



Evaluating Attack Resistance Levels of Biometric Systems

Tony Mansfield
National Physical Laboratory, UK

IBPC 7 March 2012

Outline

- 1. Rationale/Scope/Terminology**
- 2. NPL / CPNI evaluation of biometric terminals for automated access control**
- 3. Attack levels of the CPNI Grading System, with examples**
- 4. General findings on attack resistance of biometric systems from th NPL / CPNI evaluation**
- 5. Issues in evaluating attack resistance**

Rationale

Quotes on the web

- *We claim that we can fake every sensor ...*
- *Fingerprints in particular are laughably easy to spoof....*

But ...

- Are some systems harder to spoof than others
 - e.g. systems with fake finger detection
- Are biometrics easier to spoof than other components of your system?
- Are these attacks relevant for your use case?

Measures of attack resistance are needed that

- Distinguish between good and poor attack resistance
 - Broad equivalence of metrics over different biometric technologies
- Relate attack resistance to the use case & risk assessment
 - Commensurate with security levels of other system components

Terminology

Attack

- This talk focuses on attacks at the sensor / terminal, including:
 - Artefact
 - Tamper
 - Bypass

Level of an attack

- Difficulty or level of sophistication of the attack

System resistant to an attack

- $\text{Prob}[\text{Attack Succeeds}]$ is sufficiently low
- $\text{Prob}[\text{Attack detected \& alerted}]$ is sufficiently high

Level of attack resistance

- Attack resistance at level n implies the system is resistant to attacks at level n or lower.

CPNI Classification for Security Products



Guidance, standards & evaluation for ...

- Automated access control
- Intruder detection
- Barriers
- ...
- Biometrics used in access control

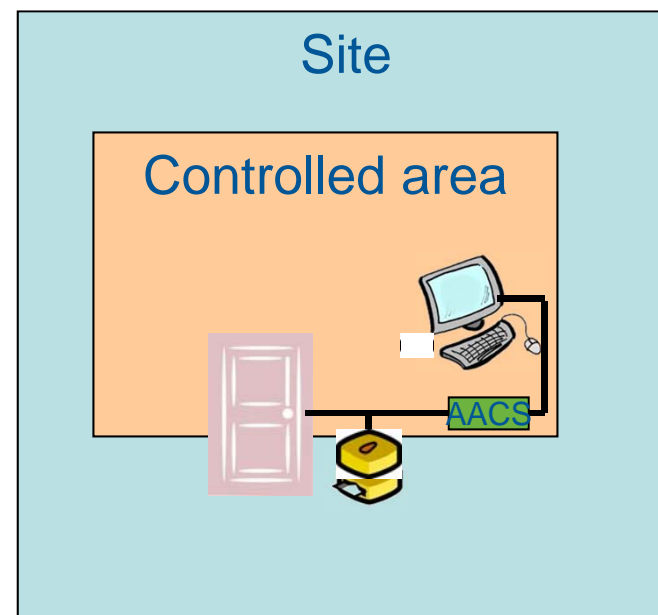
CPNI/NPL Evaluation of Biometric Authentication for Automated Access Control Systems (AACCS)

Use case

- Access to controlled area within site
- Biometrics as 2nd authentication factor
 - combined with prox card
 - independent of prox card
- Trusted administration staff
 - Attacker must impersonate a properly enrolled identity

Evaluation

- Evaluate biometric subsystem only
 - Security of dependent AACCS system evaluated separately
 - Assure security at the same level as the rest of the AACCS



CPNI Evaluation Standard for Biometric Access Control

1. Security-related functionality

- Admin & operator access: (i) *Authenticated* (ii) *NOT at terminal*
- Reference storage: (i) *NOT in device at portal* (ii) *NOT on card*
- Communications with AACS: (i) *Protected* (ii) *Alert on tamper, spoof*
- Check on installation

2. Biometric performance requirements

- $FAR < 0.1\%$ & requirements on *FRR, FTE, Transaction times*
- Scenario test

3. Attack resistance

- CPNI Grading depends on level of attack resistance
 - Spoofing
 - Tamper
 - ...
- Practical assessment

Testing Attack Resistance

Variety of types of attack

- Zero-effort impostor – e.g. targeting lookalike
- Fake finger, fake iris, ...
- Tamper
 - Remove from wall, Connect attacker's PC to terminal or AACS
- Exploiting poor quality enrolment, ...

