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

EAB-ICAO-Workshop, July 1st, 2024

NTNU

European Association for Biometrics
eab
Human Identity in Europe

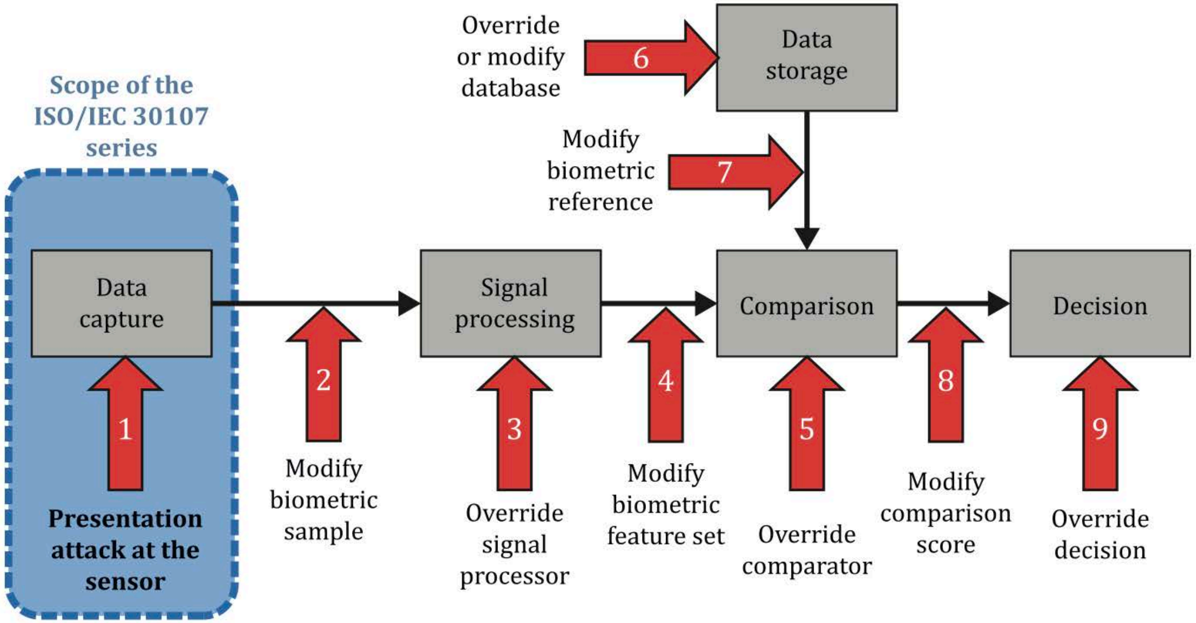
ATHENE

da/sec
BIOMETRICS AND INTERNET-SECURITY RESEARCH GROUP

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) - see ISO/IEC CD2 20059
- Data storage (6): Database, token
  - Providing attackers with references


Override or modify database
6
Data storage
Modify biometric reference
7
Scope of the ISO/IEC 30107 series
Data capture
Signal processing
Comparison
Decision
1
2
3
4
5
8
9
Presentation attack at the sensor
Modify biometric sample
Override signal processor
Modify biometric feature set
Override comparator
Modify comparison score
Override decision

Source: ISO/IEC 30107-1:2023

Capture Device -
Replicates of Biometric Characteristics

Fingerprint Presentation Attacks

1971

Attack without support of an enrolled individual

- James Bond: Diamonds Are Forever

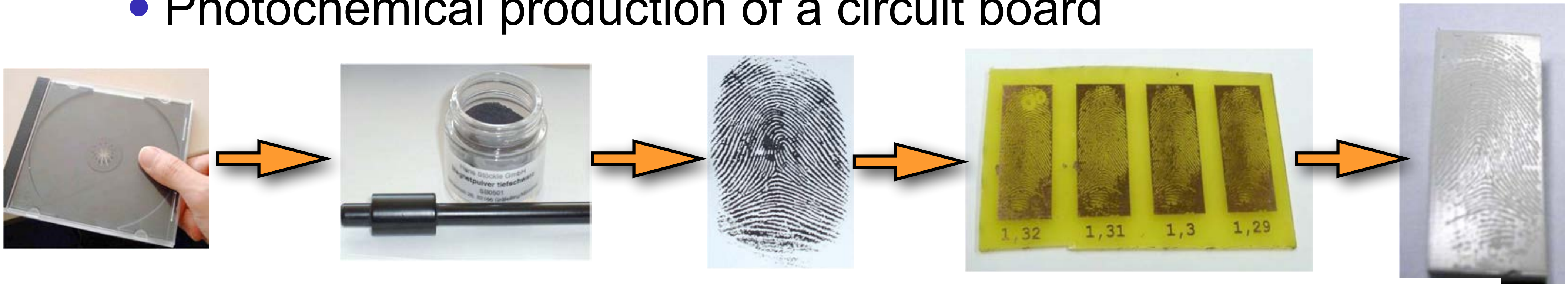
Source: https://www.imdb.com/title/tt0066995 (1971)

