Indirect Attacks on Biometric Systems

Dr. Julian Fierrez
(with contributions from Dr. Javier Galbally)

Biometric Recognition Group - ATVS
Escuela Politécnica Superior
Universidad Autónoma de Madrid, SPAIN

Gjovik, Norway, March 2015

Outline

• Introduction: Security Perspective
• Introduction to Vulnerabilities in Biometrics: Indirect Attacks
• Case Studies:
  1. Brute-Force Attack with Synthetic Data (Signature & Iris)
  2. Stolen Template > Masquerade Indirect Attack (Finger)
  3. Matcher-Specific Hill-Climbing (Finger)
  4. Time-based Side-Channel Hill-Climbing (Finger)
  5. General/Advanced Hill-Climbing (Face) → Score Quantization CM
• A Note on Common Criteria
• Conclusions

1/73
Outline

• Introduction: Security Perspective
• Introduction to Vulnerabilities in Biometrics: Indirect Attacks
• Case Studies:
  1. Brute-Force Attack with Synthetic Data (Signature & Iris)
  2. Stolen Template > Masquerade Indirect Attack (Finger)
  3. Matcher-Specific Hill-Climbing (Finger)
  4. Time-based Side-Channel Hill-Climbing (Finger)
  5. Advanced Hill-Climbing (Face) → Score Quantization CM
• A Note on Common Criteria
• Conclusions

Security Evaluation in Biometrics

• FAQ when dealing with IT solutions for security applications:
  - How secure is this technology?
  - Why should I trust it?
  - Who assures the level of security offered by this system?
  - …
• Five observations from the state of the art:
  
  **Obs. 1**: other works try to answer: is this system vulnerable to this attack?, but not *HOW* vulnerable is it?
  
  **Obs. 2**: results are obtained without following a specific protocol (very difficult to compare)
  
  **Obs. 3**: different standards for security evaluation (CC, BEM, ISO 19792) → very general → need for supporting documents with examples, lists of threats...
  
  **Obs. 4**: constant need to search for new threats
  
  **Obs. 5**: need to develop countermeasures for the detected vulnerabilities

---

**Security Perspective**

• There are two ways of addressing the security problem:

  ![Diagram](image)

  **Security Through Obscurity**
  - Relies on secrecy (of design, implementation, protocols...) to provide security.
  - “Publicity helps attackers”

  **Security Through Transparency**
  - Relies on openness to provide security. Largely used in cryptography.
  - “The simpler and fewer the things that one needs to keep secret, the easier it is to maintain the security”

Let’s face the problems and find solutions for them (controlled risk), before somebody else finds the way to take advantage of our secrets (unpredictable consequences)
**Security Perspective**

Searching for new threats (can the system be broken using this attacking approach?), evaluating those vulnerabilities following a systematic and replicable protocol (how vulnerable is the system to this approach?), proposing new countermeasures that mitigate the effects of the attack, and publicly reporting the results of the whole process, help to develop a more mature and secure biometric technology.

**Outline**

- Introduction: Security Perspective

- *Introduction to Vulnerabilities in Biometrics: Indirect Attacks*

- Case Studies:
  1. Brute-Force Attack with Synthetic Data (Signature & Iris)
  2. Stolen Template > Masquerade Indirect Attack (Finger)
  3. Matcher-Specific Hill-Climbing (Finger)
  4. Time-based Side-Channel Hill-Climbing (Finger)
  5. Advanced Hill-Climbing (Face) \(\rightarrow\) Score Quantization CM

- A Note on Common Criteria

- Conclusions
**Attack Points in Biometrics**

- Possible points of attack to a biometric system.

**DIRECT ATTACKS**  
(Spoofing, mimicry)

1. Sensor
2. Feature extractor
3. Matcher
4. Database

**INDIRECT ATTACKS**  
(Trojan Horse, Hill Climbing, Brute Force, channel interception, replay attacks, ...)

5. Threshold
6.  
7. Database
8.  
9. Accept/Reject
10.  

---

**Security Evaluation of Biometric Systems**

- Proposed steps for security evaluation of biometric systems:
  1) Description of the attack
  2) Description of the biometric systems being evaluated
  3) Description of the information required to be known by the attacker
  4) Description of the database
  5) Description of the tests that will be performed
  6) Compute the performance (FAR and FRR curves) of the systems being evaluated → determine the operating points where they will be tested
  7) Execution of the vulnerability evaluation in the defined operating points: Success Rate (SR), and Efficiency (E

