

Presentation Attack Detection - ISO/IEC 30107

Christoph Busch

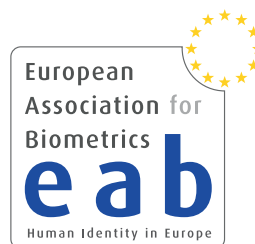
Convenor ISO/IEC JTC1 SC37 WG3

copy of slides available at:

<https://christoph-busch.de/about-talks-slides.html>

latest news at:

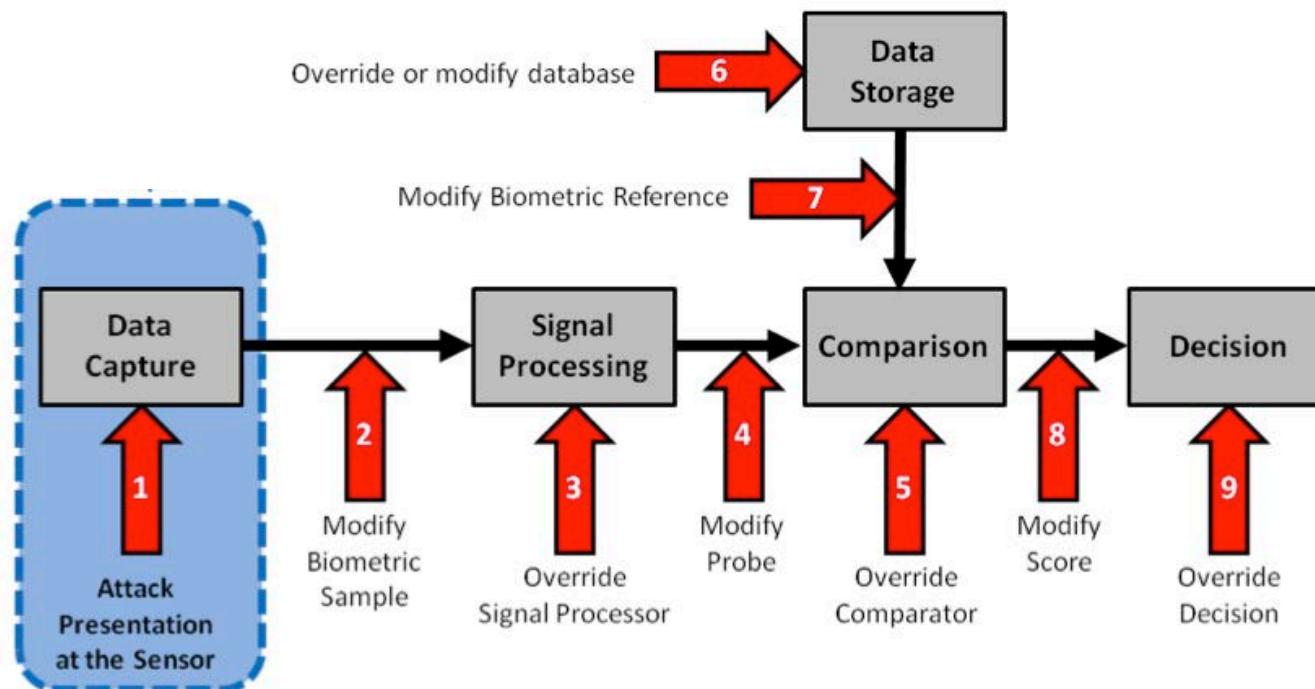
https://twitter.com/busch_christoph



Weakness of Biometric Systems

Three main points for a targeted attack

- Capture device (1): Camera, optical- / capacitive sensor
 - Replay attacks must be countered by presentation attack detection
- Data transmission (2): USB, firewire etc.
 - Susceptibility to attacks on data transmission channel
 - Enrolment attacks (i.e. face morphing attacks)
- Data storage (6): Database, token



