Presentation Attack Detection Standards

Christoph Busch
Hochschule Darmstadt - CRISP

TTT Working Group Biometrics
2017-09-20

Presentation Attack Detection

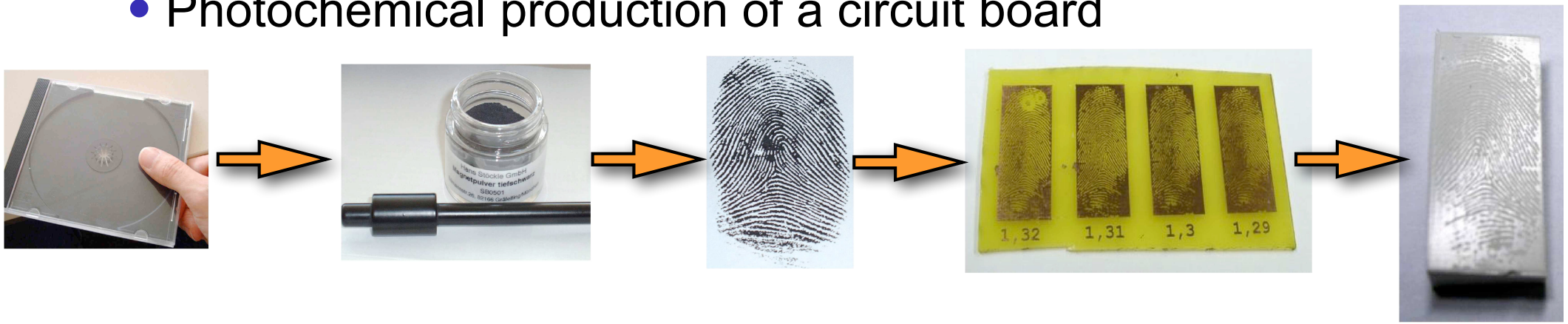
Outline

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

Gummy Finger Production in 2000 !

Attack without support of an enroled individual

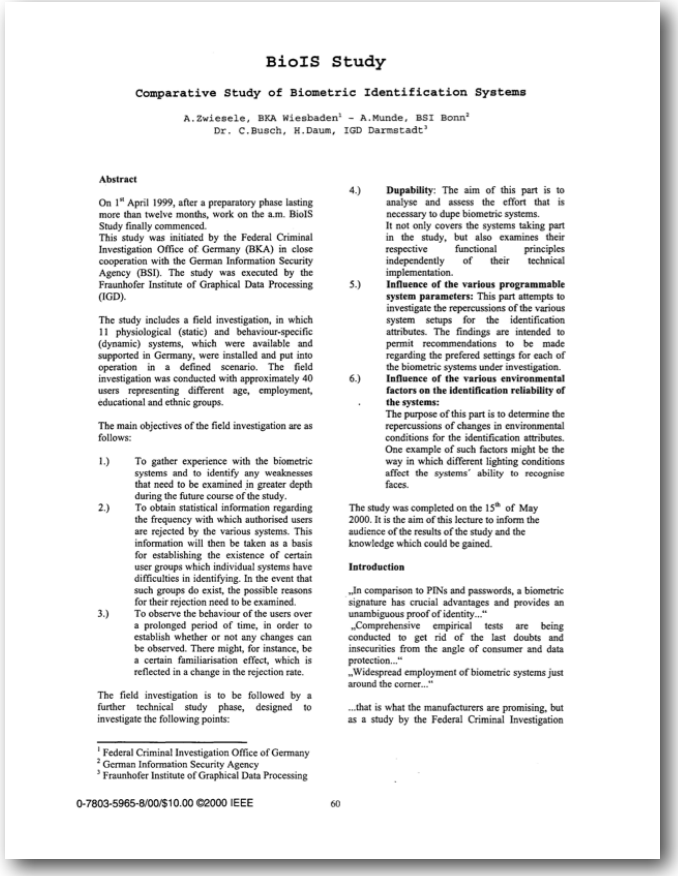
- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
    with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production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



Gummy Finger Production in 2000 !

Reported in a publication by the German Federal Police

- [Zwie2000] A. Zwiesele, A. Munde, C. Busch, H. Daum: "Comparative Study of Biometric Identification Systems", in 34th Annual IEEE International Carnahan Conference on Security Technology, Ottawa, (2000)



BioIS Study

Comparative Study of Biometric Identification Systems

A.Zwiesele, BKA Wiesbaden[1] – A.Munde, BSI Bonn[2]
Dr. C.Busch, H.Daum, IGD Darmstadt[3]

Abstract

On 1st April 1999, after a preparatory phase lasting more than twelve months, work on the a.m. BioIS Study finally commenced.
This study was initiated by the Federal Criminal Investigation Office of Germany (BKA) in close cooperation with the German Information Security Agency (BSI). The study was executed by the Fraunhofer Institute of Graphical Data Processing (IGD).

The study includes a field investigation, in which 11 physiological (static) and behaviour-specific (dynamic) systems, which were available and supported in Germany, were installed and put into operation in a defined scenario. The field investigation was conducted with approximately 40 users representing different age, employment, educational and ethnic groups.

The main objectives of the field investigation are as follows:

1.) To gather experience with the biometric systems and to identify any weaknesses that need to be examined in greater depth during the future course of the study.
2.) To obtain statistical information regarding the frequency with which authorised users are rejected by the various systems. This information will then be taken as a basis for establishing the existence of certain user groups which individual systems have difficulties in identifying. In the event that such groups do exist, the possible reasons for their rejection need to be examined.
3.) To observe the behaviour of the users over a prolonged period of time, in order to establish whether or not any changes can be observed. There might, for instance, be a certain familiarisation effect, which is reflected in a change in the rejection rate.

The field investigation is to be followed by a further technical study phase, designed to investigate the following points:

4.) **Dupability**: The aim of this part is to analyse and assess the effort that is necessary to dupe biometric systems.
It not only covers the systems taking part in the study, but also examines their respective functional principles independently of their technical implementation.
5.) **Influence of the various programmable system parameters:** This part attempts to investigate the repercussions of the various system setups for the identification attributes. The findings are intended to permit recommendations to be made regarding the prefered settings for each of the biometric systems under investigation.
6.) **Influence of the various environmental factors on the identification reliability of the systems:**
The purpose of this part is to determine the repercussions of changes in environmental conditions for the identification attributes. One example of such factors might be the way in which different lighting conditions affect the systems´ ability to recognise faces.

The study was completed on the 15th of May 2000. It is the aim of this lecture to inform the audience of the results of the study and the knowledge which could be gained.