Fingerprint Presentation Attacks

Attack without support of an enrolled individual

1999

- 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



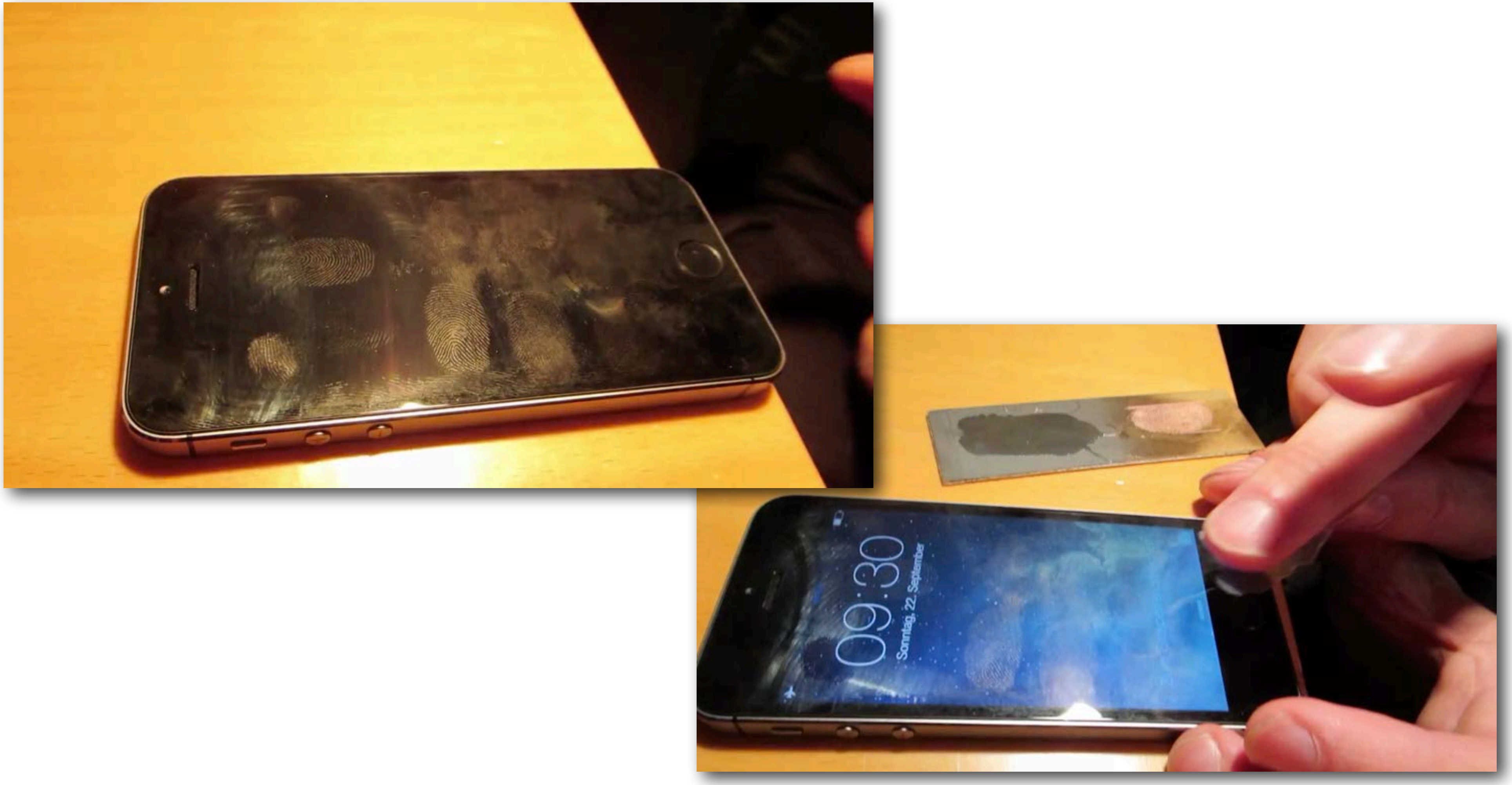
Source: A. Zwiesele et al. „BioIS Study - Comparative Study of Biometric Identification Systems“, In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, pp. 60-63, (2000)

Fingerprint Presentation Attacks

Overlay attack without support

2013

- Recording of an analog fingerprint from the phone



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

Fingerprint Alteration

Example for fingerprint alterations

1997

- Z-shaped alteration (Finger of Jose Izquierdo)

