The ISO/IEC standards for testing of Presentation Attack Detection

Christoph Busch /
Hochschule Darmstadt - CRISP

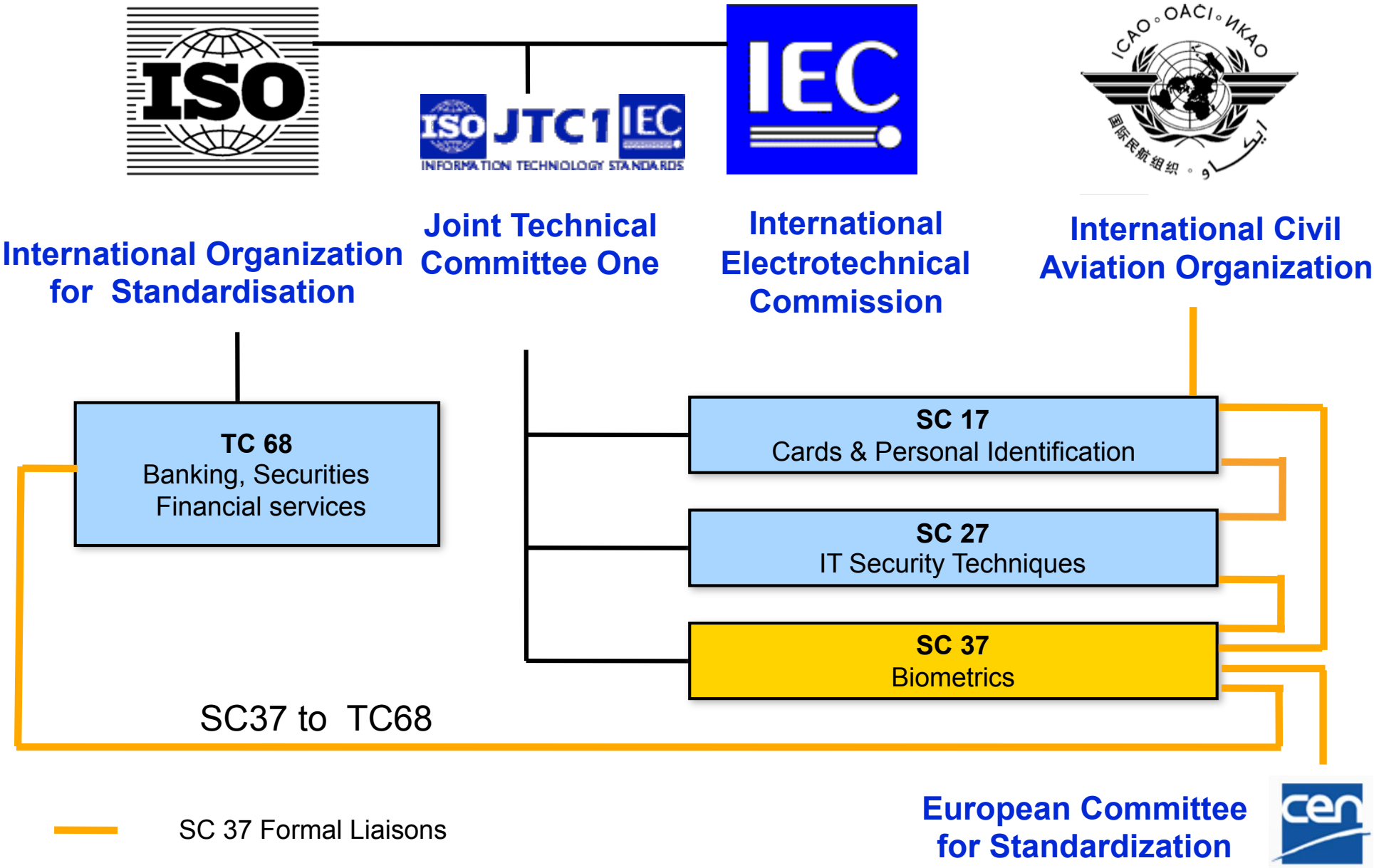
TTT Working Group Biometrics
2017-03-29

Presentation Attack Detection

Outline

- International Standardisation on PAD
- ISO/IEC 30107
- ISO/IEC 19989
- Application areas
- ISO/IEC and FIDO

Biometric Standardisation



ISO/IEC SC37 Biometrics

Established by JTC 1 in June 2002 to ensure

- a high-priority, focused and comprehensive approach worldwide for the rapid development of formal generic biometric standards

