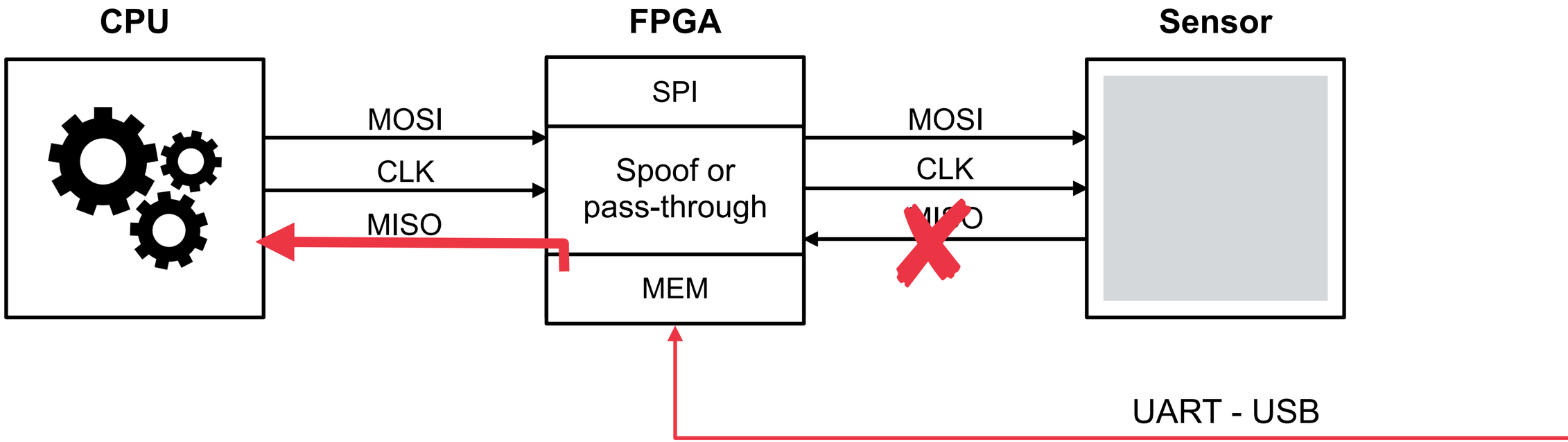
(Data send from the sensor)

Proof of Concept - Man in the Middle



- Cutting the wires and connect each end to an FPGA
- Create a Design to pass-through or modify the communication data
- **Spoof the device in various ways, while a real test person is enrolled**

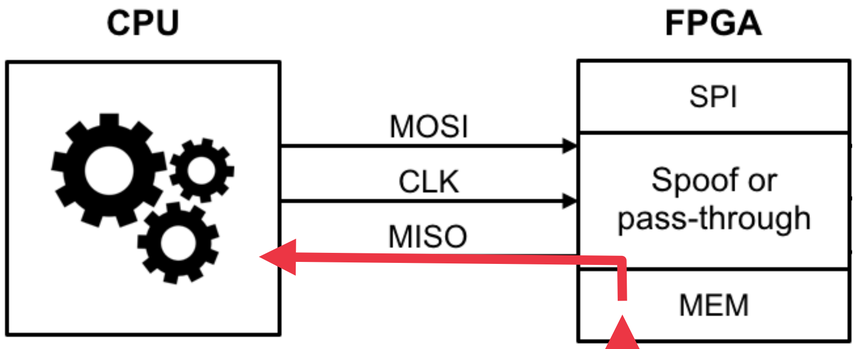
Replay a Valid Authentication



1. Load the valid authentication record in the FPGA memory
2. Activate the card: Dismiss any sensor data and inject the recorded data
   - **Accepted on first try, repeated multiple times**
   - No replay or livenesses detection in place, no tamper protection violated

Fuzzing the Payload!