Source: ISO/IEC 30107-1:2016

Capture Device - Replicates of Biometric Characteristics

Fingerprint Presentation Attacks

1971

Attack **without** support of an enrolled individual

- James Bond: Diamonds Are Forever



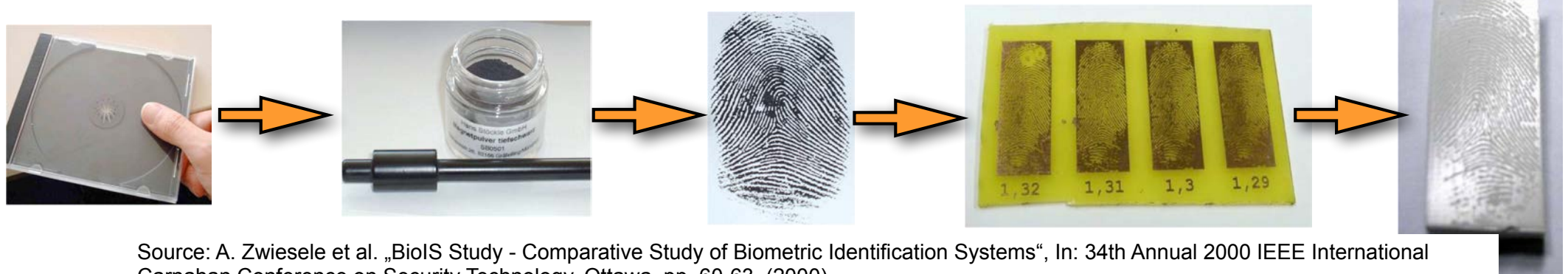
Source: <https://www.imdb.com/title/tt0066995> (1971)

Fingerprint Presentation Attacks

1999

Attack **without** support of an enrolled individual

- Recording of an analog fingerprint from flat surface material
 - ▶ z.B. glass, CD-cover, etc.
with iron powder and tape
- Scanning and post processing:
 - ▶ Correction of scanning errors
 - ▶ Closing of ridge lines (as needed)
 - ▶ Image inversion
- Print on transparent slide
- Photochemical production of a circuit board



Source: A. Zwiesele et al. „BioIS Study - Comparative Study of Biometric Identification Systems“, In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, pp. 60-63, (2000)

Fingerprint Presentation Attacks

2013

Overlay attack **without** support

- Recording of an analog fingerprint from the phone



Source: <https://www.ccc.de/en/tags/apple>, (2013)

Fingerprint Alteration

1997

Example for fingerprint **alterations**

- Z-shaped alteration (Finger of Jose Izquierdo)



Image Source: S. Yoon, J. Feng, and A. Jain, "Altered fingerprints: Analysis and detection,"
IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, pp. 451–464, Mar. 2012

Face Presentation Attacks

2018

3D silicone mask

- Targeted attack with 3D silicone custom mask
- Cost more than 3000 USD



Concealer Presentation Attack

Face disguise for organized crime

2012

- <http://www.dailymail.co.uk/news/article-2153346/Black-armed-robber-disguised-white-man-using-latex-mask.html>



The man in the latex mask: **BLACK** serial armed robber disguised himself as a **WHITE** man to rob betting shops

- Henley Stephenson wore the disguise during a 12-year campaign of hold-ups at betting shops and other stores across London
- He was part of a three-man gang jailed for a total of 28 years
- CCTV footage showed him firing a semi-automatic pistol into the ceiling during a raid on a betting shop
- The mask was bought from the same London shop which supplied masks used in the £40m Graff Diamonds heist

By ROB PREECE and REBECCA CAMBER FOR THE DAILY MAIL

PUBLISHED: 17:22 GMT, 1 June 2012 | UPDATED: 16:21 GMT, 2 June 2012

Most masked robbers opt for a balaclava to hide their identity.

Not this one. Henley Stephenson, 41, eluded police for more than ten years thanks to an extraordinarily lifelike latex mask, which turned him into a white skinhead.