Scope of SC37

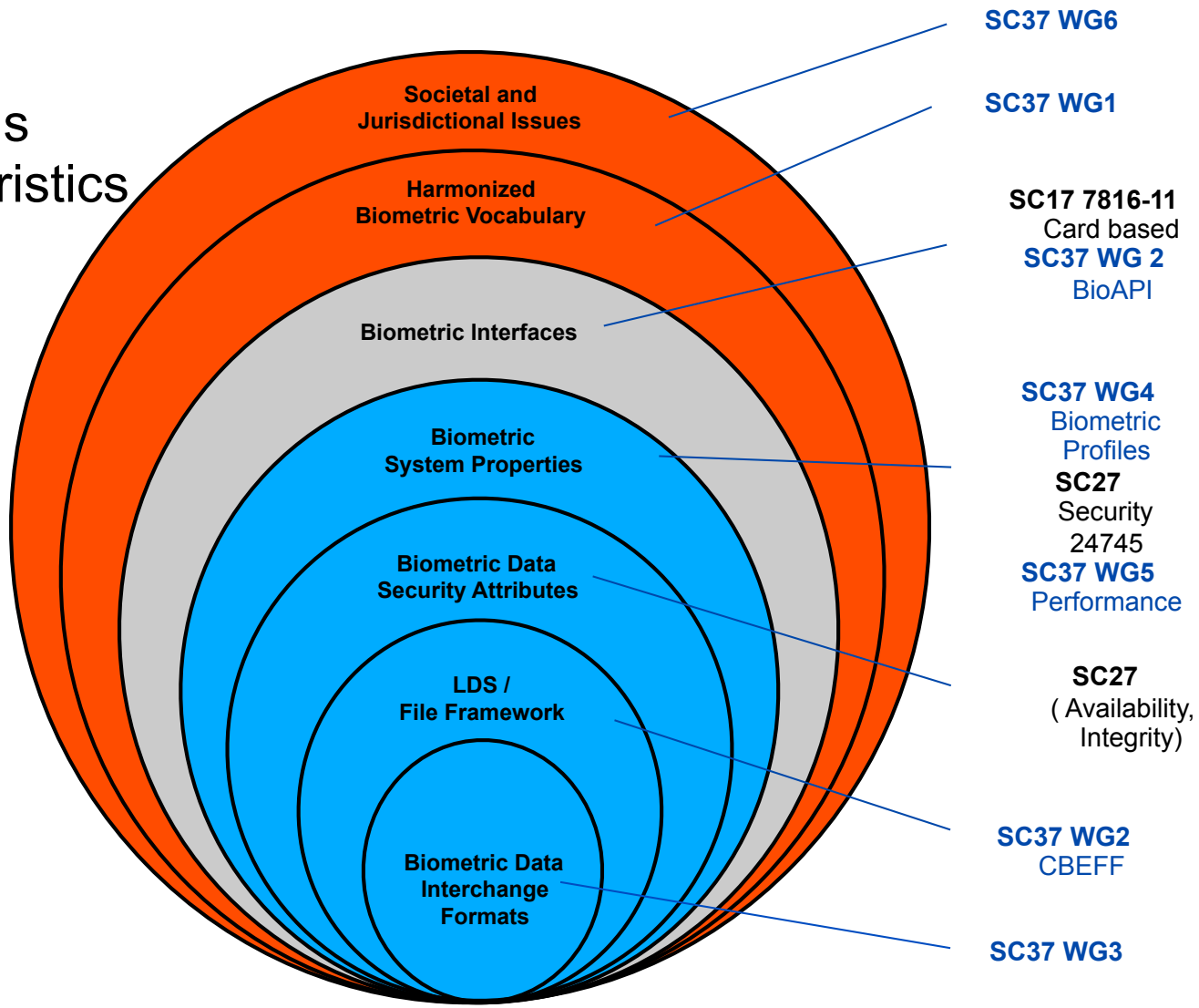
- *"Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange formats; related biometric profiles; application of evaluation criteria to biometric technologies; methodologies for performance testing and reporting and cross jurisdictional and societal aspects"*
- http://www.jtc1.org

Next meeting: July, 2017

Biometric Standardisation

Onion Layers

- Layer 1: BDIR
  - Digital representations of biometric characteristics
- Layer 2: LDS
  - CBEFF Meta-data
- Layer 3+4: System properties
  - Security
  - Performance
- Layer 5: BioAPI, BIP
  - System Integration

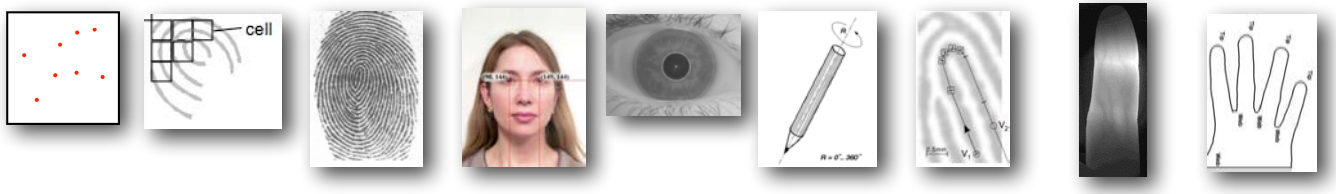


First Generation Format Standards

G1

19794-1:2006

-2: 2005	-3: 2006	-4: 2005	-5: 2005	-6: 2005	-7: 2007	-8: 2006	-9: 2007	-10: 2007



