

Biometric Spoof Detection in the Context of Common Criteria

Frank Grefrath, German Federal Office for Information Security
Nils Tekampe, TÜV Informationstechnik GmbH

11. ICC, September 2010, Turkey

- ❑ BSI-motivation – Lifefinger I Project

- ❑ Spoof Detection and Common Criteria
 - ❑ Problems in context of Common Criteria
 - ❑ Fingerprint Spoof Detection Protection Profiles
 - ❑ Fingerprint Spoof Detection Evaluation Guidance

- ❑ Summary and Outlook

The Lifefinger I Project



- ❑ Incidents all over the world showed that spoofing biometric characteristics is a real issue
- ❑ 2009 the first fingerprint sensors claiming to be resistant against spoofing came into the market
- ❑ BSI launched a series of projects in order to facilitate the development of technology in this area
- ❑ The scope of the LifeFinger I project included
 - ❑ A detailed analysis of initial situation
 - ❑ The development of innovative prototype technologies for spoof detection
 - ❑ The development of evaluation criteria for spoof detection systems

Spoofing is a real issue

GIZMODO THE GADGET BLOG Display · Condensed · search Most recent · Login

iPhone APPS ▶ BESTMODO ▶

PHONE APPS DIRECTORY presented by

New York, 1:53 PM
Fri Jan 2
16 posts in the last 24 hours
UK | FR | NL | IT | DE | SP | JP | AU | BR

GIZMODO TEAM

Tip your editors:
tips@gizmodo.com

Editorial Director:
Brian Lam | Email

Editor:
Jason Chen | Email | AIM

Features Editor:
Wilson Rothman | Email

Senior Associate Editor:
Jesus Diaz | Email | AIM

Associate Editors:
John Mehoney | Email
Mark Wilson | Email | AIM
Matt Buchanan | Email | AIM
Adam Frucci | Email

Reporter:
Adrian Covert | Email

Contributing Editors:
Sean Fallon | Email
Elaine Chow | Email
Jack Loftus | Email

BIOMETRICS « next »

Million Dollar Border Security Machines Fooled with Ten Cent Tape

By [Jesus Diaz](#), 1:00 PM on Fri Jan 2 2009, 5,723 views



So much for biometrics and immigration security: A South Korean woman managed to fool a million-dollar fingerprint reading machine in Japanese border controls using a simple piece of tape stuck to her fingers.

It happened at Tokyo airport. The woman has repeatedly entered Japan using the same

trick without anybody noticing. Japanese officials say that they suspect many others have been doing the same things, demonstrating that the biometric systems they installed in 30 airports in 2007—to the tune of \$45 million—are completely useless. The woman was deported in July 2007 for illegally staying in Japan as a bar hostess in Nagano, but she entered again with the system, using the tape and a fake passport allegedly provided by a South Korean broker. [\[Sidney Morning Herald via Fashion Funky\]](#)

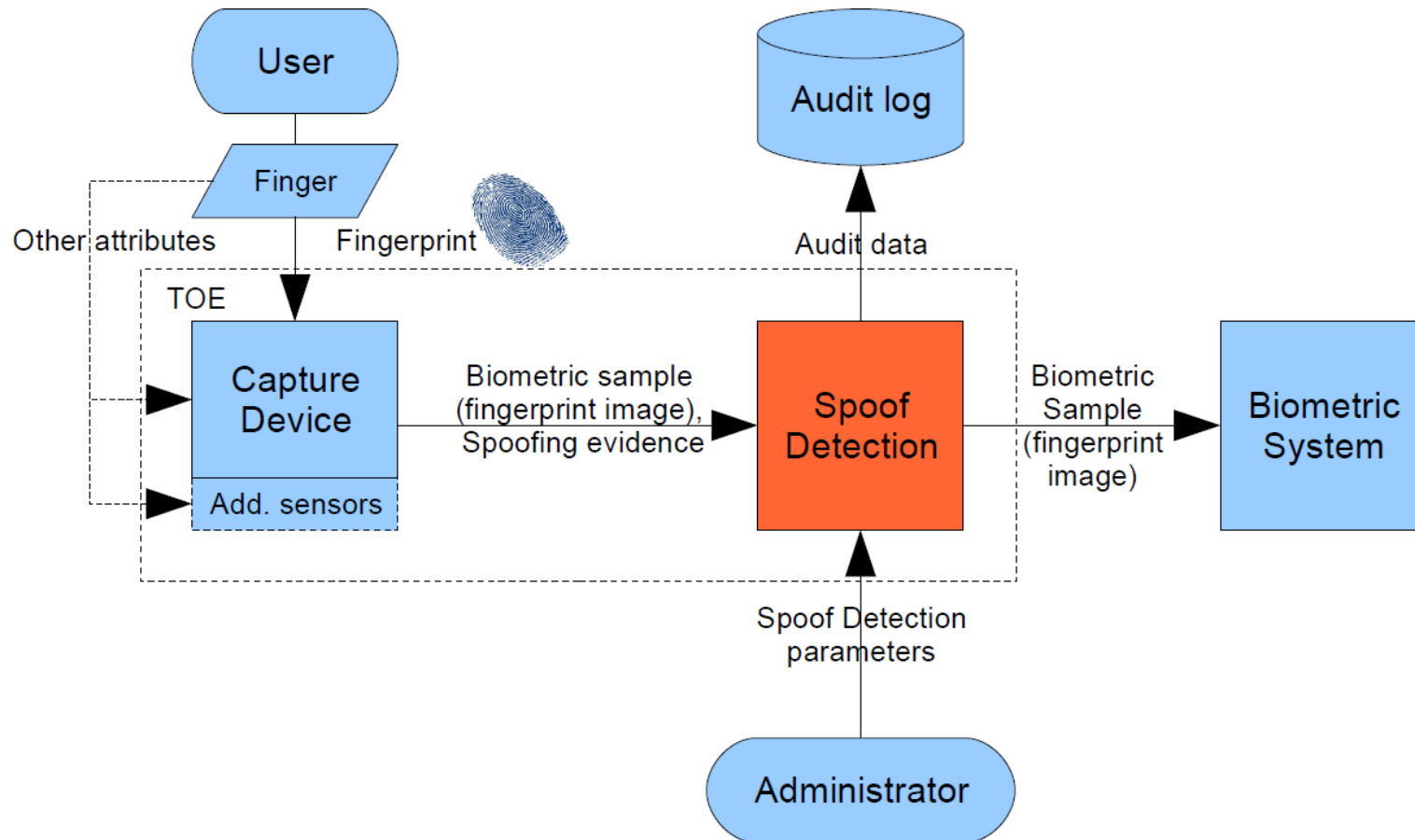
- ❑ Every fingerprint sensor that has been available in the market by the time of the project can be spoofed with relatively simple fakes
- ❑ Some sensors did recognize a subset of the available fakes in the market
- ❑ For each sensor a “golden” fake could be identified that worked reproducibly
- ❑ The project showed however promising technologies to counter fakes in future
- ❑ In order to rate the performance of current and future spoof detection technologies there is a need for a comprehensive evaluation methodology