Introduction

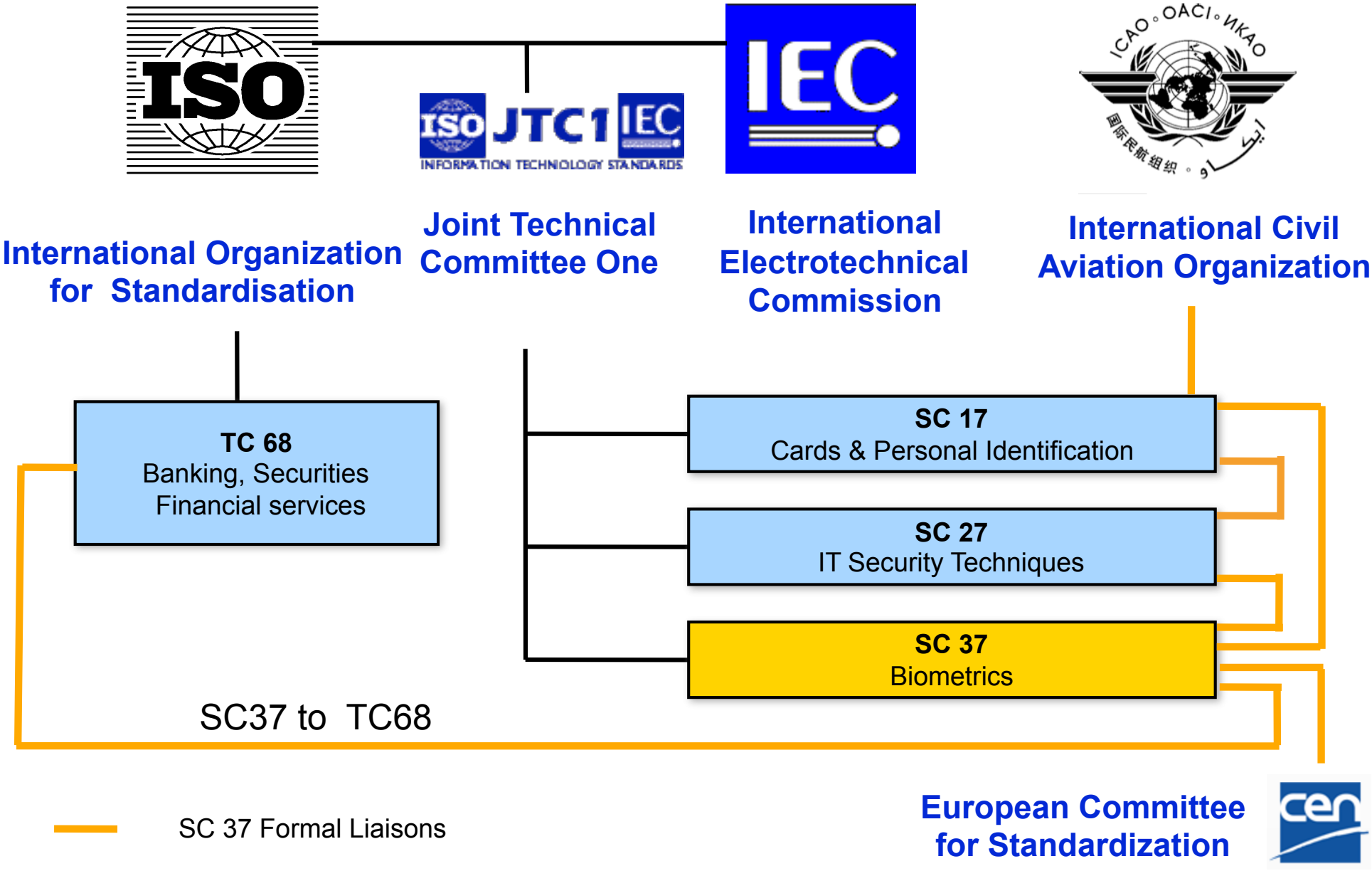
„In comparison to PINs and passwords, a biometric signature has crucial advantages and provides an unambiguous proof of identity..."
„Comprehensive empirical tests are being conducted to get rid of the last doubts and insecurities from the angle of consumer and data protection..."
„Widespread employment of biometric systems just around the corner..."

...that is what the manufacturers are promising, but as a study by the Federal Criminal Investigation

[1] Federal Criminal Investigation Office of Germany
[2] German Information Security Agency
[3] Fraunhofer Institute of Graphical Data Processing

0-7803-5965-8/00/$10.00 ©2000 IEEE

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

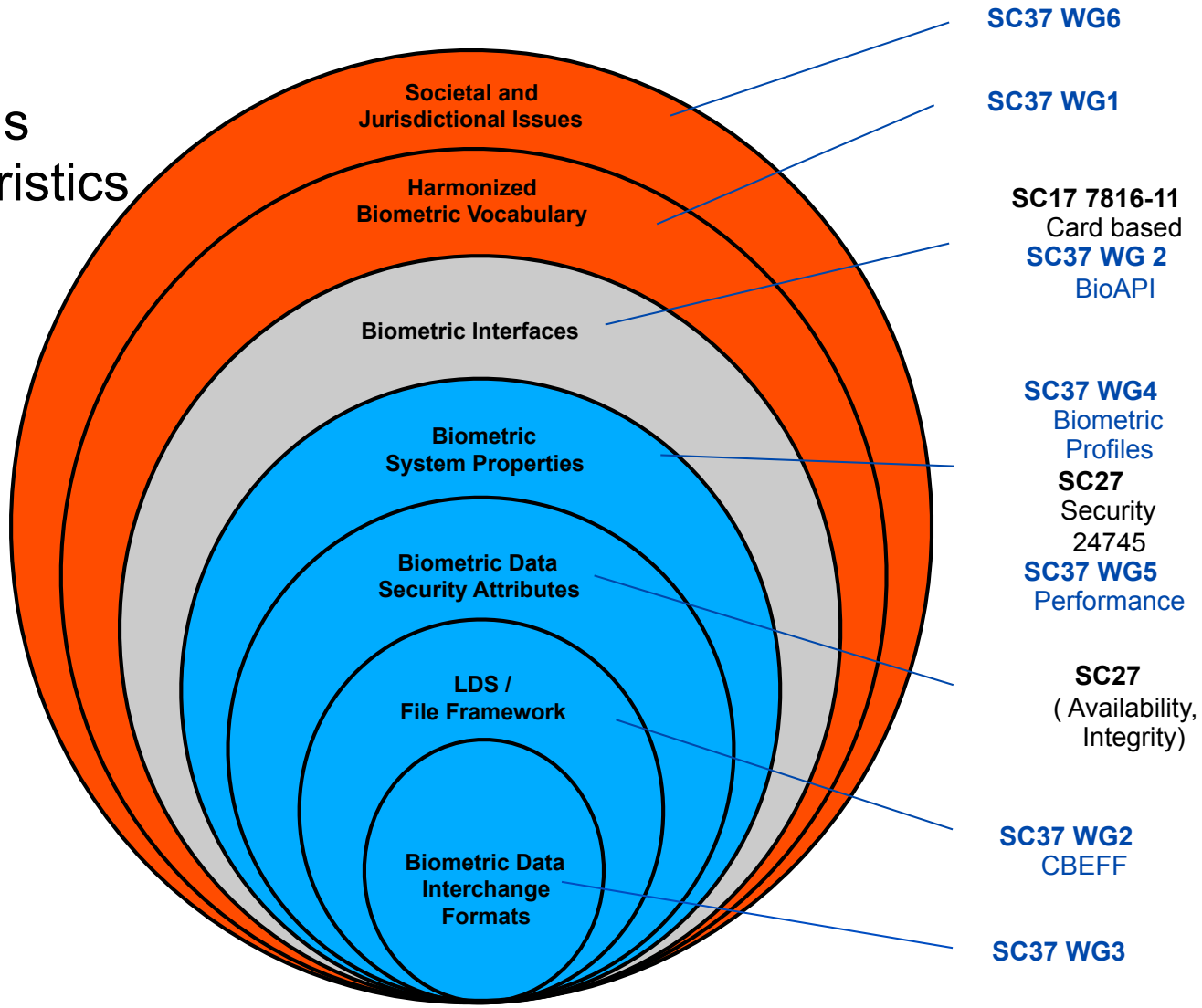
- *"Standardization of generic biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. Generic human biometric standards include: common file frameworks; biometric application programming interfaces; biometric data interchange 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: January, 2018