All parts
binary encoding

The 19794-Family: Biometric data interchange formats

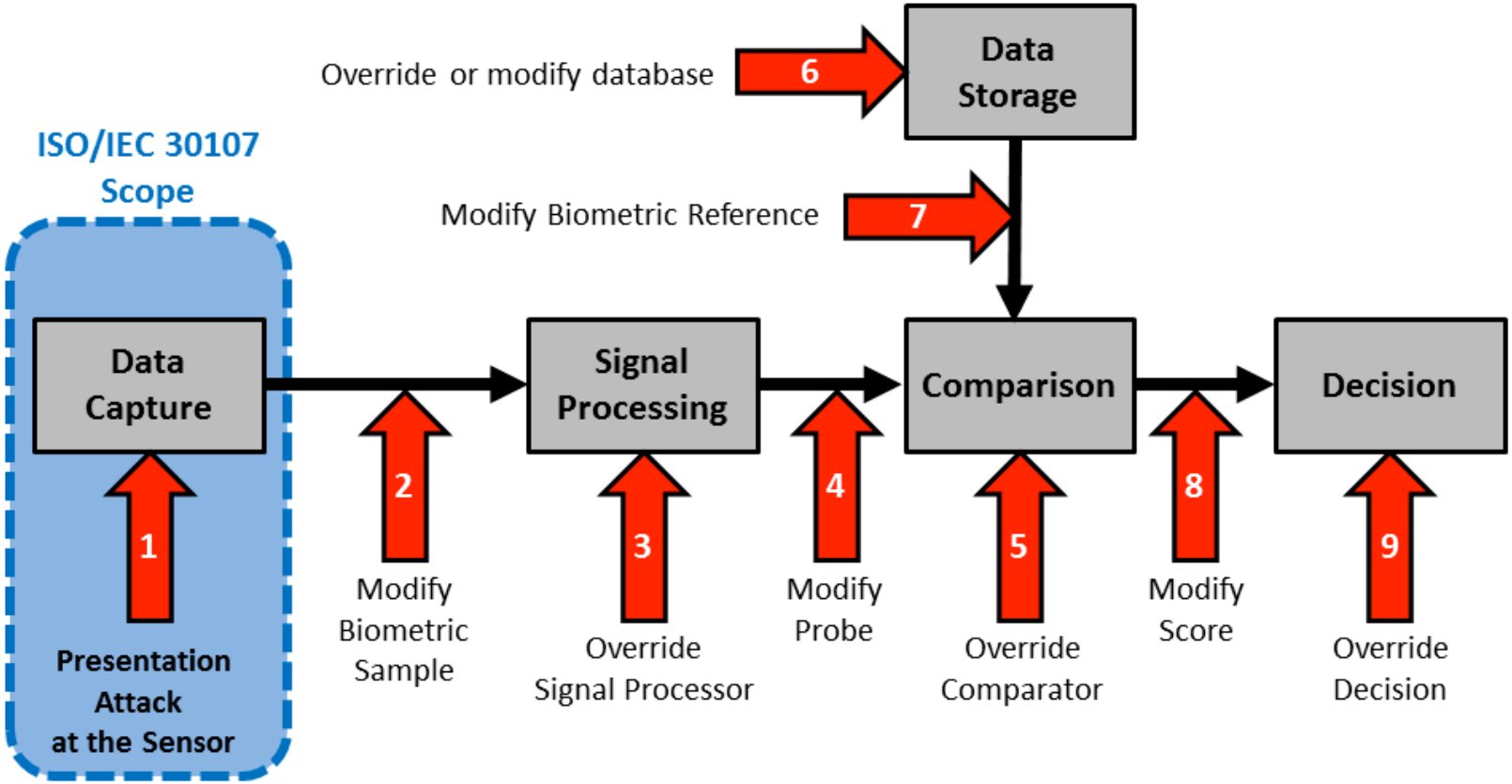
Presentation Attack Detection

ISO/IEC 30107 - Overview and Part 1

System Perspective - Framework

ISO/IEC 30107-1:2016 Presentation Attack Detection

- Attacks on Biometric Systems



Source: ISO/IEC 30107-1
Inspired by N.K. Ratha, J.H. Connell, R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, Vol 40. NO 3, 2001.

Presentation Attack Detection

ISO/IEC 30107 - Scope

- terms and definitions that are useful in the specification, characterization and evaluation of presentation attack detection methods;
- a common data format for conveying the type of approach used and the assessment of presentation attack in data formats;
- principles and methods for performance assessment of presentation attack detection algorithms or mechanisms; and
- a classification of known attacks types (in an informative annex).

Outside the scope are

- standardization of specific PAD detection methods;
- detailed information about countermeasures (i.e. anti-spoofing techniques), algorithms, or sensors;
- overall system-level security or vulnerability assessment.

Presentation Attack Detection - Framework

ISO/IEC 30107-1

- now freely available in the ISO-Portal
  http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip

Online Browsing Platform (OBP)

Search | ISO/IEC 30107-1:2016(en)

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

Table of contents

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).

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

ISO/IEC 30107-1 - Definitions

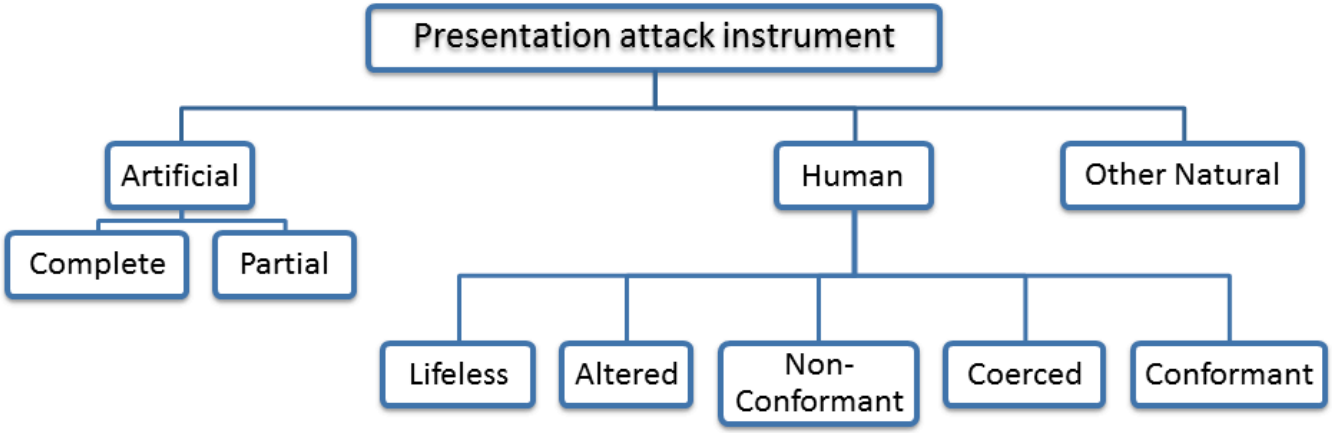
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)