- Reporting the results
  - SR: percentage of accounts broken out of the total attacked
  - E
  - average number of attempts needed to break an account
Outline

• Introduction: Security Perspective
• Introduction to Vulnerabilities in Biometrics: Indirect Attacks
• Case Studies:
  1. Brute-Force Attack with Synthetic Data (Signature & Iris)
  2. Stolen Template > Masquerade Indirect Attack (Finger)
  3. Matcher-Specific Hill-Climbing (Finger)
  4. Time-based Side-Channel Hill-Climbing (Finger)
  5. Advanced Hill-Climbing (Face) → Score Quantization CM
• A Note on Common Criteria
• Conclusions

Brute-Force Attack with Synthetic Signatures

**Synthetic Generation of On-Line Signatures**

- We consider an on-line signature is defined by \([x, y, p]\).
- General system architecture:
**Synthetic Generation of On-Line Signatures**

- Examples of real and synthetic signatures:

**Database and Systems**

- ENROLL (performance eval.)
  - MCYT db: 330 users
  - 25 Real Signatures / user
  - x, y, p signals

- TEST (security eval.)
  - MCYT-Synth. db: 330 users
  - 25 Synth. Signatures / user
  - x, y, p signals

- 330 accounts attacked (5/20 training signatures)
- HMM-based system:
  - 4 states, 12 gaussians per state
  - EER ≈ 3.5%

### Results

- The system distinguishes better between real and synthetic signatures than in the case of considering only real signatures.
- The difference is lower when we take into account the pressure function \( \rightarrow \) pressure information is useful.
- The difference is higher for more training signatures.

<table>
<thead>
<tr>
<th>FAR real impostors (in %)</th>
<th>0.5</th>
<th>0.05</th>
<th>0.01</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No Pressure</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Tr.</td>
<td>0.04</td>
<td>0.001</td>
<td>NA</td>
</tr>
<tr>
<td>20 Tr.</td>
<td>0.02</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td><strong>Pressure</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 Tr.</td>
<td>0.1</td>
<td>0.006</td>
<td>0.001</td>
</tr>
<tr>
<td>20 Tr.</td>
<td>0.05</td>
<td>0.002</td>
<td>NA</td>
</tr>
</tbody>
</table>

**Brute-Force with Synthetic Data: Other Biometrics**

J. Galbally, A. Ross, M. Gomez-Barrero, J. Fierrez and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms", Comp. Vision and Image Under., Oct 2013 (Also in Elsevier Virtual Issue: Celebrating the Breadth of Biometrics Research; and featured in CNN, Wire, BBC, etc.)
Brute-Force with Synthetic Data: Other Biometrics

### Table: SR (%) - VeriEye

<table>
<thead>
<tr>
<th>FAR</th>
<th>SR(_{1a})</th>
<th>SR(_{1b})</th>
<th>SR(_{2a})</th>
<th>SR(_{2b})</th>
<th>SR(_{3})</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1%</td>
<td>81.2</td>
<td>66.7</td>
<td>96.2</td>
<td>92.8</td>
<td>96.7</td>
<td>86.7</td>
</tr>
<tr>
<td>0.05%</td>
<td>79.2</td>
<td>63.4</td>
<td>96.2</td>
<td>91.4</td>
<td>95.2</td>
<td>85.1</td>
</tr>
<tr>
<td>0.01%</td>
<td>77.3</td>
<td>60.9</td>
<td>95.2</td>
<td>90.9</td>
<td>93.8</td>
<td>83.6</td>
</tr>
<tr>
<td>0.0001%</td>
<td>69.0</td>
<td>49.1</td>
<td>92.8</td>
<td>82.8</td>
<td>82.9</td>
<td>75.3</td>
</tr>
</tbody>
</table>

- Unrealistically high security scenario $\rightarrow$ 75\% of breaking the system
- For the most likely attacking scenario $\rightarrow$ 92\% SR
- More than one reconstruction $\rightarrow$ 30\% SR increase

J. Galbally, A. Ross, M. Gomez-Barreto, J. Fierrez and J. Ortega-Garcia, "Iris image reconstruction from binary templates: An efficient probabilistic approach based on genetic algorithms", Comp. Vision and Image Under., Oct 2013 (Also in Elsevier Virtual Issue: Celebrating the Breadth of Biometrics Research; and featured in CNN, Wire, BBC, etc.)