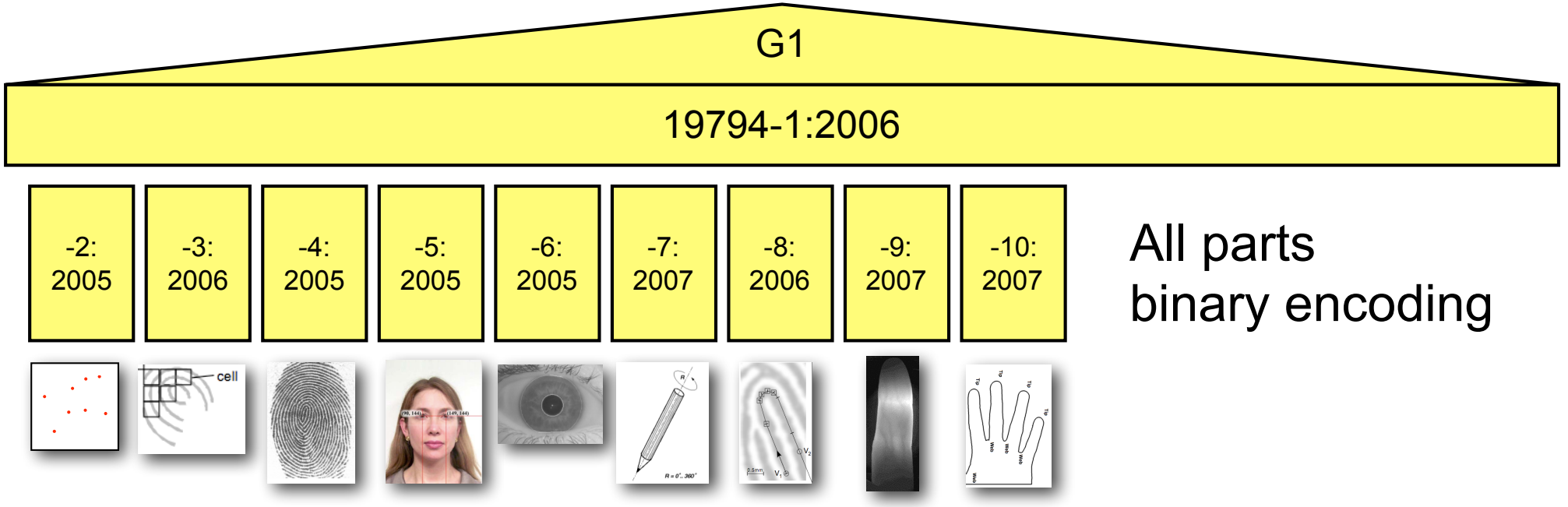
Biometric Standardisation

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



All parts
binary encoding

The 19794-Family: Biometric data interchange formats

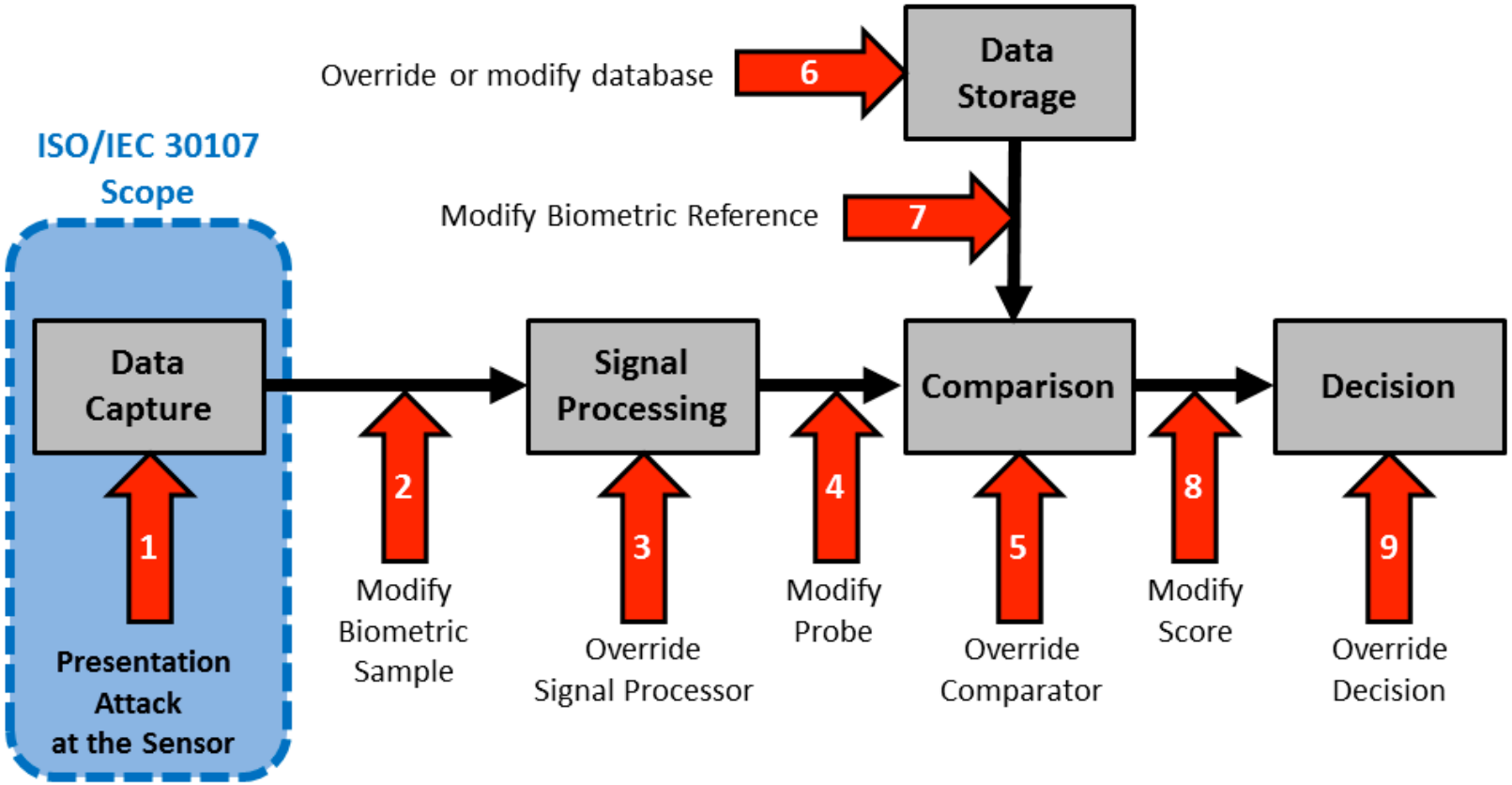
Presentation Attack Detection

ISO/IEC 30107 - Biometric presentation attack detection - Part 1: Framework

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).