Source: ISO/IEC 30107-1

Presentation Attack Detection

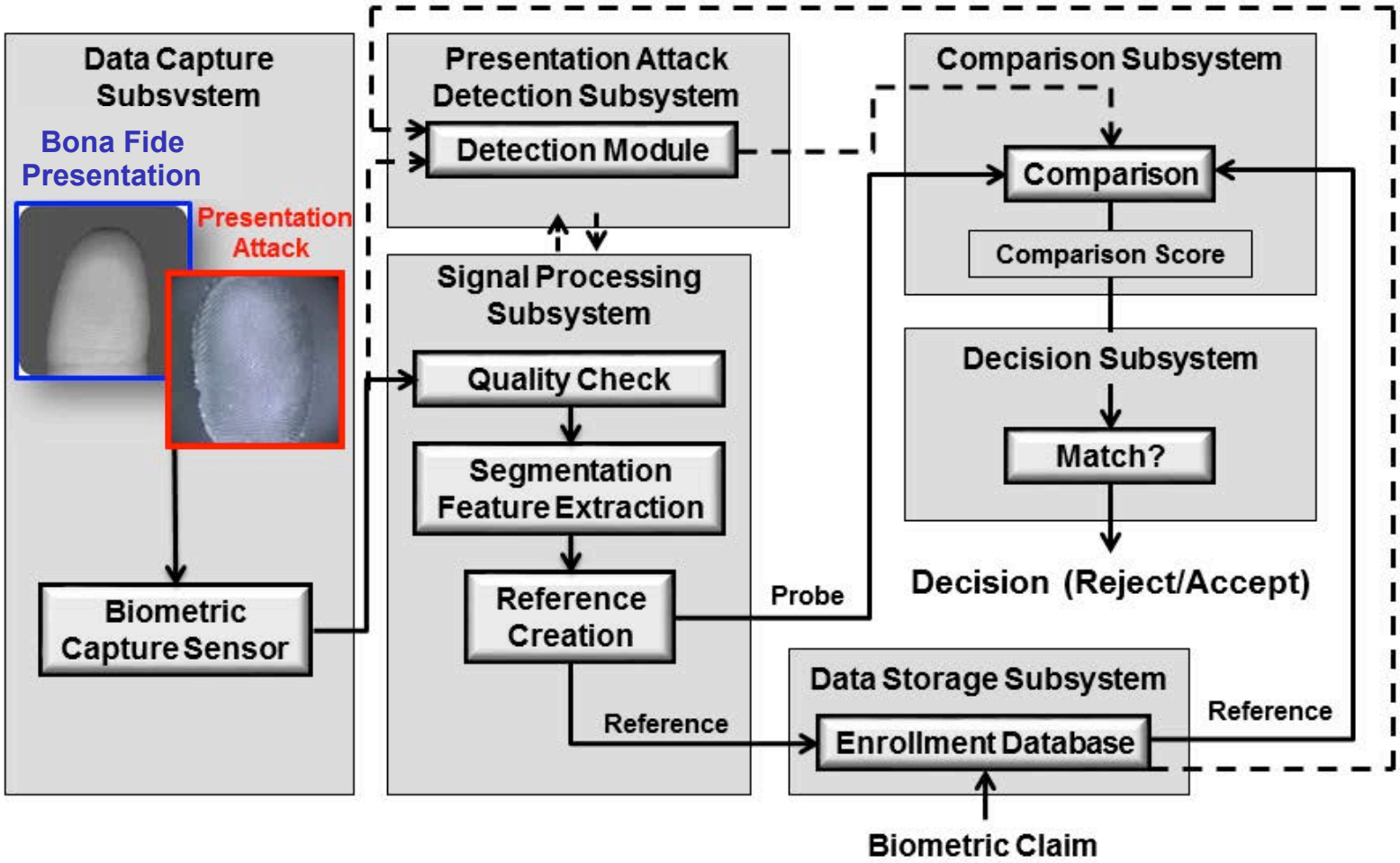
ISO/IEC 30107-1: Examples of Artificial and Human Presentation Attack Instruments

Artificial	*Complete*	gummy finger, video of face
	Partial	glue on finger, sunglasses, artificial/patterned contact lens
Human	*Lifeless*	cadaver part, severed finger/hand
	Altered	mutilation, surgical switching of fingerprints between hands and/or toes
	Non-Conformant	facial expression/extreme, tip or side of finger
	Coerced[1]	unconscious, under duress
	Conformant	zero effort impostor attempt

Source: ISO/IEC 30107-1

Presentation Attack Detection

Biometric framework with PAD



Source: ISO/IEC 30107-1

Presentation Attack Detection

ISO/IEC 30107 - Part 3

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- **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

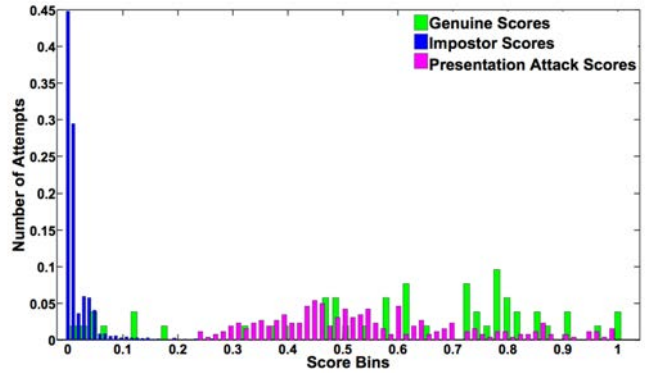


Image Source: K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE TIFS, June 2015

- **Concealer attack presentation non-match rate (CAPNMR)**
  in a full-system evaluation of a verification system, the proportion of concealer attack presentation using the same PAI species in which the target reference is not matched.

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem:

- **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 in ISO/IEC 30107-3

- Testing the PAD subsystem:

- **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

- Testing the PAD subsystem:

- **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

$$APCER_{PAIS} = 1 - \left(\frac{1}{N_{PAIS}}\right) \sum_{i=1}^{N_{PAIS}} Res_i$$

Source: ISO/IEC 30107-3

- *N_{PAIS} is the number of attack presentations for the given PAI species*
- *Res_i takes value 1 if the ith presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem with different species:

- **Attack presentation classification error rate (APCER)** *the highest APCER (i.e. that of the most successful PAI species) should be reported as follows:*

$$APCER_{AP} = \max_{PAIS \in \mathcal{A}_{AP}} (APCER_{PAIS})$$

Source: ISO/IEC 30107-3

where A_{AP} is a subset of PAI species with attack potential at or below AP.

