Spoof Detection and the Common Criteria

Ralph Breithaupt (BSI)

Nils Tekampe (TÜViT)

Bundesamt
für Sicherheit in der
Informationstechnik

TÜViT®

Content

- Today's situation
- The BSI projects LifeFinger I & II
- Spoofing – The definition
- Spoof Detection in Common Criteria
  - Protection Profiles
  - Evaluation of Spoof Detection Systems
- Conclusions and Recommendations

Today‘s Situation

- Biometric systems have developed markets that have highly sophisticated requirements for the security of the used systems
- The issue of spoofing biometric characteristics has been known and reported in literature for years but have not been exhaustively discussed
- Recent incidents (e.g. in Japan 2008 & 2009) brought this issue into the focus for a while
- However, in the meantime the situation is nearly as ignorant as before.
- All world is ignoring spoofs… All world? Not all world. Some institutes consider this being one of the major challenges for biometrics today.
- Some developers of sensor devices for fingerprints have started to implement countermeasures against spoofed fingerprints

Today‘s situation – the task

“ **The trust in biometric systems depends on their reliability AND their level of security!”**

- There are many types of publicly known fakes
- … and a huge number of possible variants !

- with little experience fakes are:
  - made of cheap & easy obtainable materials
  - relatively easy to produce
  - able to deliver high quality fingerprints
  - adaptable by additives like: magnetic powder, color..

- The task for spoof detection is to distinguish between all existing human fingers and all possible spoofing materials!

Life Finger II – Goals & Result

"What is the minimal effort required to spoof a wide variety of current fingerprint scanners?"

- BSI tested a variety of current scanners (spoof detection turned off):
  - 5 optical scanners (4 FTR / 1x non FTR)
  - 3 capacitive scanners
  - 1 thermal scanner
  - 2 electric field/RF scanners
  - 1 ultra sonic scanner

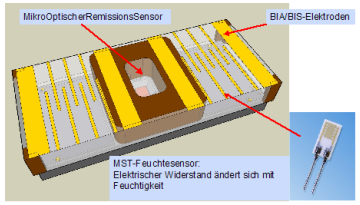
→ **There are differences, but only 5 basic fake types had to be tested to find one that spoofed all scanning technologies 100% !**

Life Finger I - Goals

“ What technical countermeasures are possible/available to detect finger fakes?“

- Composition of a “Fake-Tool-Box“ based on public knowledge and additional experience
- Performance evaluation of current scanners with spoof detection abilities (2008)
- Development of new spoof detection sensor technologies
- Development of a Common Criteria certification methodology of spoof detection technologies

Life Finger I: Results



- A “Fake-Tool-Box“ 25 different fake types and variations – regularly updated
- The few existing scanners with spoof detection perform very differently but even the best can be spoofed by new fakes or simple variations of known materials
- 5 different spoof detection approaches have been developed and tested. (using pulsoxymetry, bioimpedance, ultra sonic (2 different types, near infrared spectroscopy)
- A CC 3.1 certification methodology of spoof detection technologies of fingerprint scanners has been developed along with 2 Protection Profiles for different assurance levels

Motivation for CC-Certification:

- Basis for the comparison of spoof detection solutions
- Support for vendors of biometric devices to:
  - reward their existing efforts in spoof detection development
  - encourage further development in that area
- Setting a starting point for international standardization & cooperation in that area to make biometrics safer & more trustworthy
- A CC-certificate is a possibility to define & to demand a certain standard of reliability

Spoofing: The definition

- Spoof attack:
- Attack on biometric systems trying to enrol, identify, or verify a subject using a non-genuine (spoofed) biometric characteristic thereby claiming an identity that is different from the subjects identity.

- According to this definition a manipulation or obfuscation of biometric characteristics focussing on disguise is not considered a spoof attack.

Spoof detection in Common Criteria (CC)

- As the CC are the de facto standard when it comes to the evaluation of IT-security it was one focus of LifeFinger I to develop the necessary guidance in order to apply these criteria to spoof detection systems
- CC certifications aim to make evaluation of IT security components comparable
- CC certifications are recognized by more than 25 countries.
- A Protection Profile (PP) serves as a kind of specification for the functionality that has to be provided by spoof detection systems and how it can be evaluated

Protection Profiles

- In the course of LifeFinger I two dedicated Protection Profiles (PPs) have been developed to address the specific characteristic of spoof detection devices
- The first PP bases on Organizational Security Policies and focuses on a pure functional test of the biometric spoof detection
- The second PP defines a dedicated level for vulnerability assessment in order to describe an entry level into the classical assurance packages
- Both PPs will be published on www.bsi.de soon

Protection Profiles based on Security Policies

- Introduces an explicit Security Functional Requirement to describe the functionality around spoof detection in terms of CC
- Defines an explicit assurance package based on EAL 2 for evaluation
- An evaluation according to this PP requires
  - A Security Target
  - A functional specification of the public interfaces of the spoof detection system
  - A security architecture and a basic design documentation
  - Guidance documentation
  - A process for “flaw remediation” that addresses how new fakes can be handled
  - Resistance against a well defined toolbox

Protection Profile based on explicit VAN

- The second PP follows the same concept as the first one with only little functional differences
- The PP also defines an explicit assurance package but augments the assurance aspects of the first PP by an explicit component for vulnerability analysis.
- This component AVA_VAN.E requires a vulnerability assessment but requires less resistance against attacker than the standard assurance component for EAL 2.
- In contrast to the PP that bases on policies only an evaluation according to this PP will include dedicated modifications and adoptions of fakes specifically for the product under evaluation
- In order to pass an evaluation according to this PP a product does not only have to recognize a certain set of fakes but all fakes falling into a certain class of effort

Methodology

- The methodology aims to supplement the existing criteria in Common Criteria and provide guidance to evaluators
- Beside some generic guidance the methodology provides
  - A concept on testing
  - Guidance on vulnerability analysis for spoof detection systems in form of classical vulnerabilities and guidance on rating of those vulnerabilities.
- Concrete requirements on test sizes and acceptable error rates have been developed within a dedicated document as they are expected to be highly dynamic

Conclusions & Recommendations:

- Finger fakes are a real risk in some application scenarios
- Every scanner we know of can be spoofed today
- Every new/enhanced spoof detection technology increases security
- BSI is working on 5 new detection methods and a proposal for a CC3.1 certification methodology
- Today: supervision where applicable
- More requests for spoof detection technologies
- Multimodal biometrics to increase level of security
- A CC-certificate is a possibility to define & to demand a certain standard of reliability that is also usable for tender
- The first evaluation of a spoof detection system is ongoing
- International standards and cooperation

Thank you very much for your attention

Danke

Bedankt

Obrigado

MERCI

Grazie

Takk

Thank You!

Shukran

Thank you very much for your attention!

Nils Tekampe
Information Security

Langemarckstrasse 20
45141 Essen, Germany

Phone: +49 201 8999 – 622
Fax: +49 201 8999 – 666
E-Mail: n.tekampe@tuvit.de
URL: www.tuvit.net

Bundesamt
für Sicherheit in der
Informationstechnik

Ralph Breithaupt

E-Mail: r.breithaupt@bsi.de