Fake detection WS

Axel Munde

How can artifact detection complement common criteria and other security assessments of authentication systems?

Some Questions

- Focus of Standard?
- Is fake detection related to biometric quality?
- Fake detection vs Liveness detection?
- Are the results of fake detection predictable?
- How biometric modal specific is fake detection?
- How to measure/evaluate fake resistance?
- Actual CC approach – Security by obscurity – Useful?
  - Determination of Fake recognition rate?
- Useful to encode fake resistance in interchange formats?
- Focus on fake detection for fingerprints?
- Brute Force and Hill Climbing attacks?

Fake WS

Artefact (3 rd WD WD 30107)

artificial object(s) or characteristic(s) presenting a copy of biometric characteristics or synthetic pattern made to be presented to a biometric capture device with the aim of subverting the biometric system.

Challenges of Biometrics

1. Statistical properties (FAR / FRR <=> BEM <=> SC37 WG5 Standards)
2. Strong and weak biometrics and the “Zoo” (User depending) – Quality related?
   – In 1. and 2. – No (technical) tools used for attacking
3. Attacks on biometric systems using fakes
4. …

Other Challenges?

Attack Potential
- Calculation and Rating -

Attack Potential = Elapsed Time + Expertise + Knowledge of TOE + Window of Opportunity + Equipment

Value	Resistant against attackers with attack potential of:
0 – 4	No rating
5 – 9	**Minimal**
10 – 13	Basic
14 – 19	Enhanced-Basic
20 – 24	Moderate
>= 25	High

Elapsed Time

Elapsed Time	Factor Value
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19

Expertise and Knowledge of TOE

Expertise	Factor Value
Layman	0
Proficient	3[1]
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11

[1] When several proficient persons are required to complete the attack path, the resulting level of expertise still remains “proficient” (which leads to a 3 rating).

Window of Opportunity and Equipment

Window of Opportunity	Factor Value
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	[2]

Equipment	Factor Value
Standard	0
Specialised	4[3]
Bespoke	7
Multiple bespoke	9

[2] Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE.

[3] If clearly different test benches consisting of specialised equipment are required for distinct steps of an attack, this should be rated as bespoke.