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- **Bona fide presentation classification error rate (BPCER)**
  BPCER shall be calculated as follows:

$$BPCER = \frac{\sum_{i=1}^{N_{BF}} RES_i}{N_{BF}}$$

Source: ISO/IEC 30107-3

- *N_{BF} is the number of bona fide presentations*
- *Res_i takes value 1 if the it^h presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- **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

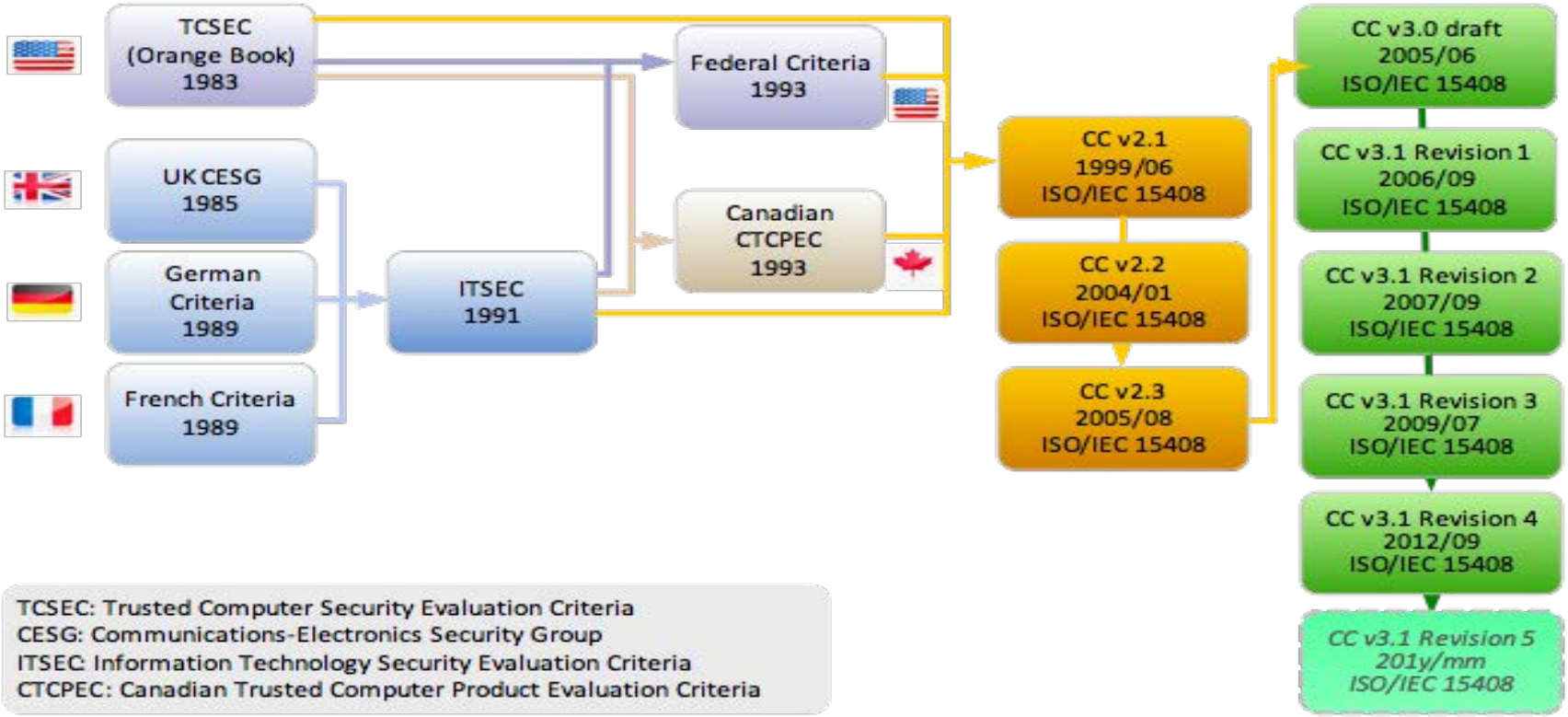
Presentation Attack Detection

ISO/IEC 19989

Common Criteria

Common („joint“) criteria

- for evaluation and assessment of IT-security technology



Presentation Attack Detection - Security

ISO/IEC WD 19989

- Calculating attack potential (in Annex C.4)
  - Overall rating for elapse time
  - Overall rating for expertise
  - Overall rating for knowledge of TOE
  - Overall rating for window of opportunity
  - Overall rating for equipment
- Example

Table C.2 — Overall factor rating for knowledge of TOE

Ratings for phases (unorderd)			Total factor rating
Public	Public	Public	Public
Restricted	Public	Public	Restricted
Restricted	Restricted	Public/ Restricted	At least Restricted (consider interim values)
Sensitive	Public	Public	Sensitive
Sensitive	Restricted/ Sensitive	Public/ Restricted/ Sensitive	At least Sensitive (consider interim values)
Critical	Any	Any	Critical

Source: ISO/IEC WD 19989

Presentation Attack Detection - Security

ISO/IEC WD 19989

- Rating of attack (in Annex C.4.2.1.3)
- *The overall rating for the attack is 4, which means, that the attack would have to be considered in penetration testing for all evaluations assuming Minimum attack potential or higher.*
- *If penetration tests show that the attack would be successful, the TOE would fail to resist against that attack potential.*

Table C.5 — Rating for attack example 1 Source: ISO/IEC WD 19989

Factors	Rating			
	Phase (1)	Phase (2)	Phase (3)	Overall
Elapsed Time	< 1 day (wood glue PAIs would be the first PAIs to try, biometric characteristic is already available)	1 week (creating PAIs and exercising takes some time)	Few seconds (attack can be performed quickly)	One week (1)
Expertise	Layman (wood glue PAIs are probably the first in mind, wood glue can be found in stores)	Layman (because wood glue PAIs are easy to create)	Layman (performing the attack does not need much expertise)	Layman (0)
Knowledge of TOE	Public (wood glue PAIs are known to work quite well for general presentation attack detection systems)	Public (manuals for creating wood glue PAIs can be found in the Internet)	Public (no knowledge needed to perform the attack)	Public (0)
Window of Opportunity	Unnecessary (no access to TOE needed)	Easy (good access to TOE available)	Easy (because of the high chance that the PAI will work)	Easy (1)
Equipment	Standard (no equipment needed)	Standard (2 points, as it is necessary to buy the TOE)	Standard (no equipment needed)	Standard (2)
Overall attack rating			Sum	4