Officers discovered that their man was in fact black when they finally caught up with Stephenson after a string of armed raids dating back to 1999.



Face Presentation Attacks

Make-Up attack



Image Source: <http://upshout.net/game-of-thrones-make-up>



(a) before

(b) after

(c) target

Image Source: <http://www.antitza.com/makeup-datasets.html>

Why is this called Presentation Attack Detection (PAD)
and not Liveness Detection ?

Categories of Presentation Attacks


Impostor

- impersonation attack
 - ▶ positive access 1:1 (two factor application)
 - ▶ positive access 1:N (single factor application)
- finding a look-a-like
- making appearance similar to the reference
- artefact presentation



Image Source: <http://upshout.net/game-of-thrones-make-up>

Concealer

- evasion from recognition
 - ▶ negative 1:N identification (watchlist application)
 - depart from standard pose
- 
- evade face detection

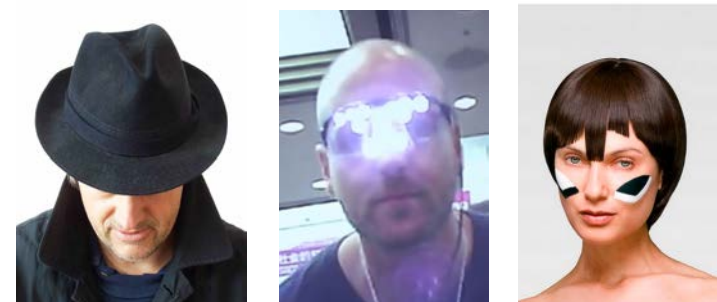


Image Source: <https://www.youtube.com/watch?v=LRj8whKmN1M>

Image Source: <https://cvdazzle.com>

Presentation Attack Detection

Definitions in ISO/IEC 30107 PAD - Part 1: Framework

- **presentation attack**

*presentation to the biometric capture subsystem with the goal of **interfering** with the operation of the biometric system*

- **presentation attack detection (PAD)**

*automated **determination of** a presentation **attack***

Definitions in ISO/IEC 2382-37: Vocabulary

<http://www.christoph-busch.de/standards.html>

- **impostor**

*subversive biometric capture subject who attempts to being matched to **someone else's** biometric reference*

- **identity concealer**

*subversive biometric capture subject who attempts to **avoid being matched** to their own biometric reference*

Presentation Attack Detection - Framework

ISO/IEC 30107-1

- provides the taxonomy
- **freely available** in the ISO-Portal

http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip

ISO/IEC 30107-1:2016(en) Information technology — Biometric presentation attack detection — Part 1: Framework

Table of contents

- Foreword
- Introduction
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Symbols and abbreviated terms
- ▼ 5 Characterisation of presentation attack detection
- 5.1 General
- 5.2 Presentation attack instruments
- ▼ 6 Framework for presentation attack detection
- 6.1 Types of presentation attack detection
- ▶ 6.2 The role of challenge-response
- 6.3 Presentation attack detection procedure
- ▶ 6.4 Presentation attack detection with
- 7 Obstacles to biometric imposter presentation
- Bibliography