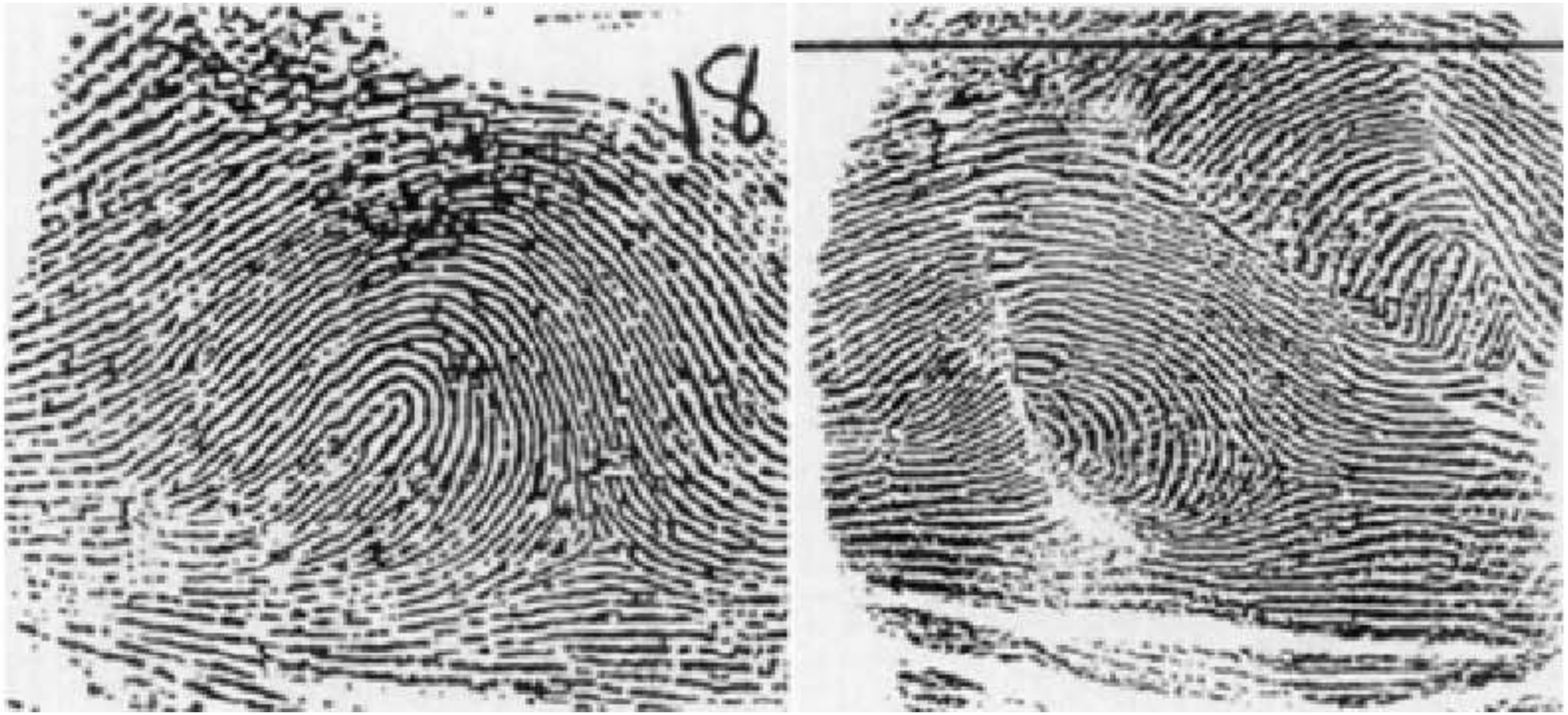


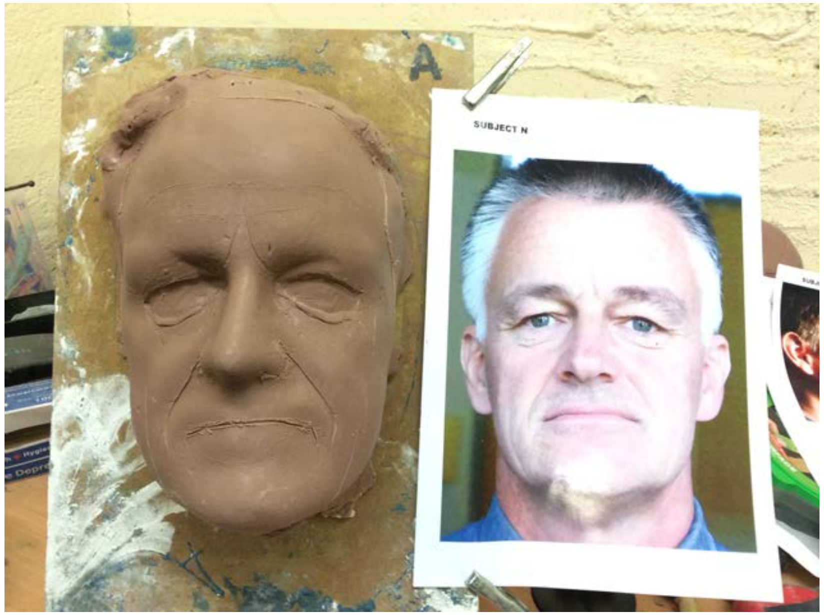
Image Source: S. Yoon, J. Feng, and A. Jain, “Altered fingerprints: Analysis and detection,”
IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 34, no. 3, pp. 451–464, Mar. 2012

