On security evaluation of fingerprint recognition systems

Olaf Henniger, Dirk Scheuermann, and Thomas Kniess
Fraunhofer Institute for Secure Information Technology
Darmstadt, Germany

Fraunhofer
SIT

Outline

- Motivation
- Potential vulnerabilities specific to fingerprint verification systems
- Assessment of attack potentials
  - For using a fingerprint dummy
  - For zero-effort attacks
- Summary

Motivation

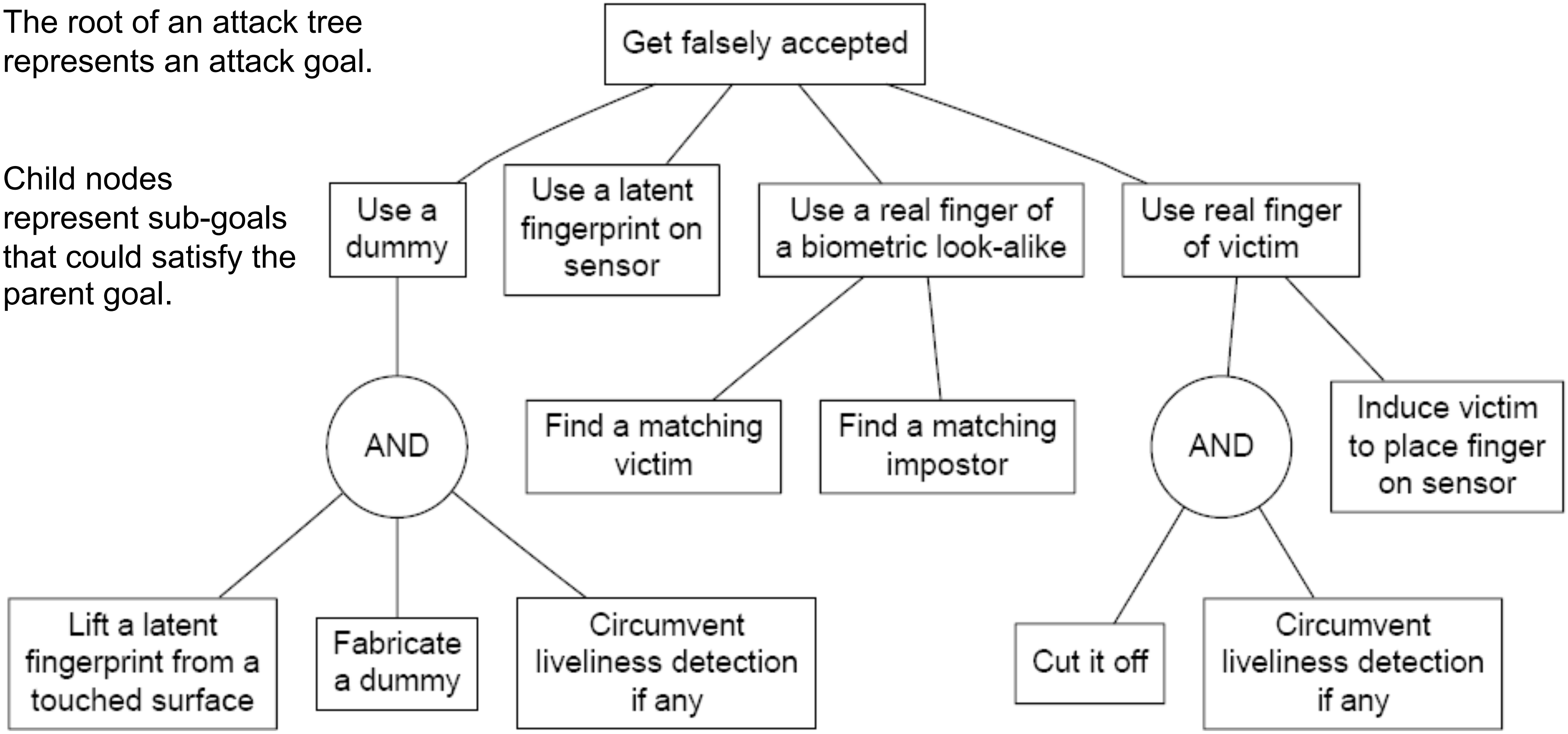
- To address open issues in the methodology for vulnerability analysis of biometric systems
  - How to assess the level of difficulty of attacks (attack potential)
  - How to keep track of the multitude of possible attacks

  using fingerprint recognition systems as example (based on hands-on experience in fabricating fingerprint dummies)
- To discuss methodology (no ready solution given)

Vulnerabilities specific to fingerprint verification systems

The root of an attack tree represents an attack goal.