- ❑ Common Criteria requires resistance against a certain attack potential (as defined by the used EAL)
- ❑ LifeFinger I showed that the systems of the early generations would even fail an EAL1
- ❑ However, LifeFinger I also showed that the systems of the next generations will most likely pass CC evaluations
- ❑ Instead of developing a proprietary and functional evaluation methodology an entry level should be defined
- ❑ Aspects of testing and vulnerability analysis need special considerations based on the results of the LifeFinger I project
- ❑ This lead to the development of
 - ❑ Two dedicated Protection Profiles
 - ❑ An evaluation methodology for CC

- ❑ BSI-CC-PP-0062-2010
Fingerprint Spoof Detection Protection Profile based on OSPs (FSDPP_OSP)
 - ❑ Aimed at functional testing of a TOE
 - ❑ SPD based on Organizational Security Policies (OSPs)
 - ❑ No threats, no vulnerability assessment

- ❑ BSI-CC-PP-0063-2010
Fingerprint Spoof Detection Protection Profile (FSDPP)
 - ❑ OSPs restated as threats
 - ❑ Vulnerability assessment included

TOE overview



- ❑ Assurance Level for FSDPP_OSP
 - ❑ No use of pre-defined EAL, based on EAL 2
 - ❑ AVA class omitted, ALC_FLR.1 added
 - ❑ CC Part 3 conformant

- ❑ Assurance Level for FSDPP
 - ❑ No use of pre-defined EAL, based on EAL 2
 - ❑ AVA_VAN.E used instead of AVA_VAN.2, ALC_FLR.1 added
 - ❑ CC Part 3 extended

- ❑ Security functionality identical for both PPs:
 - ❑ Spoof detection (FPT_SPOD.1)
 - ❑ Audit of security relevant events (FAU_GEN.1)
 - ❑ Full residual information protection (FDP_RIP.2)
 - ❑ Management of relevant parameters (FMT_MTD.3, FMT_SMF.1)

Fingerprint Spoof Detection Evaluation Guidance

- ❑ Structure of the Evaluation Guidance
 - ❑ Part A: Definition of terms, introduction of spoof detection system
 - ❑ Part B: Interpretation of the SARs and the CEM for spoof detection systems,
Definition of the extended SFR FPT_SPOD.1,
Definition of the extended SAR AVA_VAN.E
 - ❑ Part C: Discussion of testing methodology and vulnerability assessment for spoof detection functionality

Fingerprint Spoof Detection Evaluation Guidance

- Definition of the extended SAR AVA_VAN.E
 - Based on the component AVA_VAN.2 as used in EAL2 evaluations
 - Requires resistance against “minimal” attack potential instead of “basic” attack potential

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

Fingerprint Spoof Detection Evaluation Guidance

❑ Testing methodology:

- ❑ Main focus: Examination whether spoof detection functionality is able to detect spoofed biometric characteristics with a sufficient reliability
- ❑ Determination of security relevant error rate: False Spoof Not Detect Rate (FSNDR)
- ❑ Determination by use of a standardized Fake-Toolbox

❑ Vulnerability assessment:

- ❑ Addresses slight modifications to the “most effective” fakes that are used in ATE and innovative fakes adopted to the specific technology. They must not lead to a deterioration of error rates.
 - ❑ The evaluation guidance provides interpretations of the CEM work units, gives help in finding the most promising fake and gives examples for relevant attack scenarios together with example ratings.
- ❑ The TOE must not miss the maximum error rate for each fake, the “golden” fake as well, that is presented to the system.

- ❑ LifeFinger I showed a clear demand for new technology in order to fight spoofs in biometric systems
- ❑ For fingerprint systems new technology approaches and the required test infrastructure have been defined
- ❑ Developers have access to an entry level for Common Criteria evaluations defined by
 - ❑ Two Protection Profiles
 - ❑ An evaluation methodology
- ❑ The first evaluation according to the developed requirements is currently on its way

Thank you for your attention

Danke Bedankt
Obrigado
MERCI
Grazie Takk
Thank You! Shukran

Federal Office for Information Security

Frank Grefrath

Tel: +49 228 99 9582 5838

Email: Frank.Grefrath@bsi.bund.de

URL: www.bsi.bund.de



TÜV Informationstechnik GmbH

Nils Tekampe

Tel: +49 201 8999 – 622

Email: n.tekampe@tuvit.de

URL: www.tuvit.de