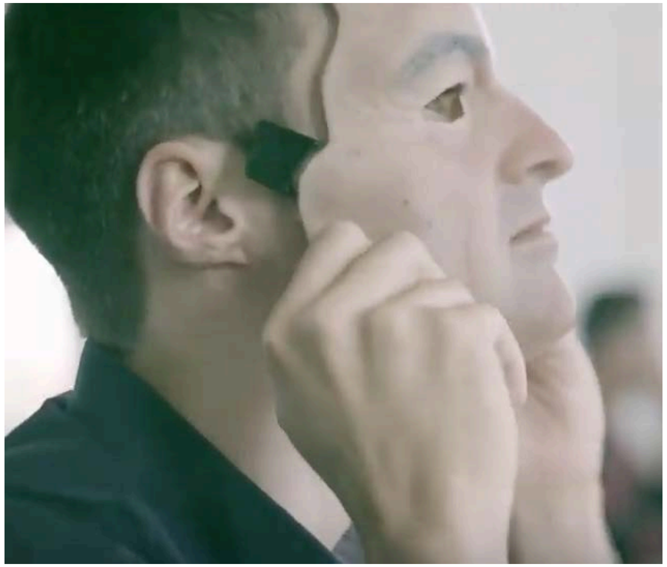
Face Presentation Attacks

2018

3D silicone mask

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



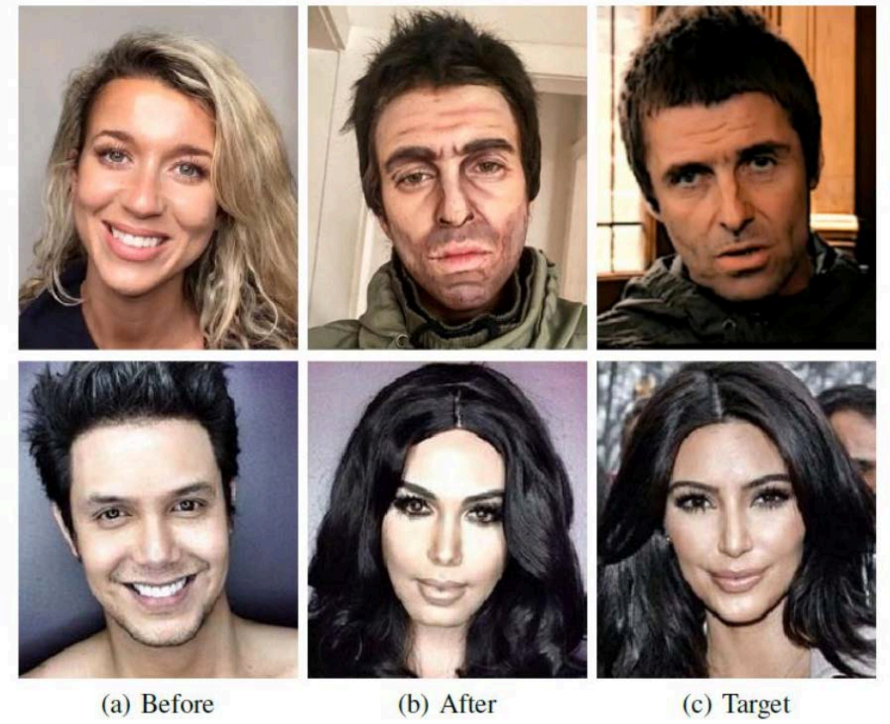


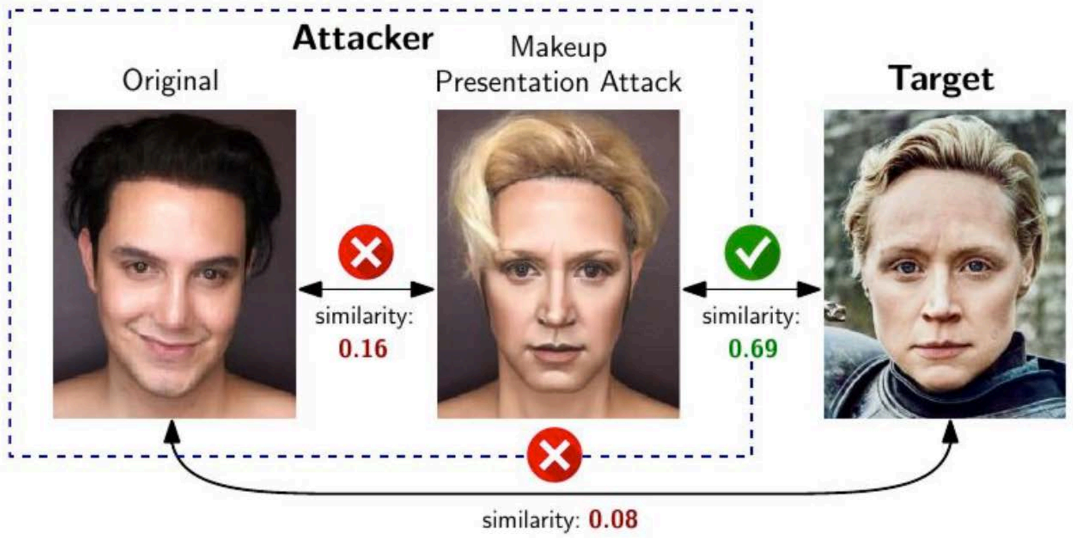
Face Presentation Attacks

Changing facial appearance by makeup alterations

2020

- Makeup for impersonation
- Liveness detection is not sufficient
- Detection difficult since bona fide users may also apply makeup