Child nodes represent sub-goals that could satisfy the parent goal.


Get falsely accepted
Use a dummy
Use a latent fingerprint on sensor
Use a real finger of a biometric look-alike
Use real finger of victim
AND
Find a matching victim
Find a matching impostor
AND
Induce victim to place finger on sensor
Lift a latent fingerprint from a touched surface
Fabricate a dummy
Circumvent liveliness detection if any
Cut it off
Circumvent liveliness detection if any

Attack potential

- Corresponds to the minimum effort required to create and carry out an attack
- For leaf nodes of attack tree (“elementary” attacks): Evaluated using established, structured approach of “Common Criteria”
- For parent nodes:
  Aggregation of attack potentials of children nodes
  - OR relation: As low as for the easiest option
  - AND relation: As high as for the hardest essential element
- Inversely related to **frequency of success**, which is used in risk analysis (risk = frequency of success · severity)
  - The easier the attacks are,
    the more frequent they occur and succeed.

Rating of attack potential

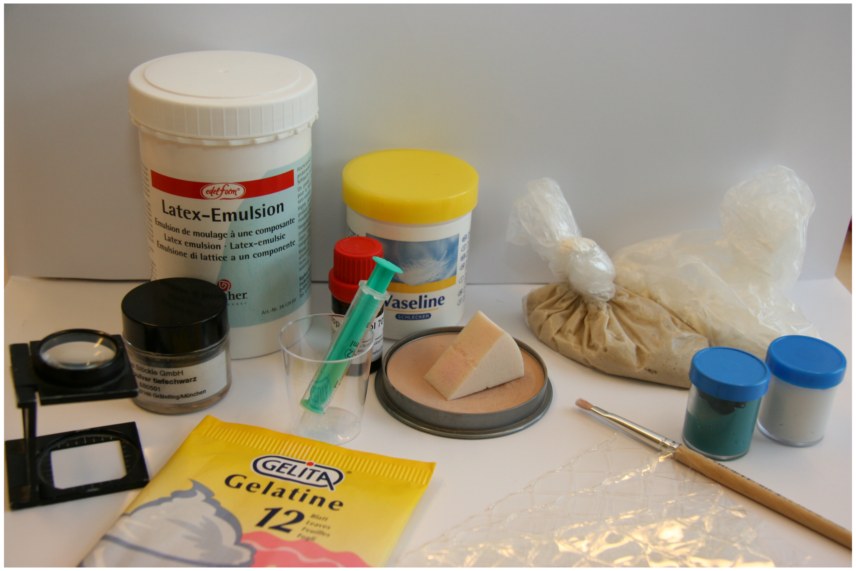
Factor	Level	Value
Elapsed time	≤ 1 day	0
	≤ 1 week	1
	≤ 1 month	4
	≤ 3 months	10
	≤ 6 months	17
	> 6 months	19
	not practical	∞
Expertise	Layman	0
	Proficient	3
	Expert	6
	Multiple experts	8
Knowledge of TOE	Public	0
	Restricted	3
	Sensitive	7
	Critical	11
Window of opportunity	Unnecessary/unlimited	0
	Easy	1
	Moderate	4
	Difficult	10
	None	∞
Equipment	Standard	0
	Specialized	4
	Bespoke	7
	Multiple bespoke	9

- Guidelines desirable for biometric systems
  - What exactly does it take to be “proficient” or “expert”?
  - What equipment can be considered “standard”?

Values	Attack potential
0–9	Basic
10–13	Enhanced-Basic
14–19	Moderate
20–24	High
≥ 25	Beyond High

Fabricate a dummy from a fingerprint image

- Steps
  1. Image enhancement
  2. Print image on transparency
  3. Expose photo-reactive polymer plate to UV light through transparency
  4. Wash out unexposed locations
  5. Press dummy material onto mould, e.g.
     – Wax, gelatin, material for dental casts



- For all tested sensor technologies,
  – Optical sensors, capacitive sensors, e-field sensors, thermal sensors

matching dummies could be fabricated if liveliness detection is deactivated.