### Outline

- Introduction: Security Perspective
- Introduction to Vulnerabilities in Biometrics: Indirect Attacks
- Case Studies:
  1. Brute-Force Attack with Synthetic Data (Signature & Iris)
  2. Stolen Template $>$ Masquerade Indirect Attack (Finger)
  3. Matcher-Specific Hill-Climbing (Finger)
  4. Time-based Side-Channel Hill-Climbing (Finger)
  5. Advanced Hill-Climbing (Face) $\rightarrow$ Score Quantization CM
- A Note on Common Criteria
- Conclusions
Direct & Indirect Masquerade Attacks Starting from an ISO Minutiae Template


INDIRECT ATTACK: Masquerade attack

Sensor

Feature extractor

Matcher

Threshold

Accept/Reject

Database
The Problem

- Attacks to biometric systems \(\rightarrow\) DIRECT / INDIRECT

- Direct attacks are easier to perform:
  - No information about the system is needed
  - Interaction with the system is done in a straightforward manner

WHAT IF AN INDIRECT ATTACK IS TRANSFORMED INTO A DIRECT ATTACK?

From a Minutiae Template to a Gummy Finger

DIRECT ATTACK (Spoofing)  INDIRECT ATTACK (Masquerade Attack)

- Gummy finger generation
- Reconstructed Image
- Stolen ISO Template
- Template Storage
- Accept/Reject

- Sensor
- Feature Extractor
- Matcher
- Computer
**Database and Systems**

**ENROLL** (performance eval.)
- FVC 2006 DB2
- 140 users / 12 samples

**TEST** (security eval.)
- 50 users
- Rec. Images + gummy fingers

- ISO Minutiae based system (proprietary)
  - EER=0.11% (computed with complete FVC 2006 DB2 - 140 users/12 samples)

**Results**

- RIASR → Reconstructed Images Attack Success Rate
- DASR → Direct Attack Success Rate

<table>
<thead>
<tr>
<th>Threshold</th>
<th>FAR</th>
<th>FRR</th>
<th>1-FRR</th>
<th>RIASR</th>
<th>DASR</th>
</tr>
</thead>
<tbody>
<tr>
<td>μ = 0.19</td>
<td>1%</td>
<td>0.08%</td>
<td>99.92%</td>
<td>100%</td>
<td>98%</td>
</tr>
<tr>
<td>μ = 0.21</td>
<td>0.1%</td>
<td>0.12%</td>
<td>99.88%</td>
<td>100%</td>
<td>96%</td>
</tr>
<tr>
<td>μ = 0.25</td>
<td>0%</td>
<td>0.17%</td>
<td>99.83%</td>
<td>100%</td>
<td>90%</td>
</tr>
<tr>
<td>μ = 0.30</td>
<td>0%</td>
<td>0.41%</td>
<td>99.59%</td>
<td>98%</td>
<td>78%</td>
</tr>
<tr>
<td>μ = 0.35</td>
<td>0%</td>
<td>1.03%</td>
<td>98.97%</td>
<td>92%</td>
<td>68%</td>
</tr>
<tr>
<td>μ = 0.40</td>
<td>0%</td>
<td>2.06%</td>
<td>97.94%</td>
<td>82%</td>
<td>50%</td>
</tr>
</tbody>
</table>

- Loss of performance between the indirect and direct attack → related to quality loss
- The system is still highly vulnerable to the direct attack: SR=50% for very high security point, SR=78% for more realistic op. point
- Standards are positive, BUT provide information to attackers → need for TEMPLATE PROTECTION
Outline

• Introduction: Security Perspective
• Introduction to Vulnerabilities in Biometrics: Indirect Attacks
• Case Studies:
  1. Brute-Force Attack with Synthetic Data (Signature & Iris)
  2. Stolen Template > Masquerade Indirect Attack (Finger)
  3. Matcher-Specific Hill-Climbing (Finger)
  4. Time-based Side-Channel Hill-Climbing (Finger)
  5. Advanced Hill-Climbing (Face) → Score Quantization CM
• A Note on Common Criteria
• Conclusions