- Reversing the protocol data and identify points of interest
- **Change values and replay:** Sensor version, image size, fuzz some random values
  → no relevant changes
- Change pre-images
  → still accepted
- **Create a tool to overwrite the full image send by the sensor.**

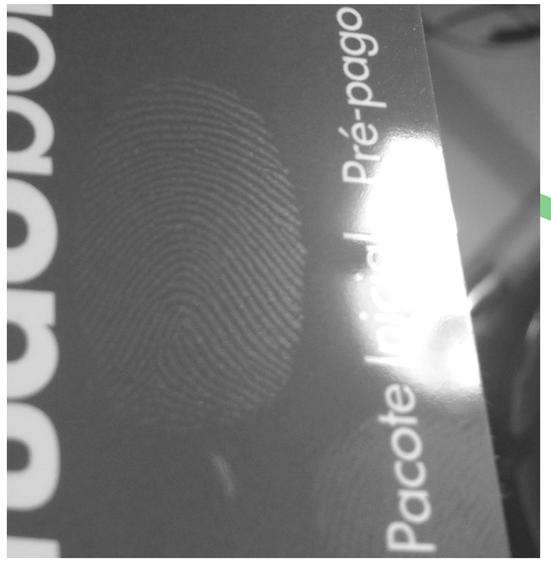


CPU Payload (MOSI)	Sensor Payload (MISO)	Description
FC00 006C 3390 3768	0002 0A00 0000 0A00	» Hardware ID - FPC1020A Sensor
3636 3636 3F3F 3F3F	0808 0909 1212 1313	
9C55 4000 3F24 8800	0055 4000 3F24 0000	» Some device configuration
0800 009C 5540 003F	0000 0000 5540 003F	
348C 32A8 0F1E 5C0B	2400 0200 0F1E 0003	
A00A 01A0 0A01	0000 0000 0A01	» Sleep 0.1448 seconds
1C00 241C 00A0 0A01	00FF 0000 0000 0A01	» Polling the sensor
1C00 A00A 01..	0000 000A 01..	Repeats until finger detected
....	....	
.... ..1C 00A0 0A01	.... ..00 8100 0A01	» Finger detected 0x81
5430 6060 081C 00C0	0000 C000 C000 8100	» Request image size 0xC0C0 = 192^2
1C00 C400 00..	0020 0000 AAA8 A59E	» Transmission of 12 subimages
.... 0000	 7870	8 bit x 8 bit x 12 times = 768 Bytes
5400 C000 C01C 00C0	0030 6060 0800 0000	
1C00 C01C 00C4 0000	0000 0000 2000 00F5	» Transmission of full image
0000 0000	F4F5 .... 9DA9	192 x 192 x 8 bit = 36864 Bytes
A00A 0100 0000 0000	000A 0100 0000 0000	» End of communication

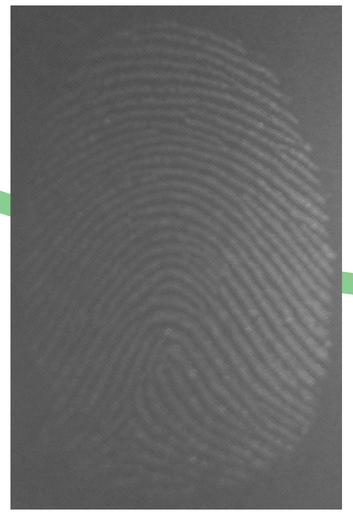
Vendor: “fingerprint data cannot be extracted from the card”

- Requested the test person **intentionally touched** a smart card surface
- Search for suitable fingerprint residues:
  - Use a light source and align the card by **90 degree**
  - Take pictures with standard **iPhone 5 camera**
- Created an extraction process to get a **digital dummy** we can inject.