Fabricate a dummy from a fingerprint image

Elapsed time:	≤ 1 week of experiments till a match is achieved (if liveliness detection is missing)
Expertise:	Proficient
Knowledge of the TOE:	Public
Window of opportunity:	Unnecessary/unlimited
Equipment:	Specialized (can be easily acquired)
Attack potential:	Basic

Circumvent liveliness detection (if any)

Elapsed time:	≤ 1 month
Expertise:	Expert
Knowledge of the TOE:	Sensitive
Window of opportunity:	Easy (if unattended)
Equipment:	Specialized
Attack potential:	High

Lift a latent fingerprint from a touched surface

Elapsed time:	≤ 1 day
Expertise:	Proficient
Knowledge of the TOE:	Public
Window of opportunity:	Difficult (if the person impersonated is not cooperati
Equipment:	Standard
Attack potential:	Moderate

Use a fingerprint dummy

Essential elements:

- Lift a latent fingerprint from a touched surface,
- Fabricate a fingerprint dummy and
- Circumvent liveliness detection

Attack potential:

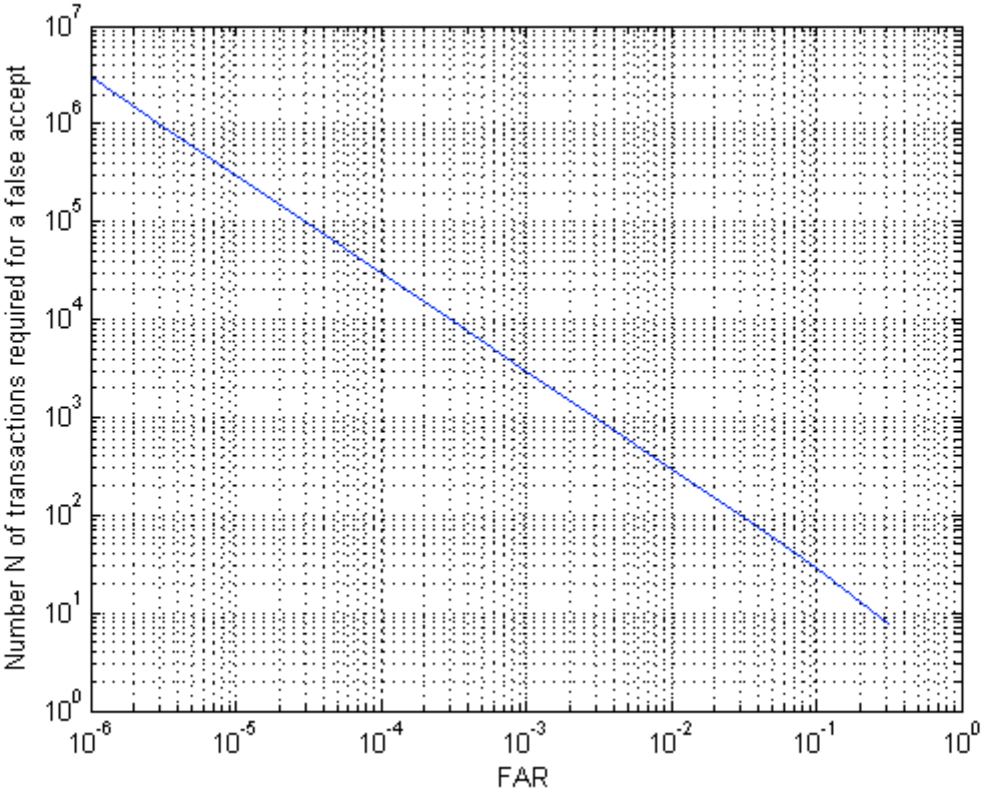
As high as that of the hardest essential element, i.e.