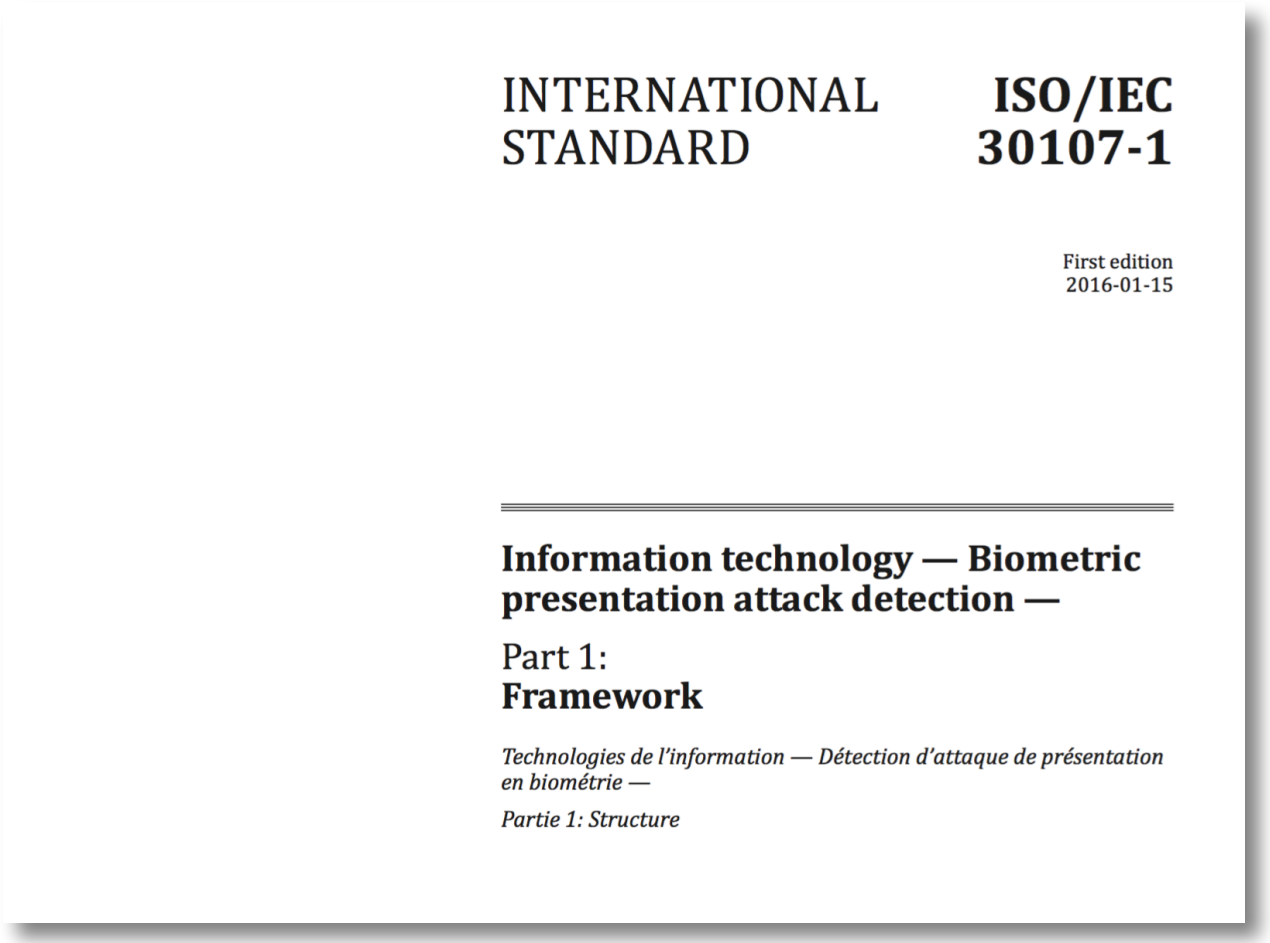
Outside the scope are

- 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

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



INTERNATIONAL STANDARD

ISO/IEC 30107-1

First edition
2016-01-15

Information technology — Biometric presentation attack detection —

Part 1:
Framework

Technologies de l'information — Détection d'attaque de présentation en biométrie —

Partie 1: Structure

Presentation Attack Detection - Framework

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: Definitions

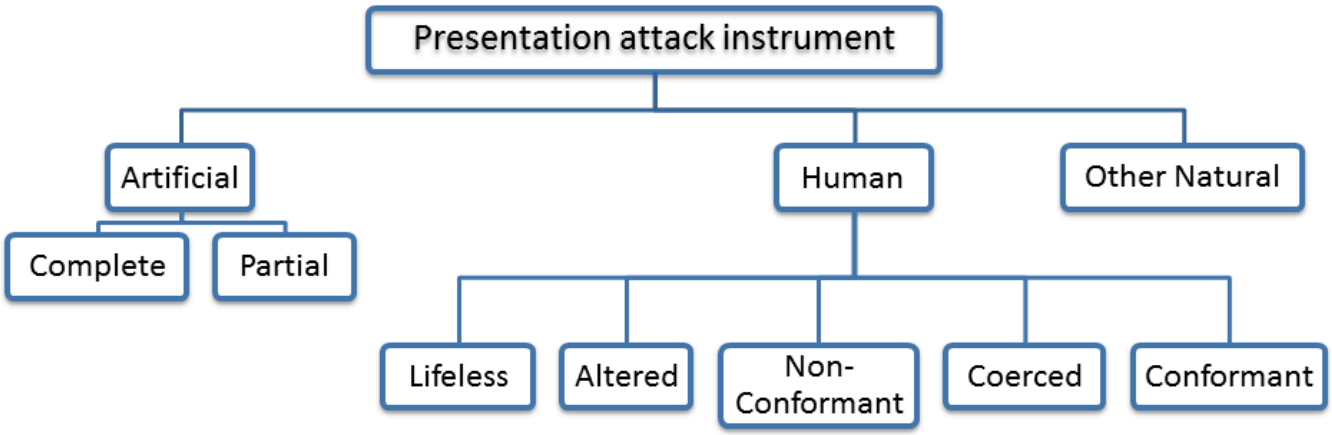
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)



Source: ISO/IEC 30107-1

Presentation Attack Detection - Framework

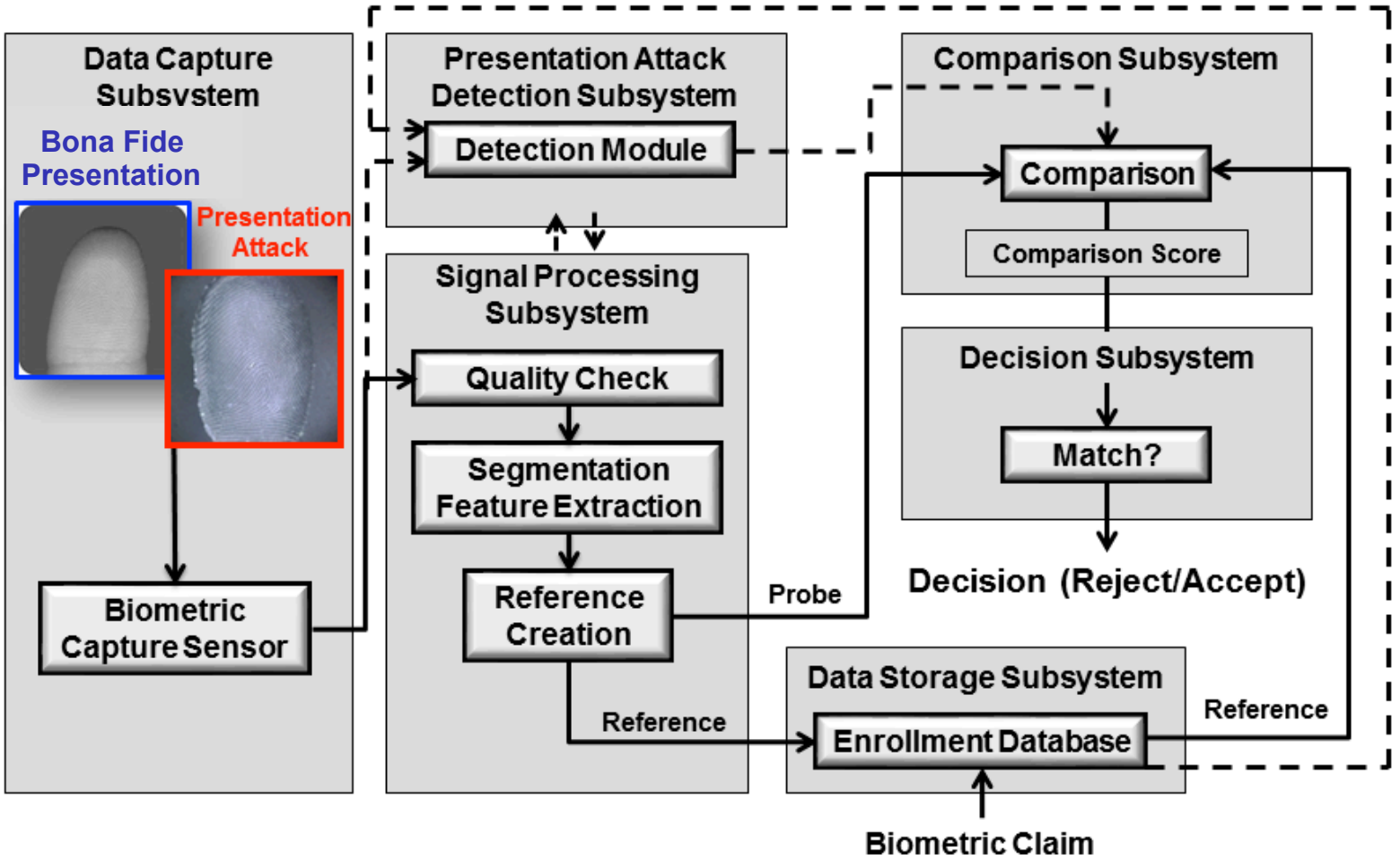
ISO/IEC 30107-1: Examples of Artificial and Human Presentation Attack Instruments