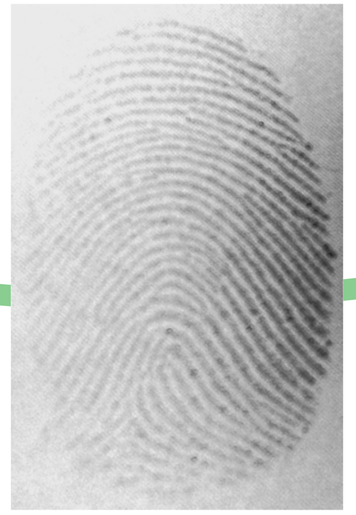
1. Identify and crop



2. Grayscale and color inversion



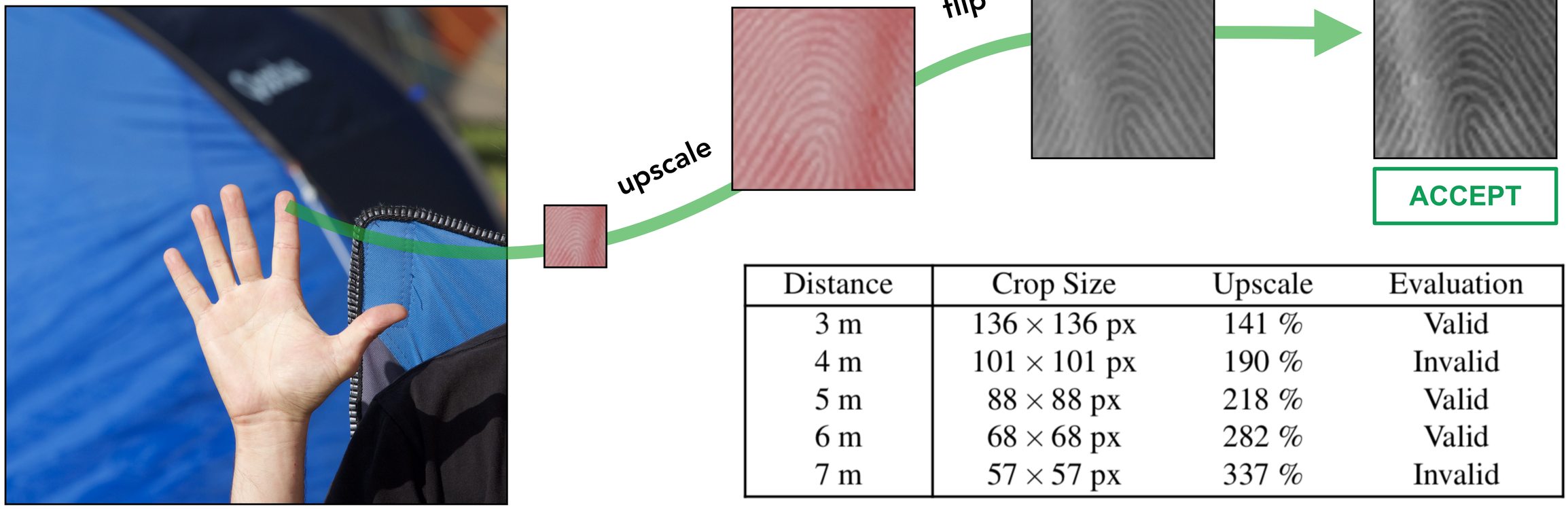
3. Scale to sensor size 11x11 mm



4. Improve brightness, contrast, gamma

Fingerprints on Digital Images

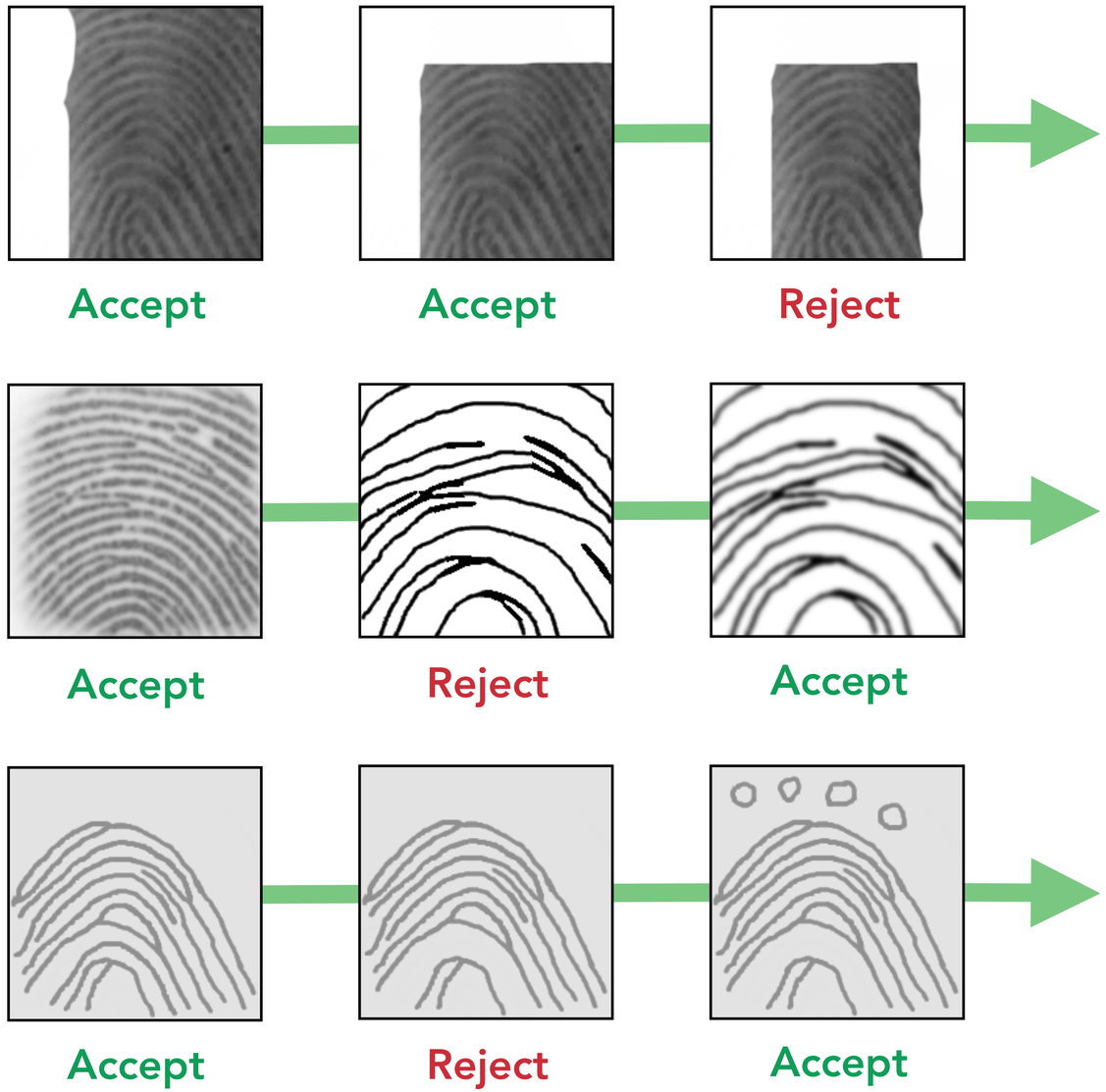
- Related work of Starbug [4]
- Canon EOS-D1 X 200mm lens, outdoor daylight
- Same extraction, but we need to flip and scale it.



Distance	Crop Size	Upscale	Evaluation
3 m	136 × 136 px	141 %	Valid
4 m	101 × 101 px	190 %	Invalid
5 m	88 × 88 px	218 %	Valid
6 m	68 × 68 px	282 %	Valid
7 m	57 × 57 px	337 %	Invalid