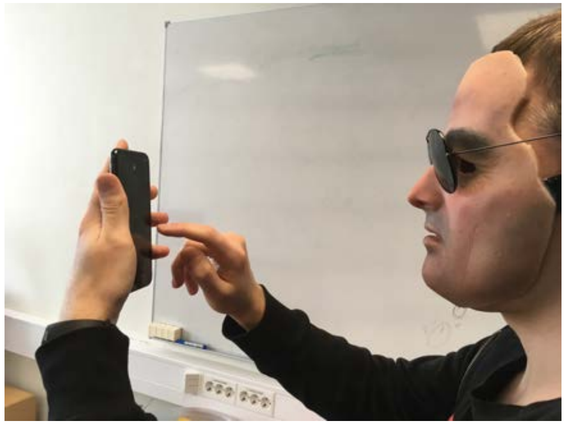


[RDB2020] C. Rathgeb, P. Drozdowski, C. Busch: "Detection of Makeup Presentation Attacks based on Deep Face Representations“, in Proceedings of 25th International Conference on Pattern Recognition (ICPR), (2020) Why is this called Presentation Attack Detection (PAD) and not Liveness Detection ?

Categories of Presentation Attacks

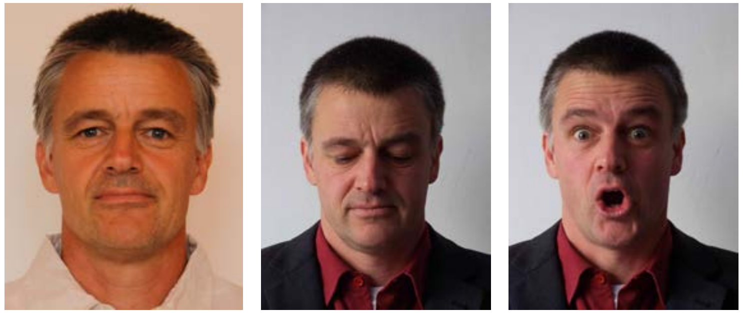
Impostor

- 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



Concealer

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



- evade face detection

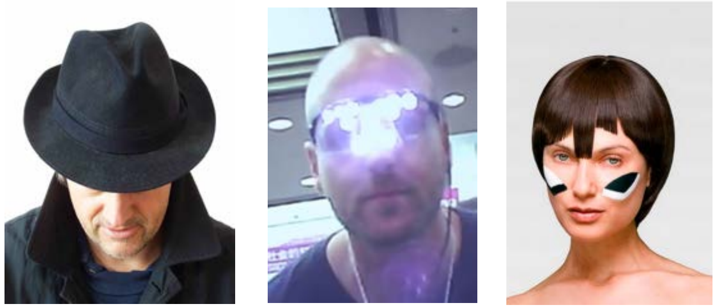


Image Source: https://www.youtube.com/watch?v=LRj8whKmN1M

Image Source: https://cvdazzle.com

Presentation Attack Detection

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

- **presentation attack**
  attack presentation
  presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system
- **presentation attack detection (PAD)**
  automated discrimination between bona-fide presentations and biometric presentation attacks

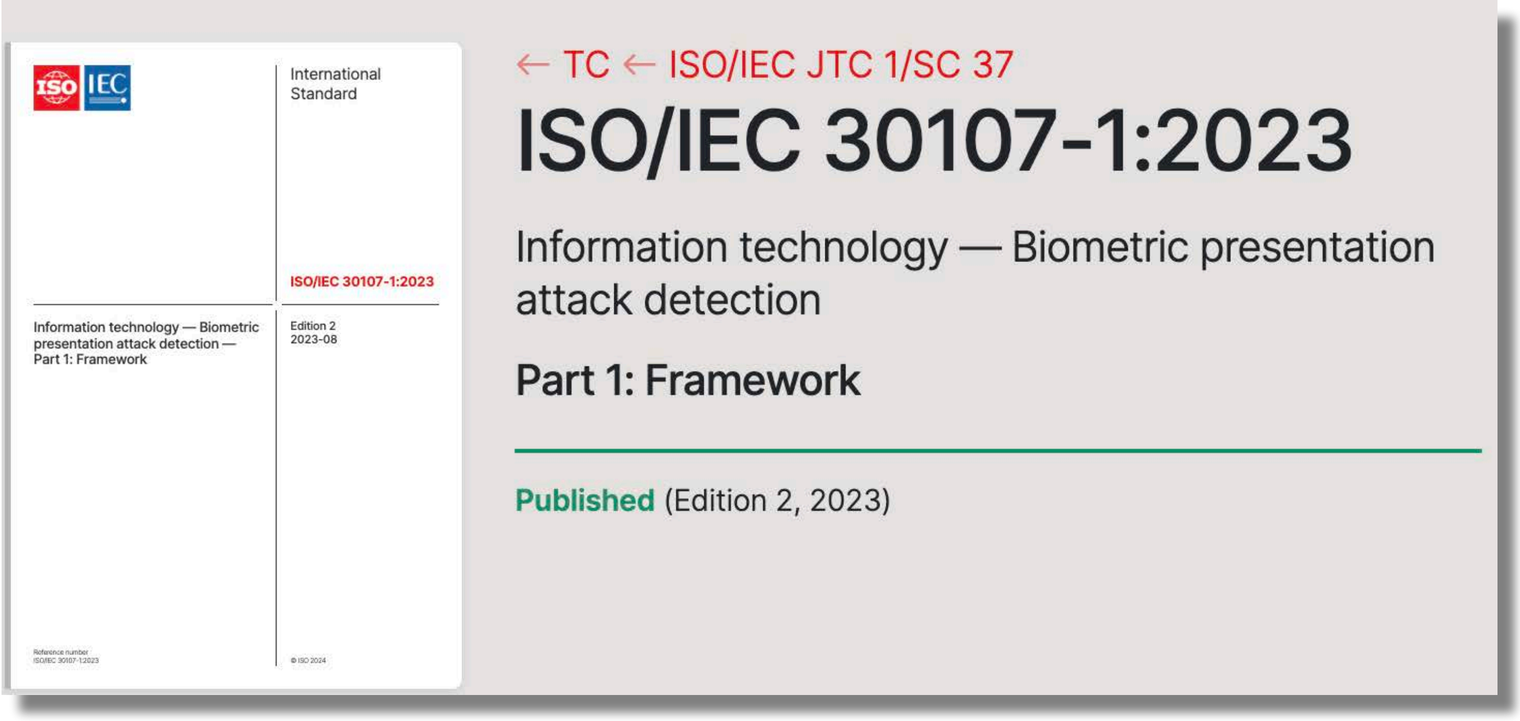
Definitions in ISO/IEC 2382-37: Vocabulary