- High if there is liveliness detection or
- Moderate if there is no liveliness detection

Get falsely accepted as somebody else (zero-effort attack)

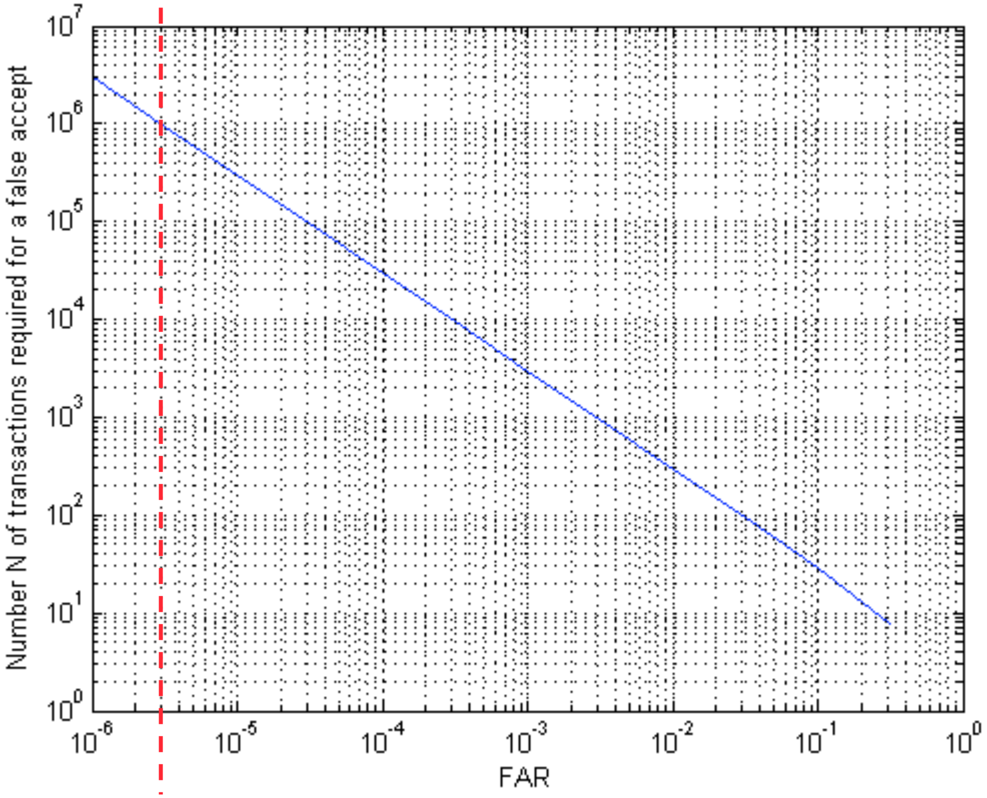
Elapsed time:	Depends on • number of persons an attacker needs to try to impersonate until being falsely accepted with 95% probability or • number of attackers that have to team up with each other to try to impersonate a particular person
Expertise:	Layman
Knowledge of the TOE:	Public
Window of opportunity:	Easy (if unattended one-factor authentication)
Equipment:	Standard
Attack potential:	Depends on FAR

Number of transactions till false accept (95% confidence)



- Let number of retries be limited to *m*.
- Then a failed transaction consists of *m* failed attempts.
- Let transactions be independent from each other (different attacker or victim in each transaction).
- Then it takes $N = \log_{(1-FAR)}(1-0.95)$ transactions to be falsely accepted with 95% confidence.
- Elapsed time and required window of opportunity proportional to *N*

Comparison with brute-force attack against PIN



- 6-digit PIN with 3 permitted retries is resistant against high attack potential
- Probability of guessing it right is $3 \cdot 10^{-6}$
- If single fingerprint presentation does not take longer than single PIN entry, then FAR should also be $3 \cdot 10^{-6}$ for the same security.
- Higher FAR admissible
  if fingerprint recognition is part of multi-factor authentication,
  e.g. in combination with smart card
  (stealing 10^6 cards should be difficult)

Summary

- Attack potential that the TOE is able to withstand depends on the particular TOE and its environment.
- System is only as secure as its “weakest link”.
- Importance of multi-factor authentication
- Need for more experiments and consensus building on attack potential assessment for biometric systems

Thank you! Questions?

- Contact: olaf.henniger@sit.fraunhofer.de
- Summary paper will be in the post-proceedings.

Fraunhofer
SIT