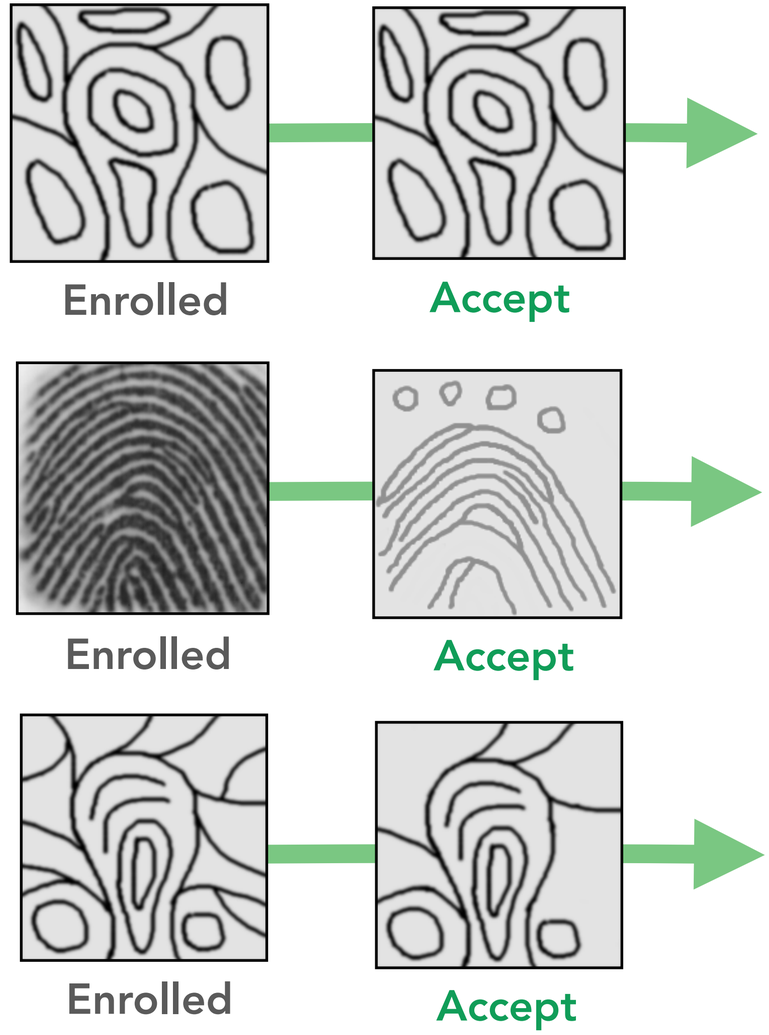
Algorithmic Weaknesses

- Access to in-depth functions of the card allows **black box analysis** of the **algorithm**
- **Proprietary fingerprint algorithm**
  - "Robust, fast & most power efficient one"
  - Patented in 2013
- **Corner Case Evaluation**
  - Missing 50% of a fingerprint is OK
  - Create minimal fingerprint to unlock
    - Ridges w/o minutiae can be removed or replaced with arbitrary ones
    - Apply blur filter for better dummies



Algorithmic Weaknesses

- **ISO/IEC 19794-2 Compliance**
  - Enrollment: minimum of **16** minutiae
    We enrolled and verified samples with **4**.
  - Verification: minimum of **12** minutiae
    We enrolled > 16 minutiae and reduce it to **9**.
  - Hard to measure with black box testing, but the examples show that the ISO requirements are already violated.