- **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 30107-1:2023

- provides the taxonomy
- freely available in the ISO-Portal
  https://standards.iso.org/ittf/PubliclyAvailableStandards/ISO_IEC_30107-1_2023_ed_2_-_id_83828_Publication_PDF_(en).zip



International Standard

ISO/IEC 30107-1:2023

Information technology — Biometric presentation attack detection — Part 1: Framework

Edition 2
2023-08

Reference number
ISO/IEC 30107-1:2023

© ISO 2024

← TC ← ISO/IEC JTC 1/SC 37

ISO/IEC 30107-1:2023

Information technology — Biometric presentation attack detection

Part 1: Framework

Published (Edition 2, 2023)

Presentation Attack Detection

ISO/IEC 30107-1 - Definitions

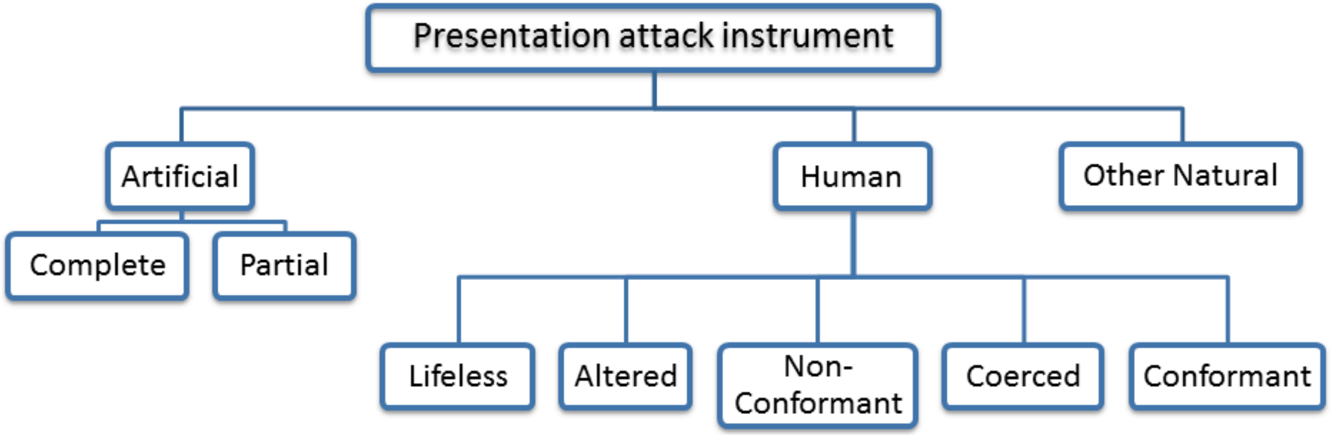
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

(Qualifying adjectives)