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

Presentation Attack Detection

ISO/IEC 30107-1 - Definitions

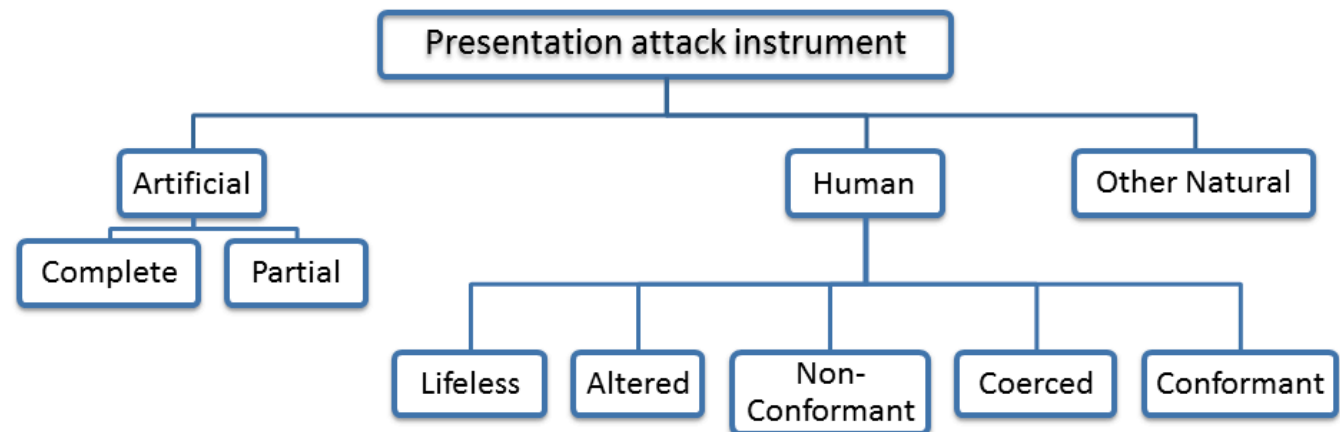
- **presentation attack instrument (PAI)**
*biometric characteristic or **object used** in a presentation attack*
- **artefact**
*artificial object or representation presenting a **copy** of biometric characteristics or synthetic biometric patterns*

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)



Source: ISO/IEC 30107-1

PAD Testing

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the **PAD subsystem** with false-negative and false-positive errors:
- **Attack presentation classification error rate (APCER)**
*proportion of **attack presentations** using the same PAI species incorrectly **classified as bona fide presentations** in a specific scenario*
- **Bona fide presentation classification error rate (BPCER)**
proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics elements

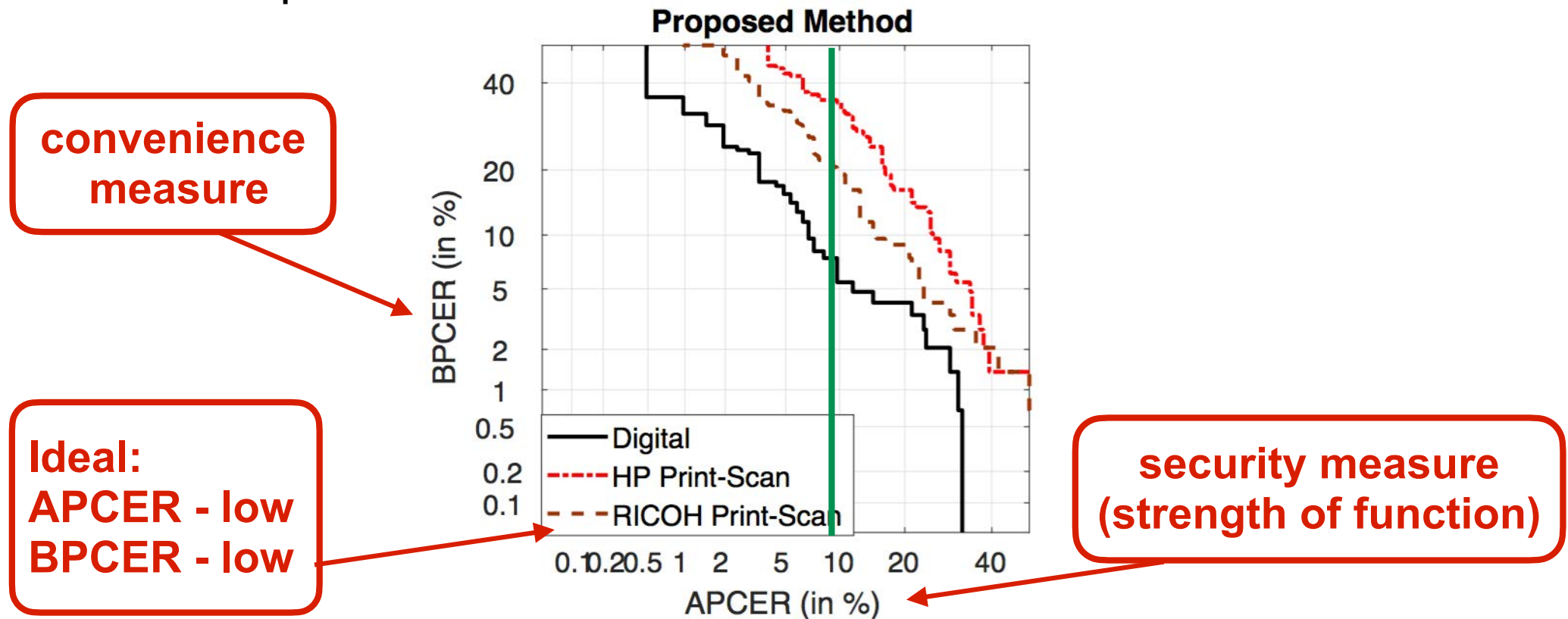
- **PAI species**
class of presentation attack instruments created using a common production method and based on different biometric characteristic
- **Attack potential**
measure of the capability to attack a TOE given the attacker's knowledge, proficiency, resources and motivation
- **target of evaluation (TOE)**
within Common Criteria, the IT product that is the subject of the evaluation