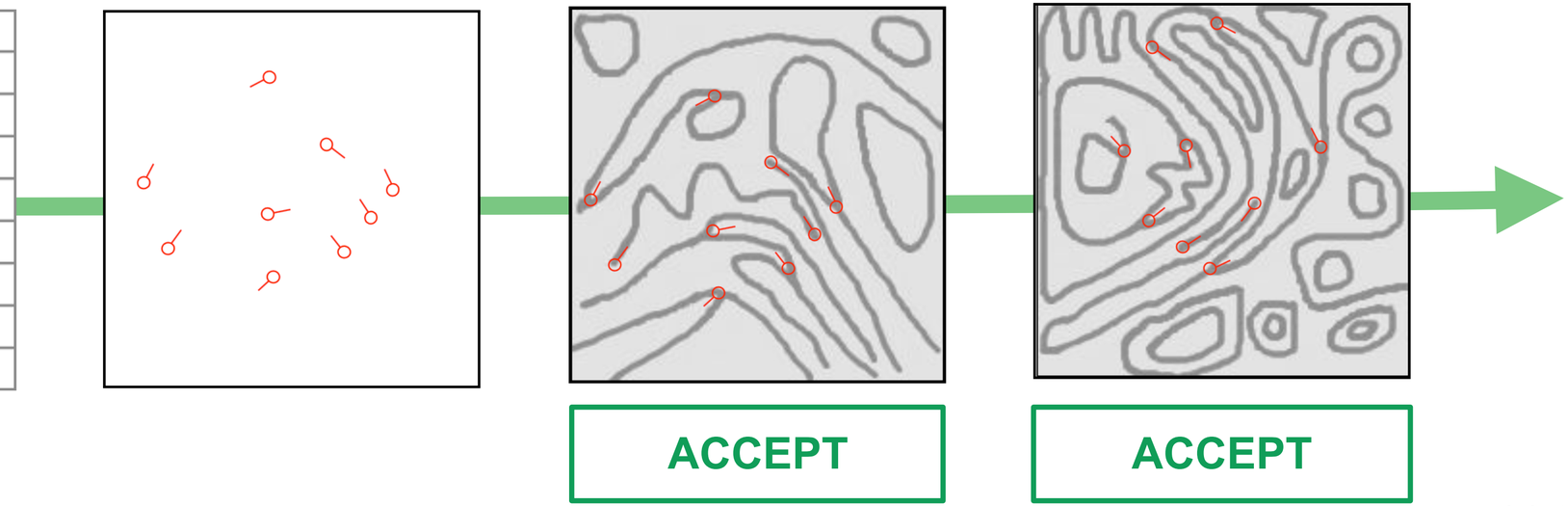


Known Template Attack

- Insecure memory technology, Software bugs, Side channel attacks, …
  - Template data can be leaked

- **Generate Fingerprints just from Template data?**
  - Take the "leaked" template of the enrolled user
  - Create clearly counterfeit fingerprints just from this data

Left Index Finger			
Type	**X**	**Y**	**Angle**
Ending	100	14	112
Ending	164	17	85
Bifurcation	55	18	22
Bifurcation	74	22	76
Ending	112	22	90
Bifurcation	42	31	44
Bifurcation	147	35	51



Conclusion

- Scrutinised a (state-of-the-art) device of a new **match-on-card platform**
  - **Weak matching algorithm** with badly chosen thresholds
  - **No** software and hardware **countermeasures** in place (only memory protection)

- This **match-on-card platform** can be easily attacked in 3/4 ways according to threat model [5]

1. **Use of dummies** - no liveness or replay detection
   Digital dummies vastly increases quality, ease of use and reusability
2. **Use of latent prints** - fingerprint residues are everywhere!
   Copy the fingerprints from the card or make a picture of the victim
3. **Use of biometric lookalikes** - Known template attack possible
   Even w/o the effort of creating natural-looking fingerprints (as considered by related work)

Conclusion

How to improve this and similar devices?

- **Use 3-factor authentication:** Card, Fingerprint and PIN (by default)
- **Choose strong thresholds** and decrease the false match rate, ISO/IEC 19794-2.
- **Apply replay and liveness detection:**
  - Rolling or fuzzy hashes of already-seen fingerprints. (related work)
  - Process multiple samples and integrate more sophisticated sensors.

- **Protect the on-device communication:** Encryption.
- **Hardware countermeasures:** Logic duplication, mesh detectors, …
- **Prevent side-channels:** Dummy instructions, side channel free algorithms, …

Conclusion

- Our research is always intended to **help people**, **improve systems** and **point out risks** to customers and stakeholders.

- Informed the company before publication
  - Requested to remove the name and all brands
  - "Payment and ID cards are fundamentally different"
  - "The analyzed card is discontinued"

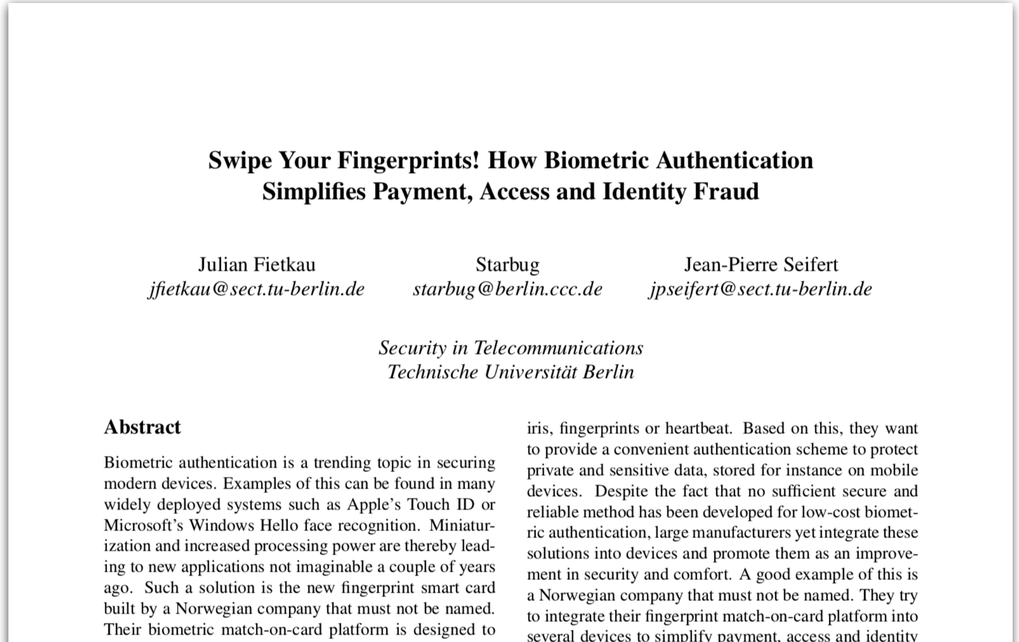
- Access Card Demo Kits are still available
- We don't know whether and how the "fundamental differences" impair the attacks on this or other devices