Attack assumptions for the evaluation (based on use case)

- Attacker has obtained possession of a user's prox card
- User is known and accessible to acquire a biometric image
- Attacks to be made at same security settings as used in determining verification performance

Attack resistance

- System considered resistant to an attack if $< 5\%$ of attacks of that type succeed



Attack Levels of CPNI Grading System

Skill & knowledge level		Resource level		
		Low	Medium	High
		Domestic / High Street	Trade / Specialist	Bespoke
Low	None	1	2	3
Medium	Knowledge of Product / Techniques	2	4	5
High	Expert	3	5	6

CPNI Grading System

Attack Level	Protection System
1	Base
2	
3	Enhanced
4	
5	High
6	

Example Attack Levels: Fake Fingerprint

	Home / High St. resources	Trade / specialist supplier	Bespoke resource
Novice No special knowledge/skill	 1	 2	 3
Knows product & techniques	2	 4	5
Expert	3	5	6




Knowledge and Resource Requirements to Fake Fingerprints

Step	Resource	Knowledge/Skill
Acquire fingerprint image		
<i>Latent print</i>	Low	Med
<i>Fingerprint scanner</i>	Med	Low
<i>Generate from template</i>		High
Make mould		
<i>Direct impression</i>	Low-Med	Low
<i>Engrave / etch from image</i>	High	Low
	Med	Med
Make fingerprint artefact		
	Depends on material	Depends on mould
Present artefact at terminal		
<i>Without practice</i>		Low
<i>With practice & knowledge of device</i>		Med-High

Knowledge and Resource Requirements to Fake Iris

Step	Resource	Knowledge/Skill
Acquire iris image		
<i>Camera phone / SLR</i>	Low	Low
<i>Iris camera</i>	Med	Low
<i>Generate from iriscodes</i>		High
<i>Image enhancement/selection</i>		Med - High
Reproduce iris image		
<i>Print</i>	Low	Low
<i>Film</i>	Low	Med
<i>Contact Lens / Glass eye</i>	High	High
Present fake eye(s) at terminal		
<i>Without practice</i>		Low
<i>With practice & knowledge of device</i>		Med ..

Example attack levels: Fake iris

	Home / High St. resources	Trade / specialist supplier	Bespoke resource
<p>Novice No special knowledge/skill</p>			3
<p>Knows product & techniques</p>			5
<p>Expert</p>	3	5	 <p>6</p>

General Findings: Liveness / Artefact Detection

Different methods of preventing use of fakes

- “Liveness/non-artefact” properties required to enable image capture
- Built in sensor measures properties associated with real characteristic
- Algorithmic processing of captured images

Choosing the setting for fake detection

- If enabled: Level of attack resistance generally higher
- Stricter settings: Reduced chance of successful attack (but not to 0)
Can also significantly increase FRR

Successful attacks at level 3 & 4 (fingerprint)

- Finding “right” material for device – catastrophe: all attacks succeed
- Tuning of methods – attack success rate increases with experience
 - Sometimes indirect signal that a fake is detected

Our use case eliminates some of the easier spoofing attacks

- E.g. recognition against an enrolled artefact

General Findings: Security Functionality & Tamper Protection

Many biometric terminals provide configuration options which would render the system less secure

- Door relay on device
- Templates stored on device – on removable media
- Admin controls on device at portal for enrolment / disable spoof-detection

Better tamper protection often needed

Knowledge of product/techniques:

- Available on the internet (for the medium level attacker)
 - Tutorials on basic fake fingerprint attacks
 - Manuals for several biometric systems with details of e.g.:
 - tamper switch location
 - default passwords
 - Software for some systems

Issues in Evaluating Attack Levels

Sufficient coverage of types of attack at each level?

- Determined by expert review (incl. CPNI & Test Organisation)
- Difficulty to thoroughly test new/novel biometric modalities

Limits to what can be tested through real use:

- No skin transplants, or severed fingers in our evaluation
- Skill level of test personnel quickly increases from novice level as more attacks are made

Attacks get easier over time – need to review levels regularly

- New vulnerabilities are found
- Expert knowledge becomes available on internet
- Black market in helping people spoof systems
- Ways to exploit legitimate services e.g.
 - Mingpao Daily journalist successfully spoofed a biometrics device of the Hong Kong-China self-service immigration clearance channel with fingerprint produced by a HK\$110 [fingerprint cast kit](#) bought on Taobao,

Your Questions & Comments

Contact details for offline comment & questions

- Tony.Mansfield@NPL.CO.UK