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 - Framework

Biometric framework with PAD



Source: ISO/IEC 30107-1

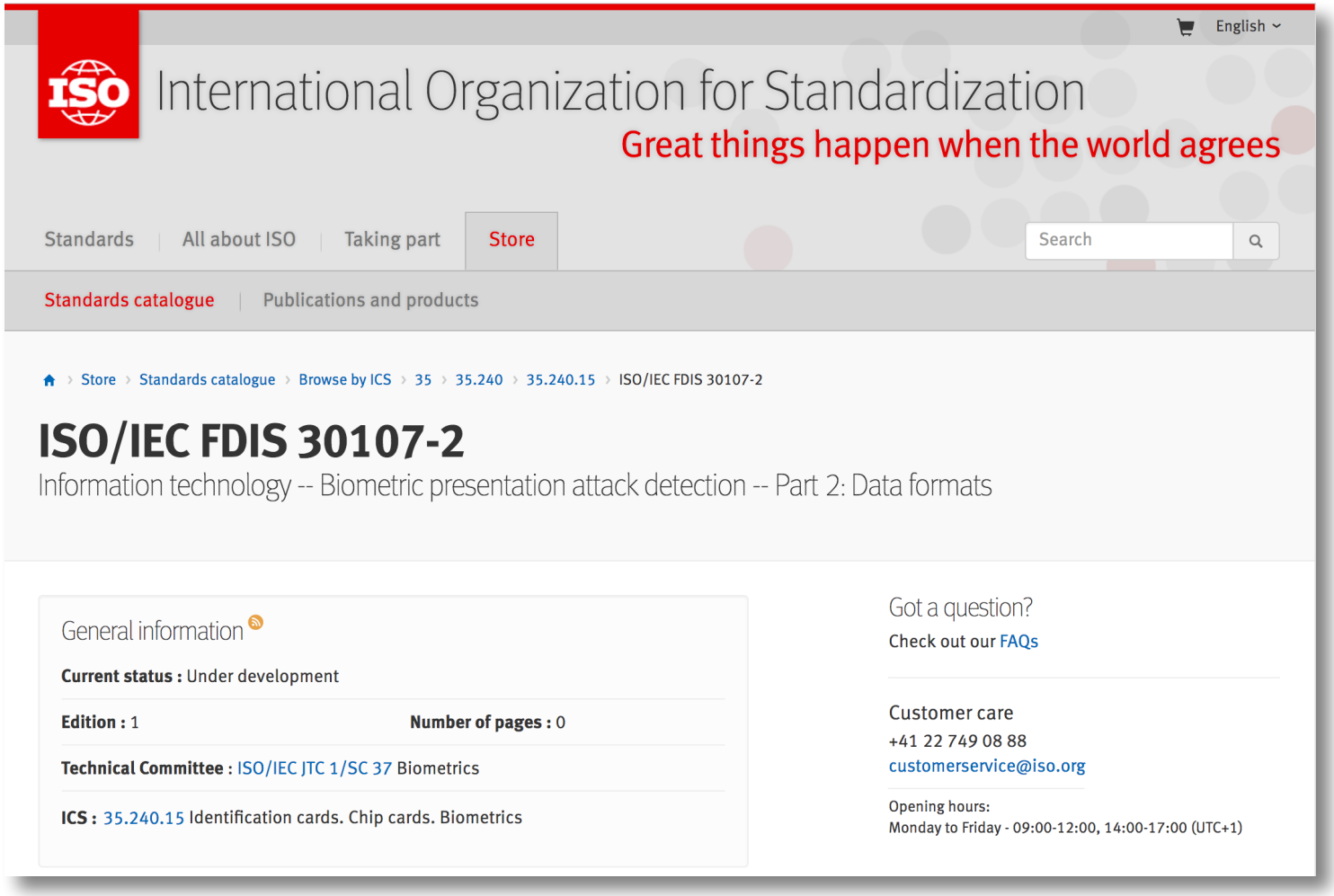
Presentation Attack Detection

ISO/IEC 30107 - Biometric presentation attack detection - Part 2: Data formats

Presentation Attack Detection - Data Formats

ISO/IEC FDIS 30107-2

- will soon be available in the ISO/IEC Portal
  https://www.iso.org/standard/67380.html



Presentation Attack Detection - Data Formats

ISO/IEC FDIS 30107-2

- Abstract syntax of the PAD information in ASN.1

```
PADDataFormatModule
{iso standard 30107 data-formats(2) modules(0) pad-data(0) version(0)}
DEFINITIONS
IMPLICIT TAGS                ::=
BEGIN
    PADData                  ::= [APPLICATION 98] SET {
        pADDecision                  [0] PADDecision                  OPTIONAL,
        pADScoreBlockSequence        [1] PADScoreBlockSequence        OPTIONAL,
        pADExtendedDataSequence      [2] PADExtendedDataSequence      OPTIONAL,
        captureContext               [3] CaptureContext               OPTIONAL,
        supervisionLevel             [4] SupervisionLevel             OPTIONAL,
        riskLevel                    [5] RiskLevel                    OPTIONAL,
        criteriaCategory             [6] CriteriaCategory             OPTIONAL,
        pADParameter                 [7] PADParameter                 OPTIONAL,
        pADChallenge                 [8] PADChallenge                 OPTIONAL,
        pADDataCaptureDateTime       [9] GeneralizedTime              OPTIONAL,
        captureDevice                [10] CaptureDevice               OPTIONAL,
        ...
    }
```

Source: ISO/IEC 30107-2

Presentation Attack Detection - Data Formats

ISO/IEC FDIS 30107-2

- PAD score

5.2.4 PAD score

Presence:	Optional
Abstract values:	Integers 0 to 100 and FAILURE_TO_COMPUTE
Contents:	If present, this data element shall indicate the PAD result as a score between 0 and 100. Bona-fide presentations shall tend to generate lower scores. Presentation attacks shall tend to generate higher scores. The abstract value FAILURE_TO_COMPUTE shall indicate that the computation of the PAD score has failed. If the PAD score value is FAILURE_TO_COMPUTE, then, if present, the PAD decision value shall also be FAILURE_TO_COMPUTE.