Conclusion

- Research Paper: "Swipe Your Fingerprints!"
  https://www.usenix.org/conference/woot18/presentation/fietkau

- Check out our GitHub-repo, tools and lots of test data!
  https://github.com/julieeen/swipe

- Questions and requests
  jfietkau@sect.tu-berlin.de
  starbug@berlin.ccc.de
  jpseifert@sect.tu-berlin.de



Swipe Your Fingerprints! How Biometric Authentication Simplifies Payment, Access and Identity Fraud

Julian Fietkau *jfietkau@sect.tu-berlin.de*
Starbug *starbug@berlin.ccc.de*
Jean-Pierre Seifert *jpseifert@sect.tu-berlin.de*

Security in Telecommunications
Technische Universität Berlin

Abstract

Biometric authentication is a trending topic in securing modern devices. Examples of this can be found in many widely deployed systems such as Apple's Touch ID or Microsoft's Windows Hello face recognition. Miniaturization and increased processing power are thereby leading to new applications not imaginable a couple of years ago. Such a solution is the new fingerprint smart card built by a Norwegian company that must not be named. Their biometric match-on-card platform is designed to

iris, fingerprints or heartbeat. Based on this, they want to provide a convenient authentication scheme to protect private and sensitive data, stored for instance on mobile devices. Despite the fact that no sufficient secure and reliable method has been developed for low-cost biometric authentication, large manufacturers yet integrate these solutions into devices and promote them as an improvement in security and comfort. A good example of this is a Norwegian company that must not be named. They try to integrate their fingerprint match-on-card platform into

References

[1] Product images from the Company Press Kit (anonymised)

[2] ISO/IEC 19794-2 standard

[3] The Fingerprints-World-Map

[4] Starbug, "Ich sehe, also bin ich ... du", Talk at 31C3, 2014.

[5] Dürmuth, Oswald, and Pastewka. "Side-Channel Attacks on Fingerprint Matching Algorithms"

[6] Cappelli, Raffaele, et al., "Fingerprint image reconstruction from standard templates.", IEEE transactions on pattern analysis and machine intelligence 29.9 (2007).

[7] Aditi Roy et al., "MasterPrint: Exploring the Vulnerability of Partial Fingerprint-Based Authentication Systems.", IEEE Transactions on Information Forensics and Security 12.9 (2017): 2013-2025.

[8] GitHub Repository

[9] Saleae, "The logic analyzer you'll love to use."

[10] Henniger, Scheuermann and Kniess. "On security evaluation of fingerprint recognition systems." International Biometric Performance Testing Conference (IBPC). 2010.

Related Work

- **Starbug, "Ich sehe, also bin ich ... du"** [4]
  Collect and physically clone the biometric features with fingerprint fuming
  Extracting fingerprints from touched objects or photos of the victim, e.g. German Politicians

- **Aditi Roy et al., "MasterPrint"** [6]
  Synthesize fingerprints based on similarities from huge fingerprint databases,
  to impersonate users with a given probability. Do not allow to target a specific person.
  No real authentication system was bypassed, The generated MasterPrints are not published

- **Known template attacks for minutiae-based matching algorithms** [7]
  Create sophisticated and natural-looking fingerprints only from the numerical template data
  Evaluated the approach against a number of undisclosed state-of-the-art algorithms