Presentation Attack Detection

Application area - Mobile Biometric Transactions

Smartphone Access Control

Finger recognition study - 2012/2013

- Observation
  - significant strong light reflection near the fingertip
  - from the cameras LED
- Reflection depends on
  - Shape of the finger
  - Consistency of the finger
  - Angle of the finger to the camera

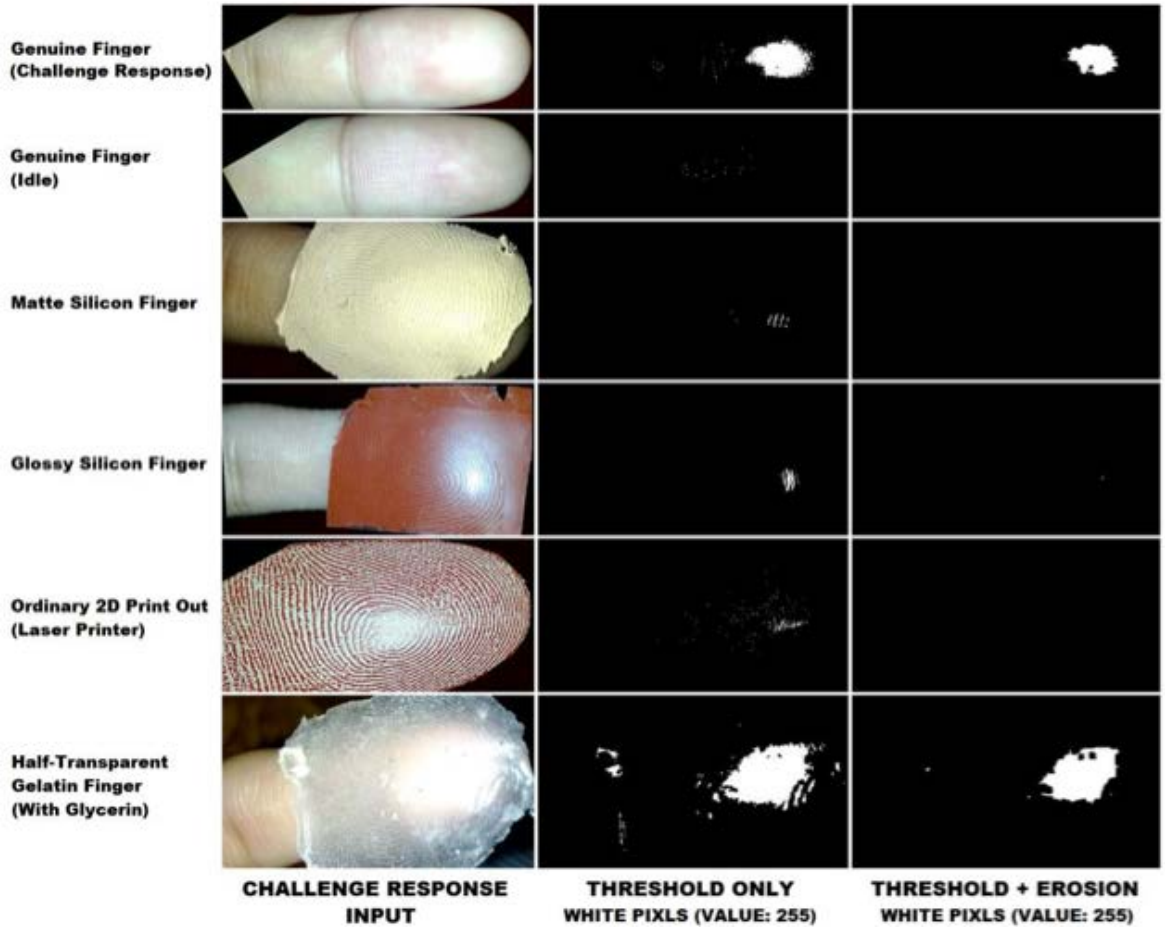
- Attack detection, as light reflection differs from artefacts to Bona Fide fingers

[SBB13] C. Stein, V. Bouatou, C. Busch, „Video-based Fingerphoto Recognition with Anti-spoofing Techniques with Smartphone Cameras“, Proceedings 12th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2013)

Smartphone Access Control - with PAD

Finger recognition study - 2012/2013

- Results: Presentation Attack Detection (PAD)



Eye Recognition Security - with PAD

Eye recognition study - 2015

- Presentation Attack Detection (PAD) videos on iPhone 5 S and Nokia 1020

- Method based on Eulerian Video Magnification (EVM)
  - Normalized Cumulative Phase Information