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- DET curve reports operating points for various thresholds showing **security** measures versus **convenience** measures
- Example:



Source: R. Raghavendra, K. Raja, S. Venkatesh, C. Busch: "Transferable Deep-CNN features for detecting digital and print-scanned morphed face images", in Proceedings of 30th International Conference on Computer Vision and Pattern Recognition Workshop (CVPRW 2017), Honolulu, Hawaii, July 21-26, (2017)

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing a **specific security level**:

PAD mechanism may be reported in a single figure

- *BPCER at a **fixed APCER**:*


One may report BPCER when $APCER_{AP}$ is 5% as BPCER20

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

ISO/IEC 30107-3:2017

- Preview: <https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v1:en>

 Online Browsing Platform (OBP)

Search ISO/IEC 30107-3:2017(en) ×

ISO/IEC 30107-3:2017(en) Information technology — Biometric presentation attack detection — Part 3: Testing and reporting

Table of contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

3.1 Attack elements

3.2 Metrics

4 Abbreviated terms

5 Conformance

6 Presentation attack detection overview

7 Levels of evaluation of PAD mechanism

7.1 Overview

7.2 General principles of evaluation

7.3 PAD subsystem evaluation

7.4 Data capture subsystem evaluation

7.5 Full-system evaluation

8 Artefact properties

8.1 Properties of presentation attack

8.2 Properties of presentation attack

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at <http://www.electropedia.org/>

— ISO Online browsing platform: available at <http://www.iso.org/obp>

3.1 Attack elements

3.1.1 presentation attack attack presentation

presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

Note 1 to entry: An attack presentation might be a single attempt, a multi-attempt transaction, or some other type of interaction with a subsystem.

3.1.2 bona fide presentation

interaction of the biometric capture subject and the biometric data capture subsystem in the fashion intended by the policy of the biometric system

