

# **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



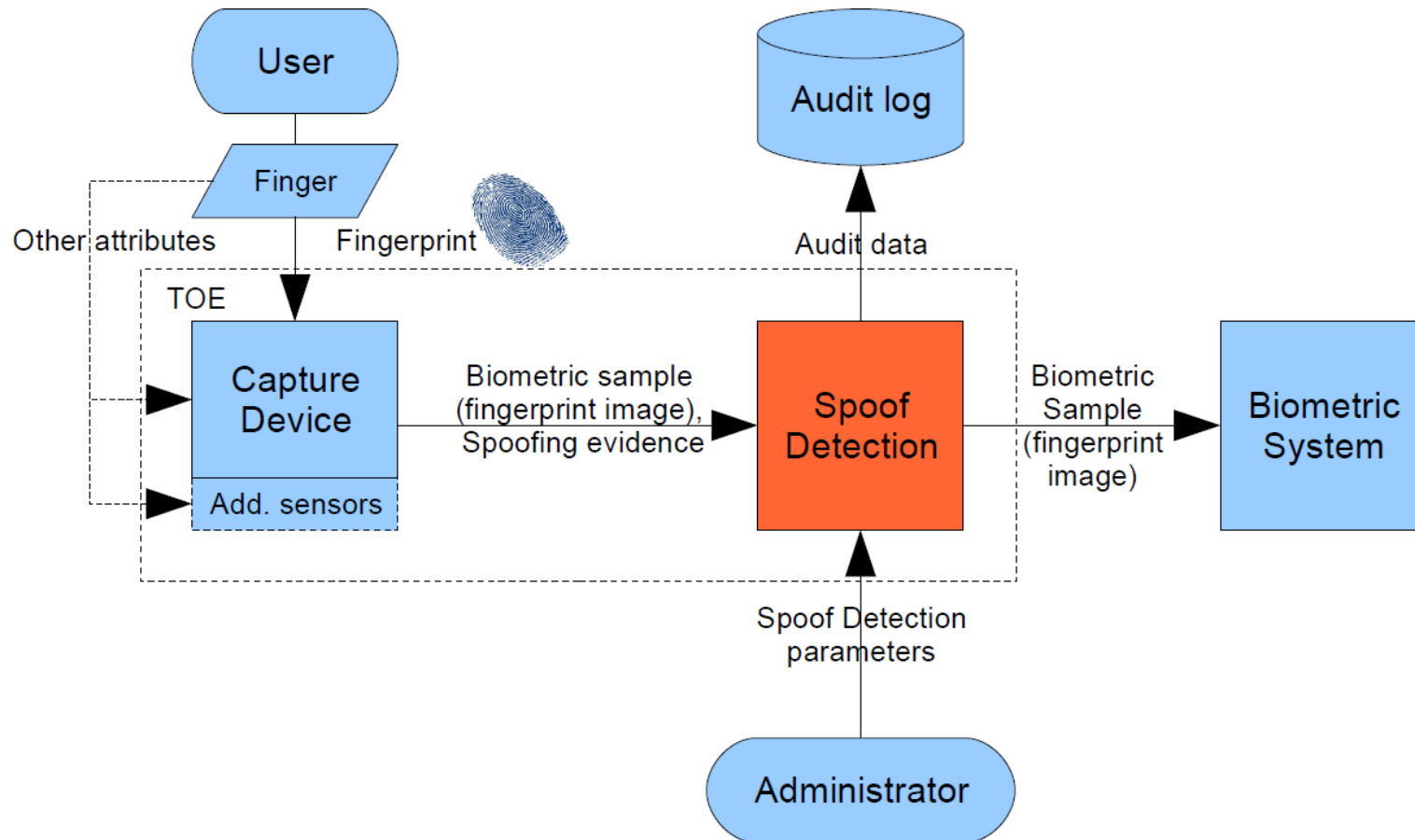
The screenshot shows a Gizmodo article page. At the top, the Gizmodo logo is on the left, and navigation links for 'Display', 'Condensed', a search bar, 'Most recent', and 'Login' are on the right. Below the logo is a 'BIOMETRICS' category tag. The article title is 'Million Dollar Border Security Machines Fooled with Ten Cent Tape'. The byline reads 'By Jesus Diaz, 1:00 PM on Fri Jan 2 2009, 5,723 views'. A 'next' link is visible on the right. On the left side of the article, there is a sidebar with 'iPhone Apps' and 'Bestmodo' buttons, and a 'Phone Apps Directory presented by Bank of America' section. The main content area features a photograph of a hand holding a piece of clear tape over a fingerprint scanner. To the right of the photo, the text reads: '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.' Below this, another paragraph states: '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 con[...]'

- ❑ 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
<b>5 – 9</b>	<b>Minimal</b>
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](mailto:Frank.Grefrath@bsi.bund.de)

URL: [www.bsi.bund.de](http://www.bsi.bund.de)



TÜV Informationstechnik GmbH

Nils Tekampe

Tel: +49 201 8999 – 622

Email: [n.tekampe@tuvit.de](mailto:n.tekampe@tuvit.de)

URL: [www.tuvit.de](http://www.tuvit.de)

