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

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

---

**Introduction**

- **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, …
**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
Introduction - Minutiae-based Matching

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]
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
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

(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.
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

[Diagram with steps 1 to 4]
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.

<table>
<thead>
<tr>
<th>Distance</th>
<th>Crop Size</th>
<th>Upscale</th>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>3 m</td>
<td>136 × 136 px</td>
<td>141 %</td>
<td>Valid</td>
</tr>
<tr>
<td>4 m</td>
<td>101 × 101 px</td>
<td>190 %</td>
<td>Invalid</td>
</tr>
<tr>
<td>5 m</td>
<td>88 × 88 px</td>
<td>218 %</td>
<td>Valid</td>
</tr>
<tr>
<td>6 m</td>
<td>68 × 68 px</td>
<td>282 %</td>
<td>Valid</td>
</tr>
<tr>
<td>7 m</td>
<td>57 × 57 px</td>
<td>337 %</td>
<td>Invalid</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Left Index Finger</th>
<th>Type</th>
<th>X</th>
<th>Y</th>
<th>Angle</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ending</td>
<td>100</td>
<td>14</td>
<td>112</td>
</tr>
<tr>
<td></td>
<td>Ending</td>
<td>164</td>
<td>17</td>
<td>85</td>
</tr>
<tr>
<td></td>
<td>Bifurcation</td>
<td>55</td>
<td>18</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Bifurcation</td>
<td>74</td>
<td>22</td>
<td>76</td>
</tr>
<tr>
<td></td>
<td>Ending</td>
<td>112</td>
<td>22</td>
<td>90</td>
</tr>
<tr>
<td></td>
<td>Bifurcation</td>
<td>42</td>
<td>31</td>
<td>44</td>
</tr>
<tr>
<td></td>
<td>Bifurcation</td>
<td>147</td>
<td>35</td>
<td>51</td>
</tr>
</tbody>
</table>
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, ...
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
References

[1] Product images from the Company Press Kit (anonymised)
[8] GitHub Repository
[9] Saleae, “The logic analyzer you’ll love to use.”
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