Source: ISO/IEC 30107-2

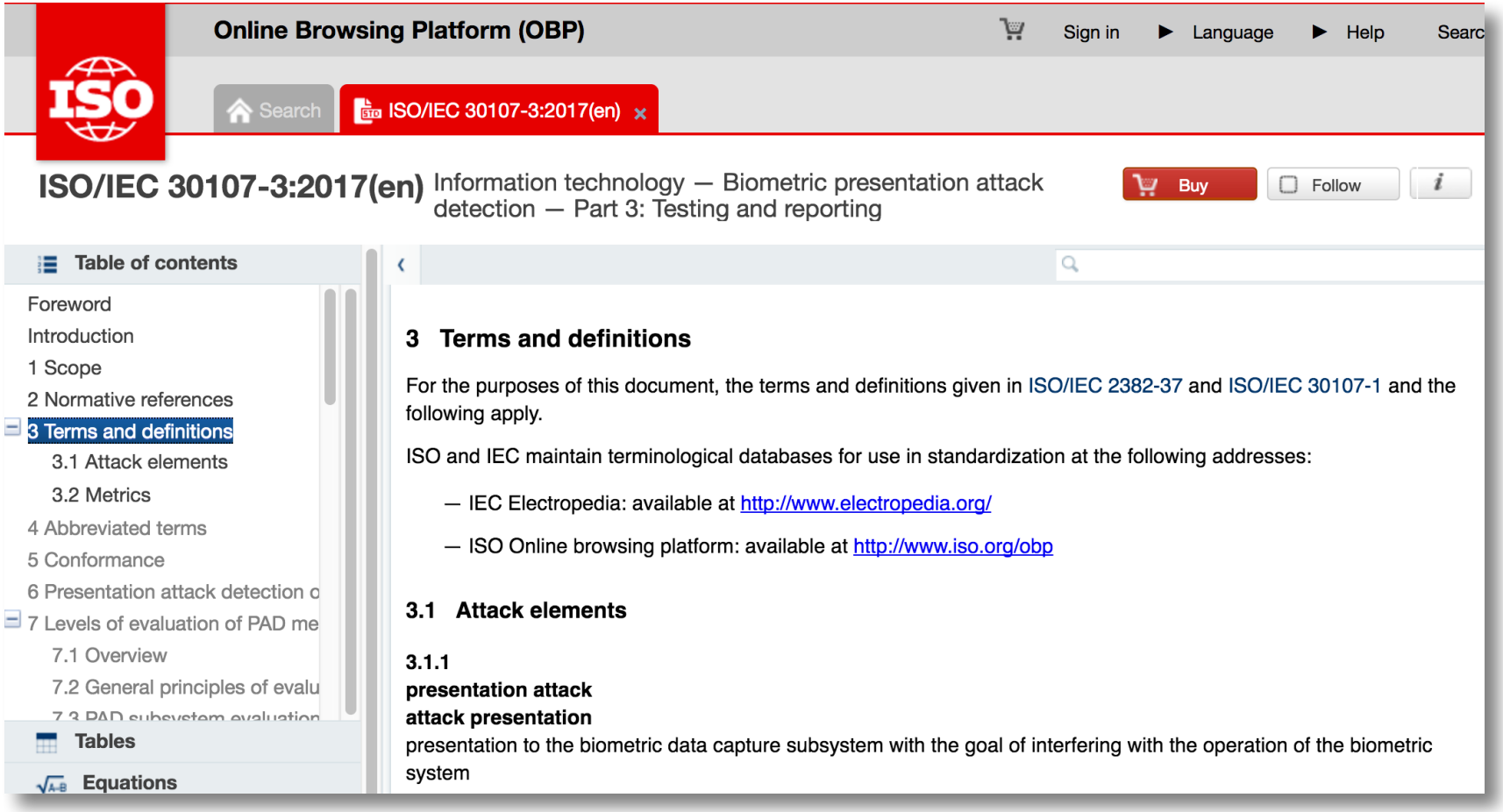
Presentation Attack Detection

ISO/IEC 30107 - Biometric presentation attack detection -
Part 3: Testing and reporting

Presentation Attack Detection - Testing

ISO/IEC 30107-3

- available in the ISO/IEC Portal
  https://www.iso.org/obp/ui/#iso:std:iso-iec:30107:-3:ed-1:v1:en

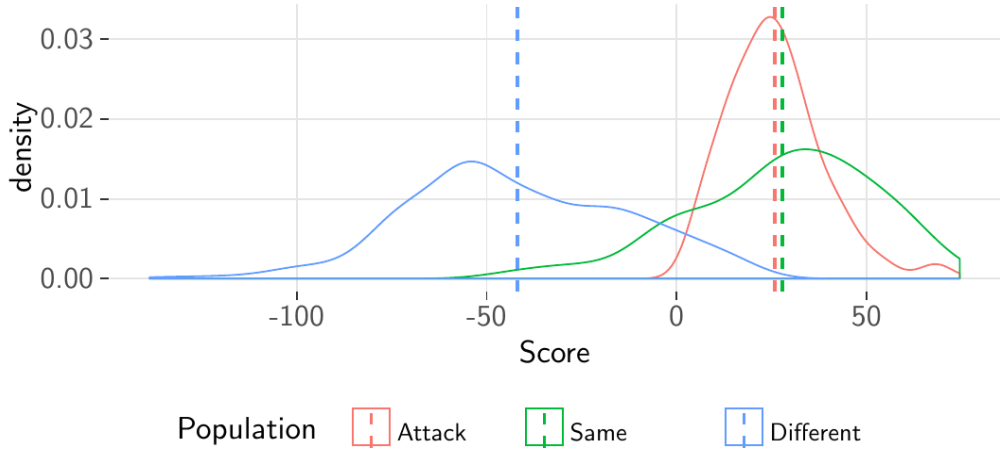


Presentation Attack Detection - Testing

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



- **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 metrics testing the PAD subsystem response:

- **Attack presentation non-response rate (APNRR)**
  proportion of attack presentations using the same PAI species that cause no response at the PAD subsystem or data capture subsystem

- **Bona fide presentation non-response rate (BPNRR)**
  proportion of bona fide presentations that cause no response at the PAD subsystem or data capture subsystem
  - *NOTE An example of a non-response is a data capture subsystem "time out" if a presentation is not registered within a certain amount of time.*

Source: ISO/IEC 30107-3

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with security measure and convenience measure:

- **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 detection capabilities metrics

- Testing the PAD subsystem with security measure:

- **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* i^{th} *presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing the PAD subsystem with security measure:

- **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 detection capabilities metrics

- Testing the PAD subsystem with convenience measure:

- **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

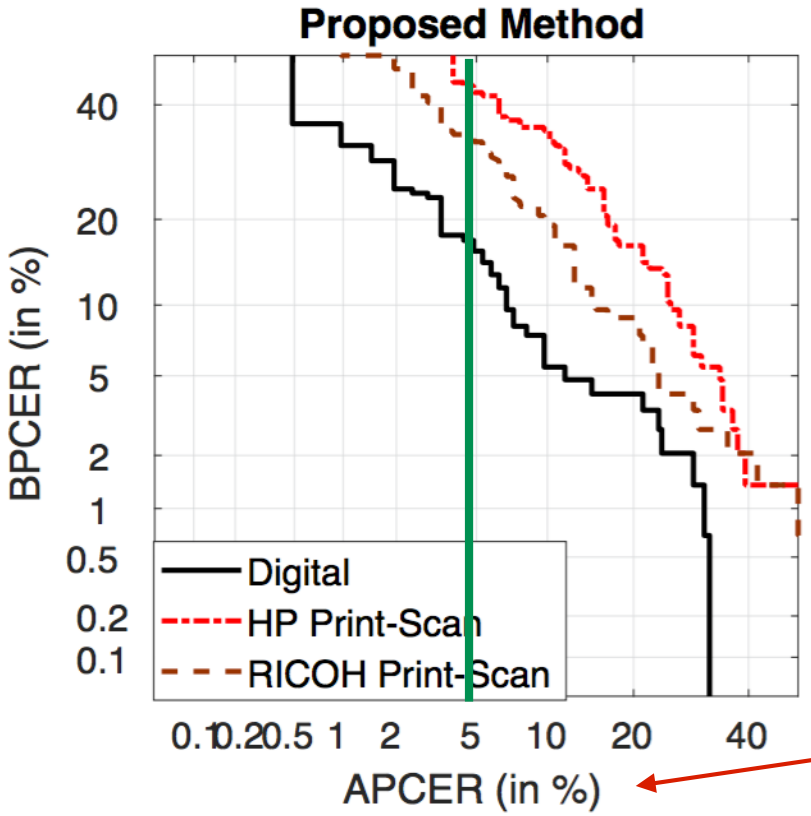
- N_{BF} *is the number of bona fide presentations*
- Res_i *takes value 1 if the* it^h *presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- DET curve analyzing operating points for various security measures and convenience measures
- Example:

convenience measure



security measure (strenght of function)