Hill-Climbing Indirect Attacks to Fingerprint Systems

Milestones on Hill-Climbing Indirect Attacks

- **2001**: Attacks classification, by Ratha et al. *Proc. AVBPA*
- **2002**: First Hill-Climbing (HC) attack, by Soutar
- **2003**: HC attack to a face recognition system, by Adler
- **2004**: HC attack to a minutia-based system, by Uludag and Jain *Proc. SPIE*
- **2006**: HC attack to a minutia-based MoC system, by Martinez-Diaz et al. *Proc. IEEE ICSST*
- **2007**: HC attack to a signature verification system, by Galbally et al. *Proc. ICB*
Hill-Climbing Attacks

- Hill-climbing attacks send random templates to the matcher, which are iteratively adapted, based on the matching score, until the decision threshold is exceeded.

Reference System

- The NIST Fingerprint Image Recognition System (NFIS) is used as a reference system for our attacks.
- PC based system composed of several software modules.
- The following modules are used:
  - MINDTCT: minutiae extractor.
  - BOZORTH3: matcher.
Match-on-Card System

- The Match-on-Card (MoC) System under consideration is an operational implementation.
- The matcher is fully embedded in a smart-card.
  - The processing capacity of MoC systems is very limited.
  - It is accessed via a smart-card reader connected to a PC.
- The only information known from the system being attacked is: sensor image size, sensor resolution, minutiae storing format (ISO).

Database: MCYT

- A sub-corpus of the MCYT database is selected.
  - UareU Optical Sensor by Digital Persona.
  - Resolution of 500 dpi.
- Sub-corpus composed of 10 samples of both index fingers of 75 users: 1,500 samples, 150 accounts
- Samples are acquired with three different control levels.
Region-of-Interest

- The 2-D histogram of the minutiae of the sub-corpus is computed.
- A Region is heuristically defined, named Region-of-Interest (RoI), where most minutiae are located.

Performance of the NIFS2 and MoC Matchers
Experimental Protocol

- Attacks are based on the work by Uludag and Jain in 2004
- 100 initial synthetic random, 38-minutiae templates are sent to the matcher
- The template that attains the higher score is stored and iteratively modified by either:
  a) Changing an existing minutia by moving it to an adjacent cell or by changing its orientation.
  b) Adding a minutia
  c) Replacing a minutia
  d) Deleting a minutia from the template
- Only if the match score increases, in any of these iterations, the modified template is saved

Experimental Protocol

- The iterations end whenever the decision point is exceeded
- The following thresholds are set:
  - NFIS2
    - Threshold = 35
    - FAR = 0.10%
    - 1,000 average Brute-force attempts
  - MoC
    - Threshold = 55
    - FAR = 0.16%
    - 640 average Brute-force attempts
- The success rate of the attacks will be determined by the attacks that need fewer iterations than the attempts a brute-force attack would need
Example attacks: NRS2

Short attack

Score progression

Original minutiae

Original minutiae (black circles) vs. synthetic minutiae (grey triangles)

Unsuccessful attack

Example attacks: Match-on-Card

Short attack

Score progression

Original minutiae

Original minutiae (black circles) vs. synthetic minutiae (grey triangles)

Unsuccessful attack
Experimental Results

- Using the initial configuration, only 2/150 accounts are broken below 1,000 iterations (NFIS).
  - Generating minutiae only inside the ROI increases the success rate to 7/150 (NFIS).
- Deleting the low performing steps, a) and d), the success rate is increased to 40/150 broken accounts (NFIS).
- The biggest difference in behavior against attacks found between NFIS and MoC is with respect to the number of initial minutiae (maybe due to the limited capacity of the MoC matcher):
  - 38 leads to the maximum attack success rate for NFIS: 40/150
  - 25 leads to the maximum attack success rate for MoC: 123/150 (i.e., MoC is more vulnerable to attacks)

Outline

- Introduction: Security Perspective
- Introduction to Vulnerabilities in Biometrics: Indirect Attacks
- Case Studies:
  1. Brute-Force Attack with Synthetic Data (Signature & Iris)
  2. Stolen Template > Masquerade Indirect Attack (Finger)
  3. Matcher-Specific Hill-Climbing (Finger)

  4. Time-based Side-Channel Hill-Climbing (Finger)

  5. Advanced Hill-Climbing (Face) → Score Quantization CM
- A Note on Common Criteria
- Conclusions
Side-Channel Hill-Climbing Attack to Fingerprint Biometrics (Time Attack)