Eye Recognition Security - with PAD

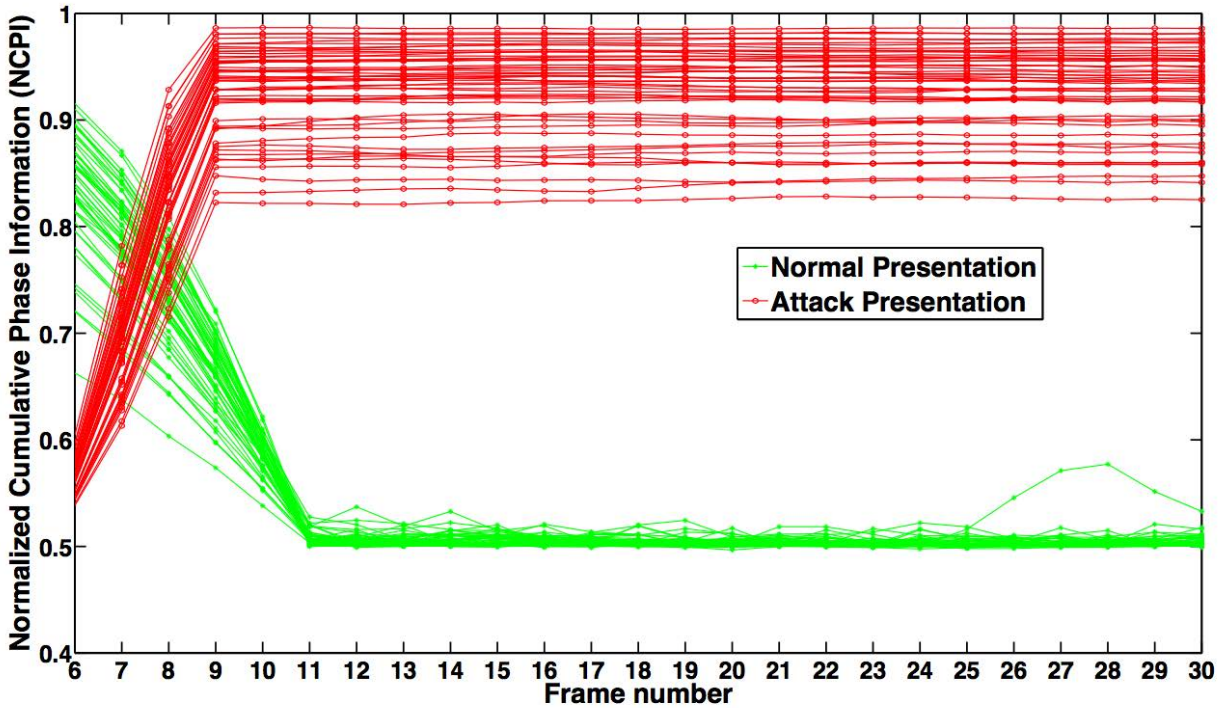
Method based on Eulerian Video Magnification (EVM)

[RRB2015] K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE Transactions on Information Forensics and Security (TIFS), June, (2015)

Eye Recognition Security - with PAD

Eye recognition study - 2015

- Method based on Eulerian Video Magnification (EVM)
  - Normalized Cumulative Phase Information
- Zero Error Rates:
  - APCER = 0 %
  - BPCER = 0 %



[RRB2015] K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE Transactions on Information Forensics and Security (TIFS), June, (2015)

PAD-Standard and FIDO

FIDO liaison with ISO/IEC

- established in February 2017 **RESOLUTION G.30 –**
  - **Establishment of Category A Liaison with FIDO Alliance**
    SC 37 approves the establishment of the Category A liaison with FIDO Alliance, and invites Adam Powers (FIDO Alliance representative) to attend the July 2017 SC 37 Meeting in Takamatsu, Japan.
- New project ISO/IEC 30107-4
  - Scope:
    - guidance for Presentation Attack Detection evaluation of personal mobile devices with local biometric authentication;
    - biometric modules for mobile devices;
    - closed system with no access to internal results;
    - definition of a minimum PAI species
    - definition of a minimum number of subjects

Source: ISO/IEC SC37 - 2017

Application area - Identity Concealer

Altered Fingerprint Detection - Testing

Example for fingerprint alterations

- Z-shaped alteration (Finger of Jose Izquierdo, 1997)

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

Altered Fingerprint Detection - Testing

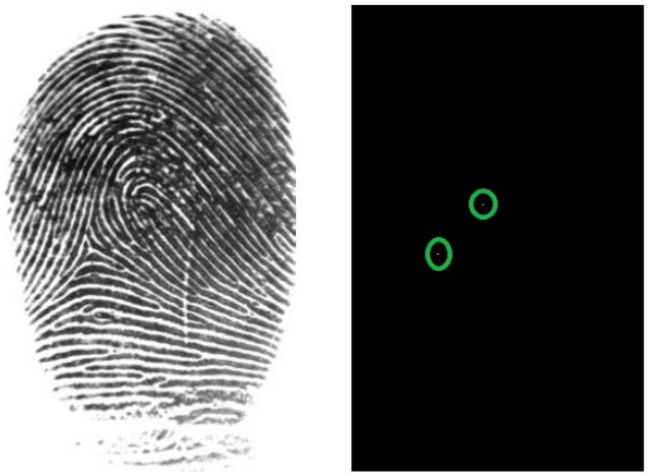
Example for fingerprint alterations

- Left middle finger of Gus Winkler (Bank robber in the 1930s)

Image Source: H. Cummins, “Attempts to alter and obliterate finger-prints,” Journal of Criminal Law and Criminology, vol. 25, pp. 982–991, May 1935.

Altered Fingerprint Detection - Algorithms

- Feature: SPDA
- Singular Point Density Analysis [Ellingsg2014]
- using the Poincare´ index to detect noisy friction ridge areas



BonaFide fingerprint

altered fingerprint

Poincare´ index response

[Ellingsg2014] J. Ellingsgaard, C. Sousedik, and C. Busch, “Detecting fingerprint alterations by orientation field and minutiae orientation analysis,” in Proc. IWBF, Valletta, Malta, (2014)