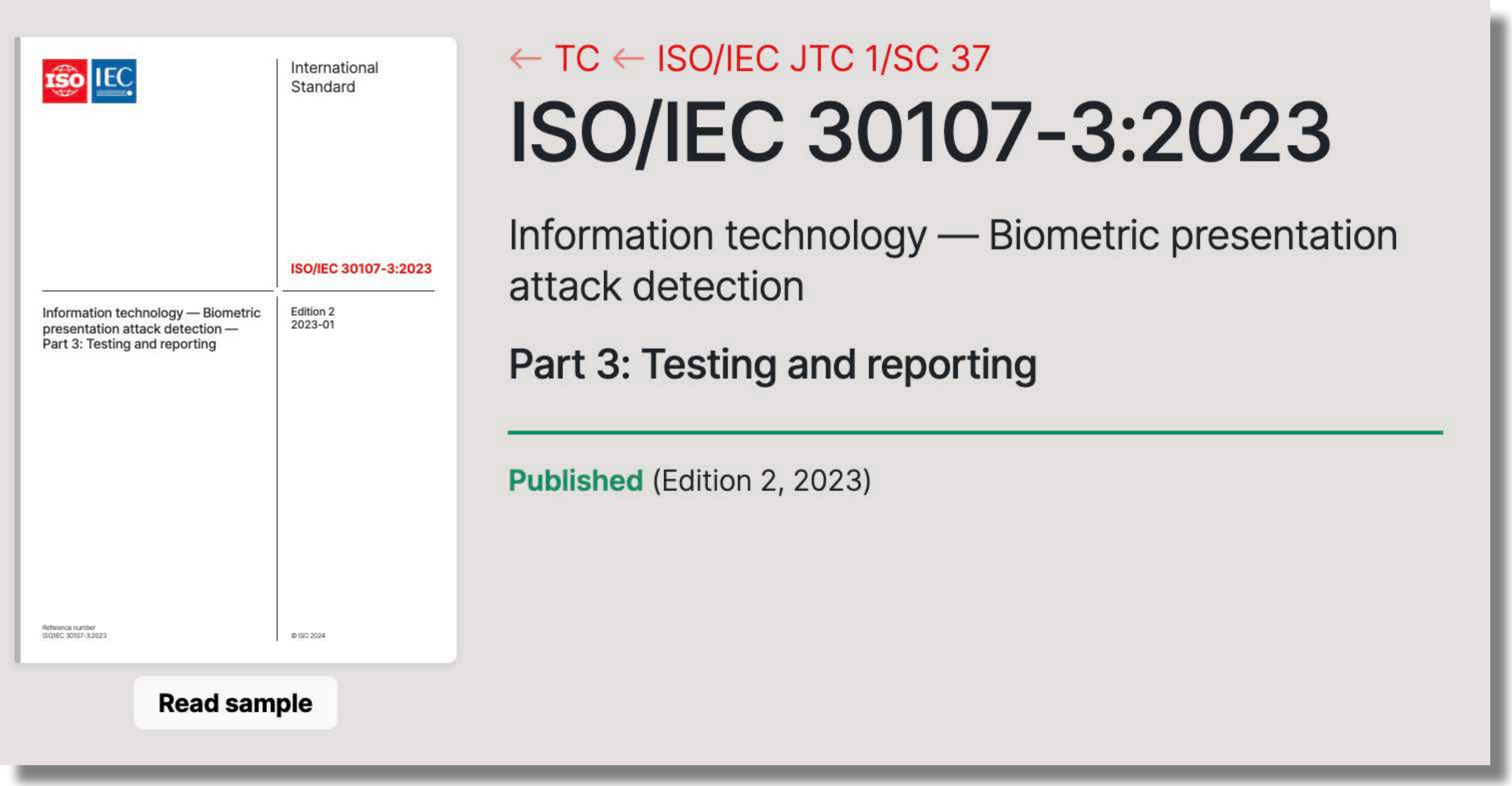
Source: ISO/IEC 30107-1

PAD Testing

Presentation Attack Detection - Testing

ISO/IEC 30107-3:2023

- Provides the testing methodology



International Standard

ISO/IEC 30107-3:2023

Information technology — Biometric presentation attack detection — Part 3: Testing and reporting

Edition 2
2023-01

Reference number
ISO/IEC 30107-3:2023

© ISO 2024

← TC ← ISO/IEC JTC 1/SC 37

ISO/IEC 30107-3:2023

Information technology — Biometric presentation attack detection

Part 3: Testing and reporting

Published (Edition 2, 2023)

Read the sample text:
https://www.iso.org/obp/ui/en/#iso:std:iso-iec:30107:-3:ed-2:v1:en