**INDIRECT ATTACK:** 
Time-based Side-Channel Hill-Climbing

1. Sensor
2. Feature extractor
3. Matcher
4. Database
5. Threshold
6. Accept/Reject
**Milestones Related to our Work**

**RELATED BIOMETRIC VULNERABILITIES**
- 2001: Attacks classification, by Ratha *et al.* (*AVBPA*)
- 2002: First HC attack, by Soutar
- 2005: HC attack to a minutia based system, by Uludag and Jain (*Proc. SPIE*)
- 2007: HC attack to an on-line signature system, by Galbally *et al.* (*ICB*)

**RELATED VULNERABILITIES ON CRYPTOGRAPHY**
- 1995: Timing attacks, by Kocher (*ICCAC*)
- 1999: Differential Power Analysis (DPA), by Kocher *et al.* (*Crypto*)

---

**Score vs Time**

- General diagram of a biometric system.

![Diagram of a biometric system]

- **Identity claim**
- **Database**
- **Feature Extractor**
- **Matcher**
- **Decision**
- **ACCEPT**
- **REJECT**

Why?

- **SCORE**: difficult to access
- **TIME**: easy to measure
**Possible Application: Hill-Climbing Attacks**

- General diagram of a hill-climbing attack.

**Reference System**

- The NIST Fingerprint Image Recognition System 2 (NFIS2) is used as a reference system in many research works.
- It's a PC based system composed of several software modules.
- The following modules are used:
  - MINDTCT: minutiae extractor.
  - BOZORTH3: matcher.
**Database: MCYT**

- **Performance Evaluation**: A sub-corpus of the MCYT database is selected (http://atvs.ii.uam.es/):
  - UareU Optical, Digital Persona, 500dpi.
  - Sub-corpus composed of 10 samples of both index fingers of 75 users: 1500 samples.
  - Samples are acquired with three different control levels.

- **Experiments**: 1 controled sample of the 75 users

---

**Results: Experiment 1**

- **EXPERIMENT 1**: Relation between Score and Time

  $S_T$

  $S_{min}$ $S_{max}$

  0% 10% 20% 30% 40% 50% 60% 70% 80% 90% 100%

  $t(s[0,10])$ vs $t(s[90,100])$

  $t(s[10,20])$ vs $t(s[80,90])$

  $t(s[40,50])$ vs $t(s[50,60])$
Results: Experiment 1

Results: Experiment 2

- **EXPERIMENT 2**: Relation between Score and Time variations
  - The original template is matched against itself (maximum score). The matching time is measured.
  - The template is iteratively modified by (one change at a time):
    a) **Changing** an existing minutia by moving it to an adjacent cell or by changing its orientation.
    b) **Adding** a minutia
    c) **Replacing** a minutia
    d) **Deleting** a minutia from the template
  - After each change the resulting template is matched against the original one. The matching time is measured.
  - The algorithm stops after 300 iterations (original and resulting template totally different \(\rightarrow\) very low matching score)
Results: Experiment 2

- Two areas can be distinguished:
  - A. Evolution of score and time are clearly correlated: a decrease in score implies a decrease in time
  - B. Score and time are independent

Conclusions

- The relation between score and matching time have been analyzed.
- A reference fingerprint system was used: NFIS2.
- Experiments are carried out on the publicly available database MCYT.
- Results show that matching time and score are not independent:
  - A higher score implies a higher matching time.
  - An increase in the score implies (on average) an increase on the matching time.
- This relation could be exploited to break the system (as has been done in cryptography with the timing attacks).
Outline

- Introduction: Security Perspective
- Introduction to Vulnerabilities in Biometrics: Indirect Attacks
- Case Studies:
  1. Brute-Force Attack with Synthetic Data (Signature & Iris)
  2. Stolen Template > Masquerade Indirect Attack (Finger)
  3. Matcher-Specific Hill-Climbing (Finger)
  4. Time-based Side-Channel Hill-Climbing (Finger)

  5. General/ Advanced Hill-Climbing (Face) → Score Quantization

- A Note on Common Criteria
- Conclusions

Bayesian Hill-Climbing Attack

**INDIRECT ATTACK:**
General/Advanced Hill-Climbing

- Sensor
- Feature extractor
- Matcher
- Threshold
- Database
- Accept/Reject

**Hill-Climbing Attack Based on Bayesian Adaptation**

- General diagram of a hill-climbing attack.
Hill-Climbing Attack Based on Bayesian Adaptation