Source: IR. 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

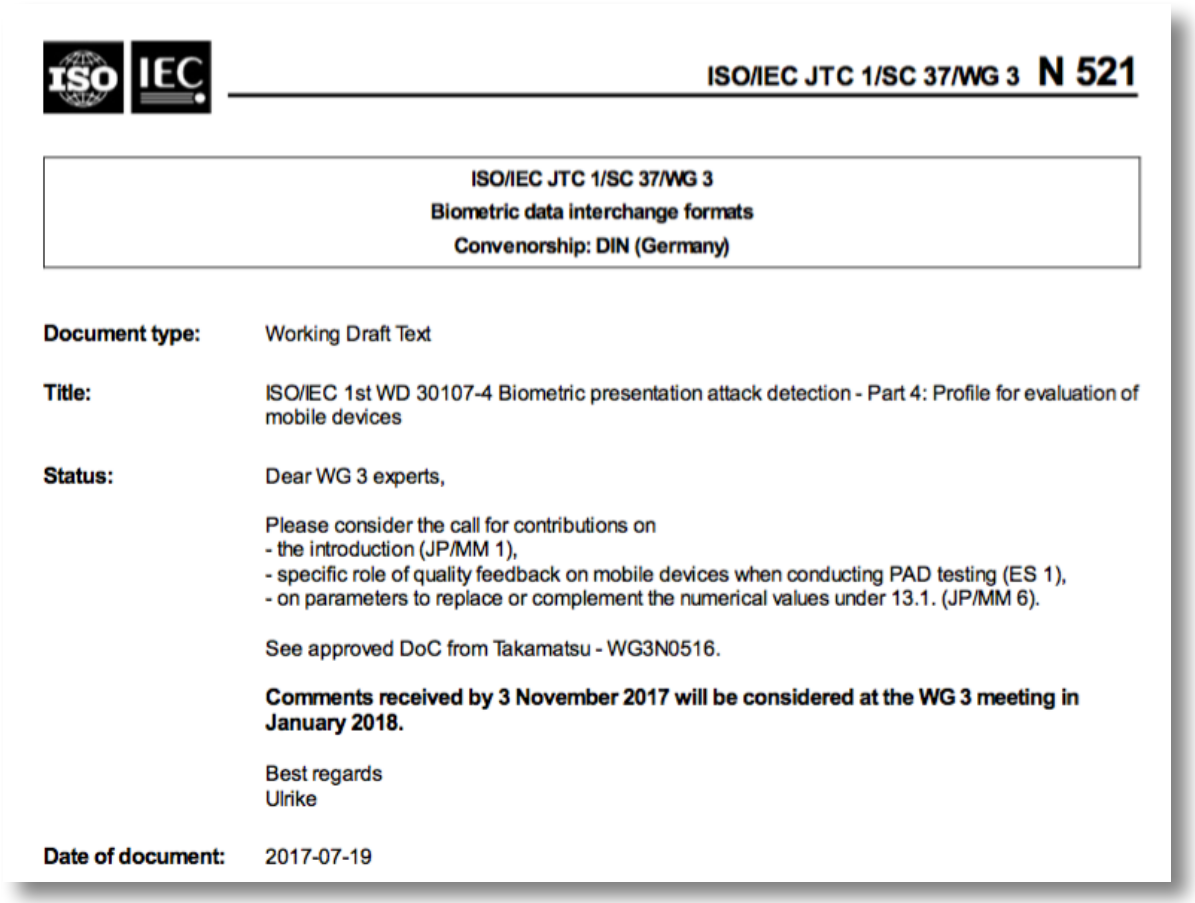
Presentation Attack Detection

ISO/IEC 30107 - Biometric presentation attack detection -
Part 4: Testing and reporting

Presentation Attack Detection - Mobile

ISO/IEC WD 30107-4

- Profile for testing and reporting on mobile devices
- Working Draft available in the ISO/IEC livelink
  http://isotc.iso.org/livelink/livelink?func=ll&objId=19121718&objAction=Open&viewType=1



ISO/IEC JTC 1/SC 37/WG 3 **N 521**

ISO/IEC JTC 1/SC 37/WG 3
Biometric data interchange formats
Convenorship: DIN (Germany)

Document type: Working Draft Text

Title: ISO/IEC 1st WD 30107-4 Biometric presentation attack detection - Part 4: Profile for evaluation of mobile devices

Status: Dear WG 3 experts,

Please consider the call for contributions on
- the introduction (JP/MM 1),
- specific role of quality feedback on mobile devices when conducting PAD testing (ES 1),
- on parameters to replace or complement the numerical values under 13.1. (JP/MM 6).

See approved DoC from Takamatsu - WG3N0516.

Comments received by 3 November 2017 will be considered at the WG 3 meeting in January 2018.

Best regards
Ulrike

Date of document: 2017-07-19

Presentation Attack Detection - Mobile

ISO/IEC WD 30107-4

- Scope:
  - *This standard provides guidance for testing biometric presentation attack detection mechanisms on mobile devices with local biometric authentication.*
  - *The standard considers: specification of a minimum PAI species and specification of a minimum number of subjects*
- Example:

30107-3 Clause	Requirement	Approach in PAD Tests for Mobile Devices
13.1	Evaluations of PAD mechanisms shall report the following:	Evaluator provides the basis and narrative. Notional values provided in the rows below:
	— number of presentation attack instruments used in the evaluation	Evaluator documents this figure based on number of IUTs, subjects, species, and series
	— number of PAI species used in the evaluation	Minimum of 3
	— number of PAI series used in the evaluation	Minimum of 3 per species
	— number of test subjects involved in the testing, including those unable to utilize artefacts or present non-conformant characteristics	Minimum of 50
	— number of artefacts created per test subject for each material tested	Minimum of 3
	— number of sources from which artefact characteristics were derived	Evaluator provides basis and narrative