Altered Fingerprint Detection - Testing

Database

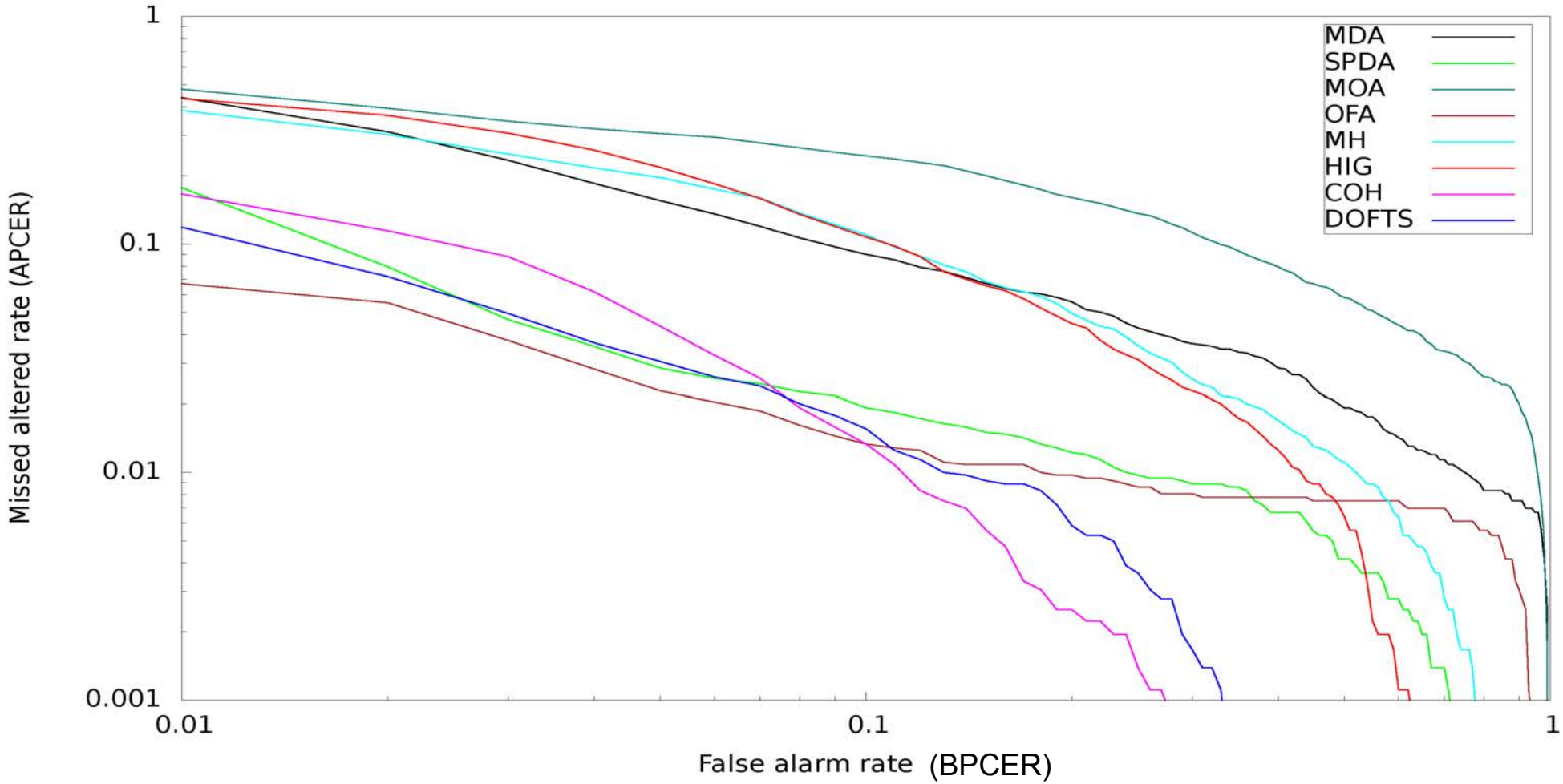
- Dataset of Ellingsgaard et al. [Ellingsg2014]
  - Size: 116 altered fingerprints and 180 unaltered fingerprints
  - This data is not of sufficient size !

- Sources:
  - subset of GUC-100 (NTNU)
  - subset of Samischenko (Book)
  - subset of Brno (collection of fingerprints with dermatological diseases)
  - subset of NIST Special Database 14

[Ellingsg2014] J. Ellingsgaard, C. Sousedik, and C. Busch, “Detecting fingerprint alterations by orientation field and minutiae orientation analysis,” in Proc. IWBF, Valletta, Malta, (2014)

Altered Fingerprint Detection - Testing

Results [Gottsch2015]



MDA = Minutia Distribution Analysis, SPDA = Singular Point Density Analysis, MOA = Minutia Orientation Analysis, OFA = Orientation Field Analysis, MH = Minutiae Histograms, HIG = Histograms of Invariant Gradients, COH = coherence, DOFTS = Differentials of Orientation Fields by Tensors in Scale,

References

Literature

- [Rag2017] R. Raghavendra, C. Busch: " Presentation Attack Detection methods for Face Recognition System - A Comprehensive Survey“, in ACM Computing Surveys, (2017)
- [Sous2014] C. Sousedik, C. Busch: "Presentation attack detection methods for fingerprint recognition systems: a survey", Journal on Biometrics, IET, (2014)
- [YoonJain2012] S. Yoon, J. Feng, and A. Jain, “Altered fingerprints: Analysis and detection,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, (2012)
- [Ellingsg2014] J. Ellingsgaard, C. Sousedik, and C. Busch, “Detecting fingerprint alterations by orientation field and minutiae orientation analysis,” in Proc. IWBF, Valletta, Malta, (2014)
- [Gottsch2015] C. Gottschlich, A. Mikaelyan, M. Olsen, J. Bigun, C. Busch: „Improving Fingerprint Alteration Detection", in 9th International Symposium on Image and Signal Processing and Analysis (ISPA 2015), Zagreb, (2015)

References

Standards

- ISO/IEC Standards
  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on
- ISO/IEC 30107-1, “Biometric presentation attack detection - Part 1: Framework”, 2016
  http://standards.iso.org/ittf/PubliclyAvailableStandards/c053227_ISO_IEC_30107-1_2016.zip
- ISO/IEC 30107-3, “Biometric presentation attack detection - Part 3: Framework”, 2016
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67381
- ISO/IEC 19989, “Criteria and methodology for security evaluation of biometric systems”
  https://www.iso.org/standard/72403.html?browse=tc
- ISO/IEC 15408: “Security Techniques - Evaluation Criteria for IT Security / Common Criteria“

Contact

CRISP
Center for Research
in Security and Privacy

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Prof. Dr. Christoph Busch
Principal Investigator

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

Telefon +49-6151-16-30090
www.dasec.h-da.de
www.crisp-da.de