- Bayesian hill-climbing algorithm.

\[
G = A \quad \text{and} \quad \alpha = 1 - \frac{1}{N}
\]

\[
\mu_A = \alpha \mu_L + (1 - \alpha) \mu_G
\]

\[
\sigma_A^2 = \alpha (\sigma_L^2 + \mu_L^2) + (1 - \alpha) (\sigma_G^2 + \mu_G^2) - \mu_A^2
\]

Reynolds et al. [DSP2000]

Database and Systems

- XM2VTS db: 295 users
- 4 sessions
- 2 samples per session

- 200 accounts attacked (4 training images)
- Eigenface-based system (91 dim \(\rightarrow\) 80% variance). EER=4.7%
- DCT-based system (GMM 512 gaussians). EER=1.2%

Turk and Pentland [ICCVPR1991]

Cardinaux, Sanderson, et al. [AVBPA2003]
Results

• For the best attack configuration (N=25, M=5, \(\alpha=0.5\)) the performance in other operation points is analyzed

<table>
<thead>
<tr>
<th>Operating points (in %)</th>
<th>FAR=0.1</th>
<th>FAR=0.05</th>
<th>FAR=0.01</th>
</tr>
</thead>
<tbody>
<tr>
<td>FRR=25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Success Rate (in %)</td>
<td>99.0</td>
<td>98.5</td>
<td>86.0</td>
</tr>
<tr>
<td>(n_{comp})</td>
<td>840</td>
<td>1,068</td>
<td>4,492</td>
</tr>
<tr>
<td>(n_{bf})</td>
<td>1,000</td>
<td>2,000</td>
<td>10,000</td>
</tr>
</tbody>
</table>

• For smaller FA \(\rightarrow\) bigger average number of comparisons and worse success rate.
• Always better efficiency than a BF attack

Eingenface+distance system

DCT+GMM system

Attack Example

• Example of a successful attack
Other Hill-Climbing Approaches

- Hill climbing based on the uphill simplex algorithm.

Stopping criteria:
- One of the points of the simplex is close enough => success
- Maximum number of iterations allowed reached => failure


Attack Protection Using Score Quantization
Results

- **Score Quantization** → increase the quantization step of the score so that the HC attack cannot take advantage of small increases in the score.
- Should not change the system performance → maximum step

<table>
<thead>
<tr>
<th></th>
<th>Eingenface-Based system</th>
<th>GMM-Based system</th>
</tr>
</thead>
<tbody>
<tr>
<td>QS</td>
<td>10(^{-6}) 10(^{-3}) 10(^{-1})</td>
<td>10(^{-4}) 10(^{-1}) 2.5 (\times) 10(^{-1})</td>
</tr>
<tr>
<td>SR</td>
<td>86 84.5 16.5</td>
<td>100 99.5 81</td>
</tr>
<tr>
<td>(E_{ff})</td>
<td>4.492 4.697 20.918</td>
<td>3.016 3.155 5.218</td>
</tr>
</tbody>
</table>

- SR and Eff decrease in both cases.
- More efficient for the PCA-based system.
- Not enough, other countermeasures should be studied.

Outline

- Introduction: Security Perspective
- Introduction to Vulnerabilities in Biometrics: Indirect Attacks
- Case Studies:
  1. Brute-Force Attack with Synthetic Data (Signature & Iris)
  2. Stolen Template > Masquerade Indirect Attack (Finger)
  3. Matcher-Specific Hill-Climbing (Finger)
  4. Time-based Side-Channel Hill-Climbing (Finger)
  5. Advanced Hill-Climbing (Face) → Score Quantization CM

- A Note on Common Criteria
- Conclusions
### Attack Potential

<table>
<thead>
<tr>
<th>Rating</th>
<th>Resistance level</th>
<th>Compatible with</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 20</td>
<td>No rating</td>
<td>None</td>
</tr>
<tr>
<td>20-27</td>
<td>Basic</td>
<td>AVA_VAN.2</td>
</tr>
<tr>
<td>28-34</td>
<td>Enhanced basic</td>
<td>AVA_VAN.3</td>
</tr>
<tr>
<td>35-42</td>
<td>Moderate</td>
<td>AVA_VAN.4</td>
</tr>
<tr>
<td>&gt;= 42</td>
<td>High</td>
<td>AVA_VAN.5</td>
</tr>
</tbody>
</table>