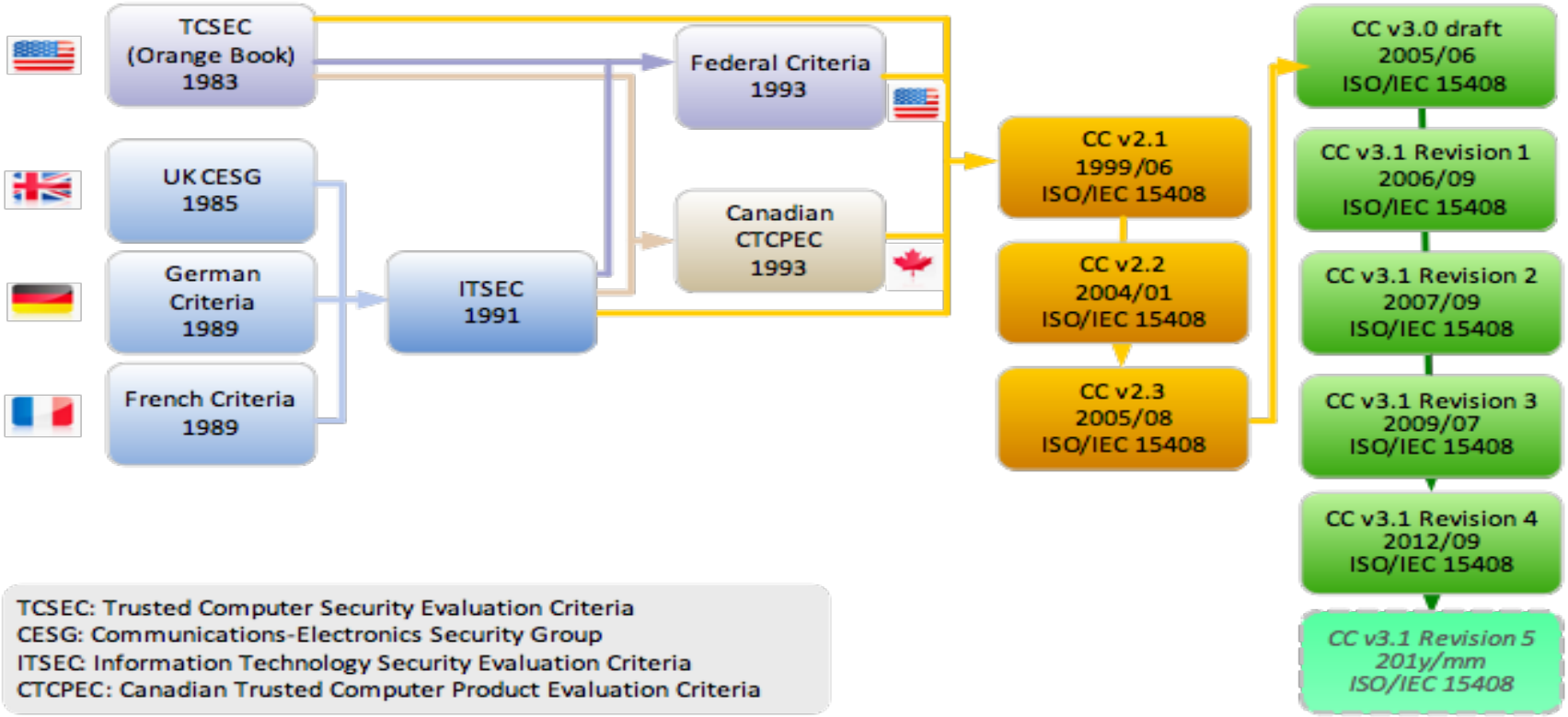
Presentation Attack Detection

ISO/IEC 19989

Common Criteria

Common („joint“) criteria

- for evaluation and assessment of IT-security technology



Presentation Attack Detection - Security

ISO/IEC 19989 - Criteria and methodology for security evaluation of biometric systems

- Part 1: Framework
  https://www.iso.org/standard/72402.html
- Part 2: Biometric recognition performance
  https://www.iso.org/standard/72403.html
- Part 3: Presentation attack detection
  https://www.iso.org/standard/73721.html
- Scope:
  For security evaluation of biometric recognition performance and presentation attack detection for biometric systems, this International Standard specifies:
  - *Extended security functional components to SFR Classes in ISO/IEC 15408-2,*
  - *Complements to methodology specified in ISO/IEC 18045 for SAR Classes of ISO/IEC 15408-3.*

Presentation Attack Detection - Security

ISO/IEC 2nd WD 19989-1

- Calculating attack potential (in Annex A.3.3)
  - 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 A.1 — Calculation of attack potential

Factor	Value	
	Identification	Exploitation
Elapsed Time		
<= one day	0	0
<= one week	1	2
<= two weeks	2	4
<= one month	4	8
> one month	8	16
Expertise		
Layman	0	0
Proficient	2	4
Expert	4	8
Multiple experts	8	Not applicable

Source: ISO/IEC 2nd WD 19989-1

Presentation Attack Detection - Security

ISO/IEC 2nd WD 19989-1

- Example calculating attack potential

Knowledge of TOE		
Public	0	Not applicable
Restricted	2	Not applicable
Sensitive	4	Not applicable
Critical	8	Not applicable
Window of Opportunity (Access to TOE)		
Easy	0	0
Moderate	2	4
Difficult	4	8
Immediate	Not applicable	0
Window of Opportunity (Access to Biometric Characteristics)		
Easy	Not applicable	2
Moderate	Not applicable	4
Difficult	Not applicable	8
Equipment		
Standard	0	0
Specialised	2	4
Bespoke	4	8

Source: ISO/IEC 2nd WD 19989-1

Presentation Attack Detection - Security

ISO/IEC 2nd WD 19989-3

- Relation among error rates, presentation type, and attack classification for PAD subsystem

Presentation Type (Input)	**PAD Result (Output)**		
	Attack	**Normal**	**No-response**
Attack	---	APCER	APNRR
Bona Fide	BPCER	---	BPNRR

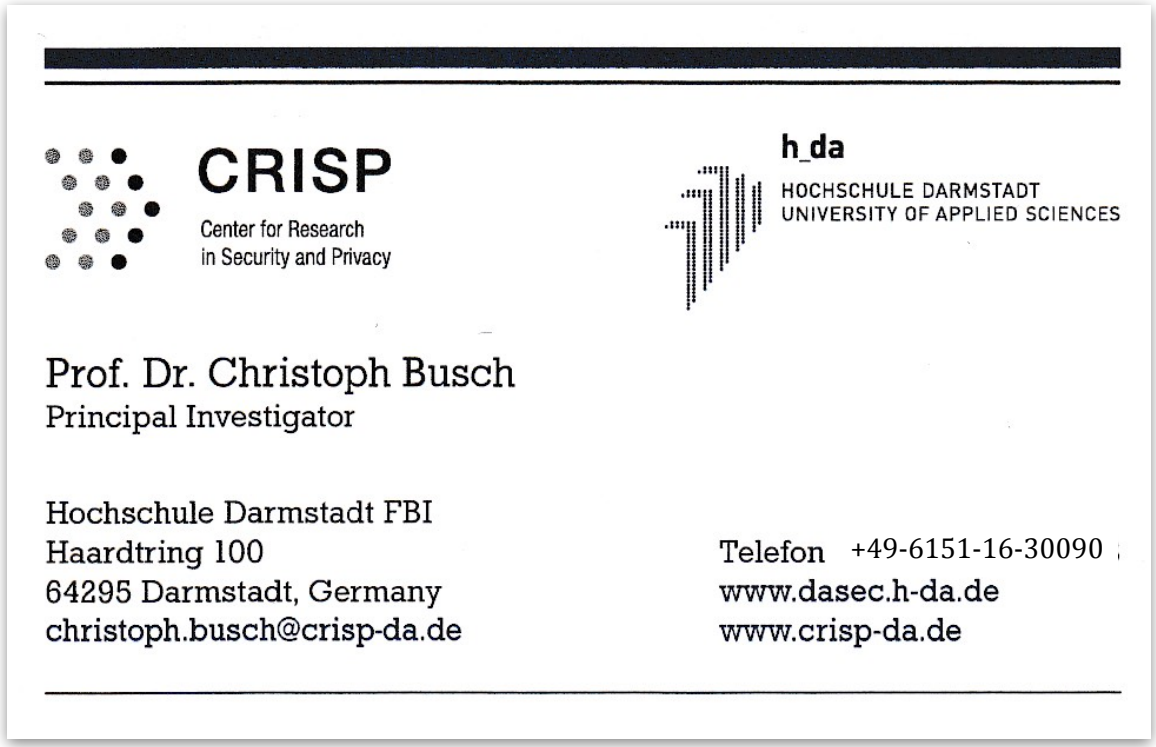
Source: ISO/IEC 2nd WD 19989-3

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”, 2017
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=67381
- ISO/IEC 2nd WD 19989-1, “Criteria and methodology for security evaluation of biometric systems - Part 1: Framework”
  https://www.iso.org/standard/72402.html
- ISO/IEC 2nd WD 19989-3, “Criteria and methodology for security evaluation of biometric systems - Part 3: Presentation attack detection
  https://www.iso.org/standard/73721.html
- 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