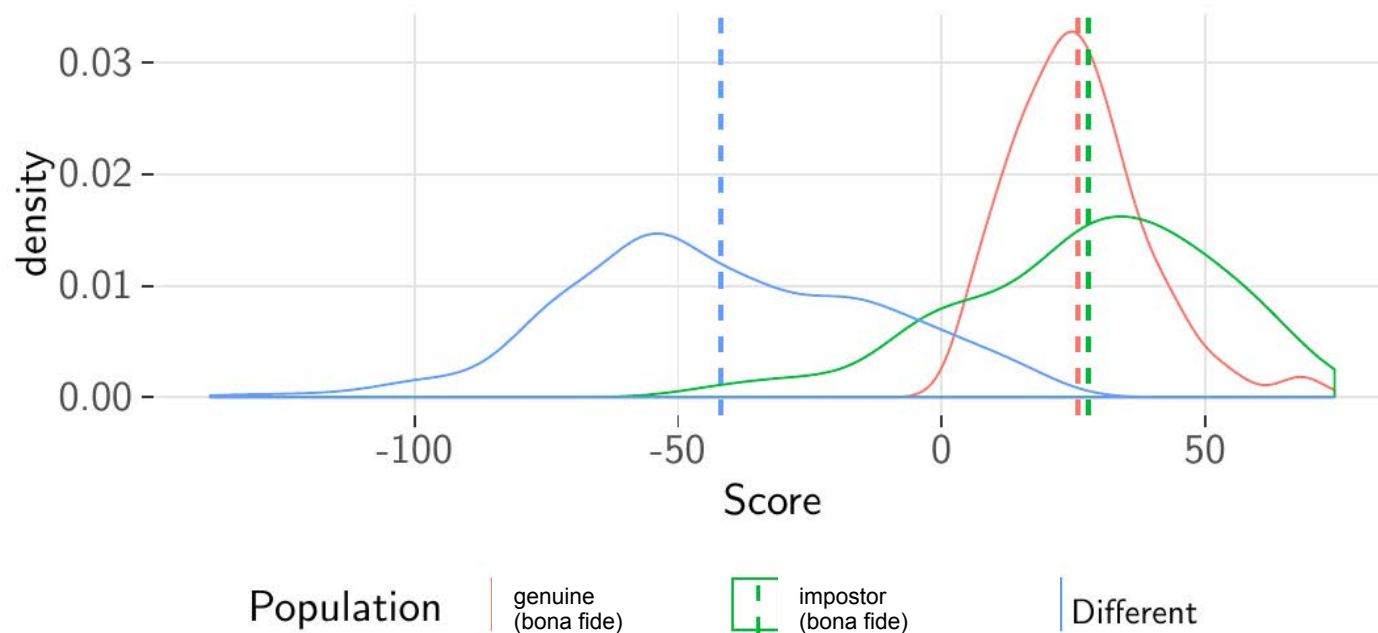
PA Vulnerability Testing

Presentation Attack Detection - Testing

Definition of **full** system **vulnerability** metric w.r.t attacks

- **Impostor attack presentation match rate (IAPMR)**
*<in a **full-system** evaluation of a verification system> the proportion of impostor attack presentation using the same PAI species in which the **target reference** is **matched***

Source: ISO/IEC 30107-3



Presentation Attack Detection - Testing

Definition of PAD metrics in **revision** ISO/IEC 30107-3

- Relationship between **vulnerability** and recognition performance
- **System** testing!
- ~~Impostor attack presentation match rate (IAPMR)~~
- **Impostor attack presentation accept rate (IAPAR)**
*in a **full-system** evaluation of a verification system, proportion of impostor presentation attacks using the same PAI species that result in a **accept***