Table identical to the CEM one

Specific level definition

---

#### Table of Contents

1. INTRODUCTION
   1.1. Motivation
   1.2. Attack Potential and CEM-based model
   1.3. Attack Information Source
   1.4. Usage of this Document

2. ATTACK METHODS
   2.1. Direct Attack
   2.2. Conclusion

3.1. Description of the attack
   3.1.1. Effect of the attack
   3.1.2. Impact on TOE

---

### Attack Potential

<table>
<thead>
<tr>
<th>Factor</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed Time</td>
<td></td>
</tr>
<tr>
<td>&lt;= one day</td>
<td>0</td>
</tr>
<tr>
<td>&lt;= one week</td>
<td>1</td>
</tr>
<tr>
<td>&lt;= two weeks</td>
<td>2</td>
</tr>
<tr>
<td>&lt;= one month</td>
<td>4</td>
</tr>
<tr>
<td>&lt;= two months</td>
<td>7</td>
</tr>
<tr>
<td>&lt;= three months</td>
<td>10</td>
</tr>
<tr>
<td>&lt;= four months</td>
<td>12</td>
</tr>
<tr>
<td>&lt;= five months</td>
<td>15</td>
</tr>
<tr>
<td>&lt;= six months</td>
<td>17</td>
</tr>
<tr>
<td>&gt;= six months</td>
<td>19</td>
</tr>
<tr>
<td>Expert</td>
<td>6</td>
</tr>
<tr>
<td>Layman</td>
<td>0</td>
</tr>
<tr>
<td>Proficient</td>
<td>2</td>
</tr>
<tr>
<td>Knowledge of TOE</td>
<td>8</td>
</tr>
<tr>
<td>Public</td>
<td>0</td>
</tr>
<tr>
<td>Restricted</td>
<td>3</td>
</tr>
<tr>
<td>Sensitive</td>
<td>7</td>
</tr>
<tr>
<td>Critical</td>
<td>11</td>
</tr>
<tr>
<td>Window of Opportunity</td>
<td></td>
</tr>
<tr>
<td>Unnecessary/unlimited access</td>
<td>0</td>
</tr>
<tr>
<td>Easy</td>
<td>1</td>
</tr>
<tr>
<td>Moderate</td>
<td>4</td>
</tr>
<tr>
<td>Difficult</td>
<td>10</td>
</tr>
<tr>
<td>None</td>
<td>+60</td>
</tr>
<tr>
<td>Equipment</td>
<td></td>
</tr>
<tr>
<td>Standard</td>
<td>0</td>
</tr>
<tr>
<td>Specialised</td>
<td>4+10</td>
</tr>
<tr>
<td>Basic</td>
<td>7</td>
</tr>
<tr>
<td>Multiple basic</td>
<td>9</td>
</tr>
</tbody>
</table>

Specific level definition
Outline

• Introduction: Security Perspective
• Introduction to Vulnerabilities in Biometrics: Indirect Attacks
• Case Studies:
  1. Brute-Force Attack with Synthetic Data (Signature & Iris)
  2. Stolen Template > Masquerade Indirect Attack (Finger)
  3. Matcher-Specific Hill-Climbing (Finger)
  4. Time-based Side-Channel Hill-Climbing (Finger)
  5. Advanced Hill-Climbing (Face) → Score Quantization CM
• A Note on Common Criteria
• Conclusions

Conclusions

• Security through transparency: need for security vulnerability assessment
• Indirect Attacks:
  • [NO INFO] > Brute-Force (Synthetic Data): Low SRs
  • [STOLEN TEMPLATE] > Masquerade: Very-High SRs
  • [MATCH SCORE] > Matcher-specific HC: Med-High SRs
  • [SIDE-CHANNEL - TIME] > HC: Med SRs
  • [MATCH SCORE] > General/Advanced HC: Med-High SRs
    Score Quantization as a CM: Useful, but not definitive
• Relation with Common Criteria
Indirect Attacks on Biometric Systems

Dr. Julian Fierrez
(with contributions from Dr. Javier Galbally)

Biometric Recognition Group - ATVS
Escuela Politécnica Superior
Universidad Autónoma de Madrid, SPAIN

Gjovik, Norway, March 2015