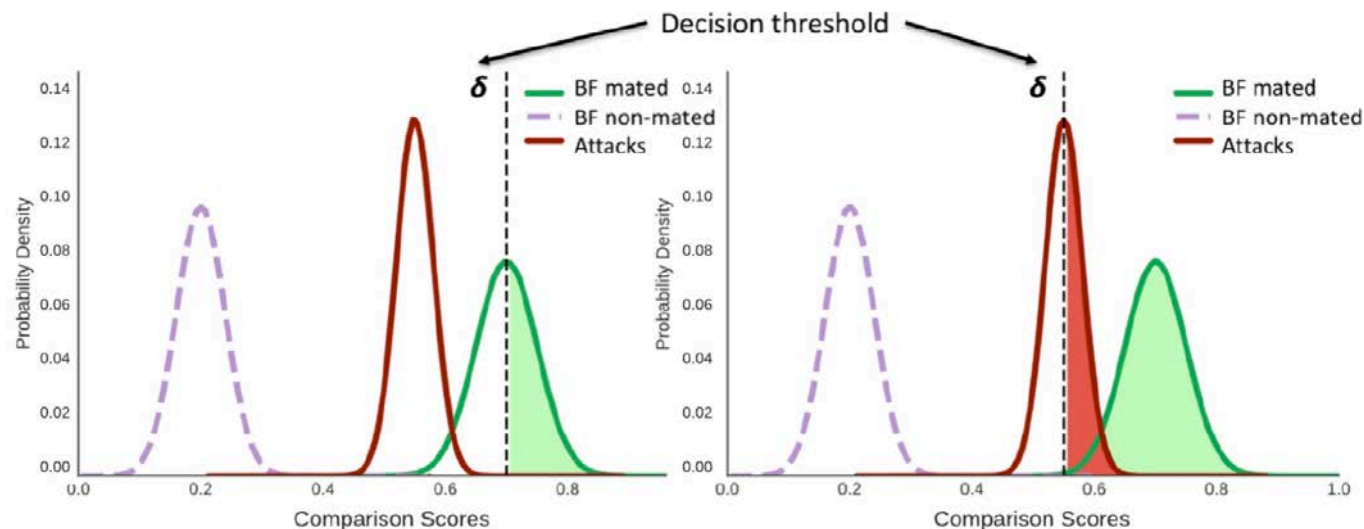
Source: revision ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics in **revision** ISO/IEC 30107-3

- Relationship between **vulnerability** and recognition performance
- **System** testing!
- **Relative** imposter presentation accept rate (**RIAPAR**)
ratio of the IAPAR to the FRR of the system

$$RIAPAR(\tau) = 1 + (IAPAR(\tau) - (1 - FRR(\tau)))$$



Source: U. Scherhag, A. Nautsch, C. Rathgeb, M. Gomez-Barrero, R. Veldhuis, L. Spreeuwiers, M. Schils, D. Maltoni, P. Grother, S. Marcel, R. Breithaupt, R. Raghavendra, C. Busch: "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting", in Proceedings of the IEEE 16th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, (2017)

PAD and FIDO

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-4

- Scope: *This document is a **profile** that provides requirements for testing biometric presentation attack detection (PAD) mechanisms on **mobile devices** with local biometric recognition.*
- Preview: <https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-4:ed-1:v1:en>

| | | |
|------|---|---|
| 13.1 | (13) Evaluations of PAD mechanisms shall report the following: | The evaluator shall provide basis and narrative for each bullet |
| | — (14) number of presentation attack instruments used in the evaluation | The evaluator shall document this number based on IUTs, PAI sources, PAI presenters, species, and series |
| | — (15) number of PAI species used in the evaluation | Best practice is to use a minimum of 3 species NOTE 3 PAD testing designed to assess susceptibility to a broader range of attacks would require that more PAI species be used. EXAMPLE 2 FIDO Biometrics Requirements [3] specifies use of 10 PAI species |
| | — (16) number of PAI series used in the evaluation | Best practice is to use a minimum of 10 PAI series per applicable PAI species NOTE 4 Certain evaluations might need to take place with fewer than 10 PAI series, such as evaluations utilizing expensive, high-quality masks. |



Prof. Dr. Christoph Busch

Norwegian University of Science and Technology
Department of Information Security and Communication Technology
Teknologiveien 22
2802 Gjøvik, Norway
Email: christoph.busch@ntnu.no
Phone: +47-611-35-194

Contact



Prof. Dr. Christoph Busch
Principal Investigator

Hochschule Darmstadt FBI
Haardtring 100
64295 Darmstadt, Germany
christoph.busch@h-da.de

Telefon +49-6151-16-30090
<https://dasec.h-da.de>
<https://www.athene-center.de>