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

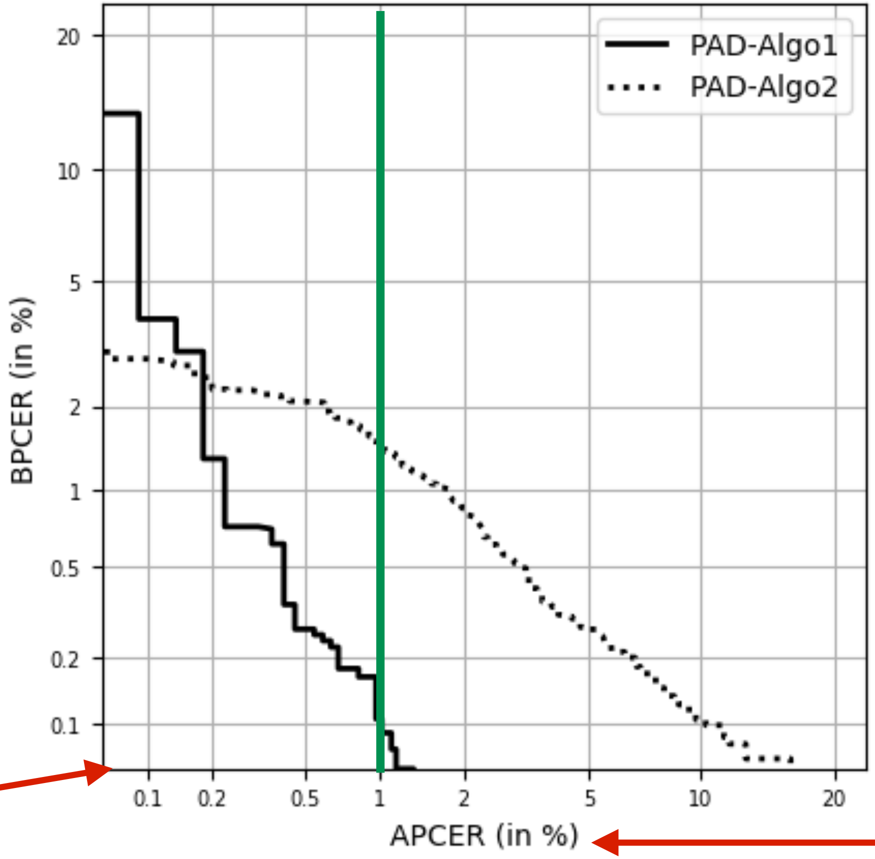
- **PAI species**
  class of presentation attack instruments created using a common production method and based on different biometric characteristic
- **attack potential**
  measure of the capability to attack a TOE given the attacker's knowledge, proficiency, resources and motivation
- **target of 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:



convenience measure

Ideal:
APCER - low
BPCER - low

security measure (strength of function)

Presentation Attack Detection - Testing

Definition of detection capabilities metrics

- Testing a specific security level:

  PAD mechanism may be reported in a single figure

- DON'T use neither the equal error rate (EER) nor the half-total error rate (HTER)

- *BPCER at a fixed APCER:*

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

  Source: ISO/IEC 30107-3

  - BPCER100: when APCER is 1%
  - BPCER20: when APCER is 5%
  - BPCER10: when APCER is 10%

PA Vulnerability Testing

Presentation Attack Detection - Testing

New definition in the revised 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 attack presentations using the same presentation attack instrument (PAI) species that result in accept

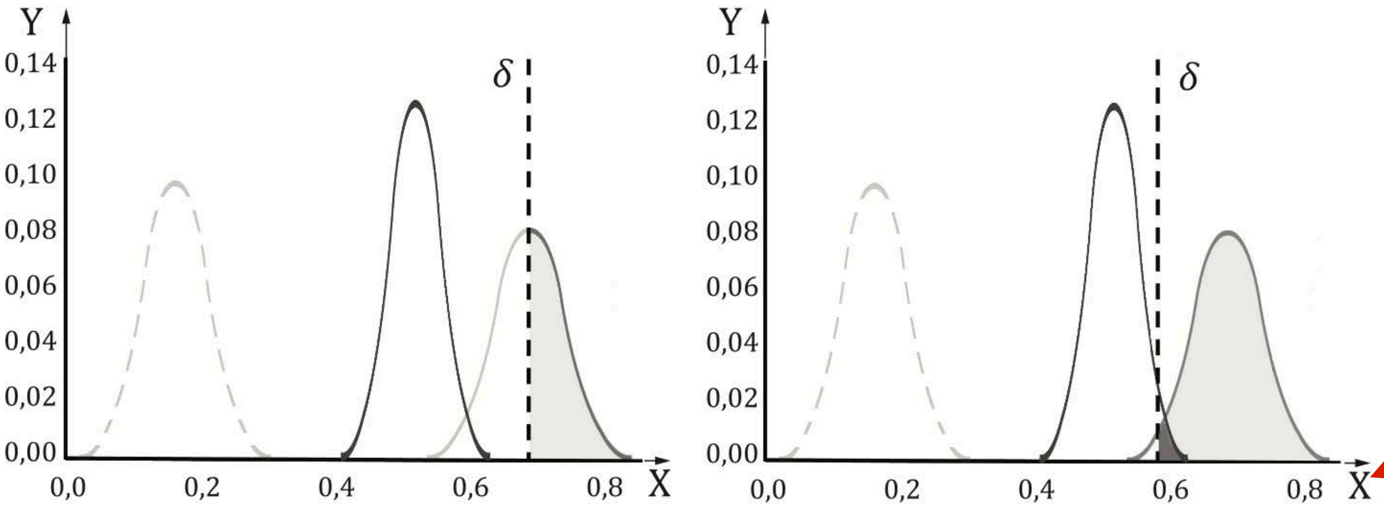
Source: ISO/IEC 30107-3:2023

Presentation Attack Detection - Testing

New definition in the revised ISO/IEC 30107-3

- Relationship between vulnerability and recognition performance
- **Relative imposter presentation accept rate (RIAPAR)**
  sum of IAPAR and FRR at a fixed decision threshold

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



a) Decision threshold with suboptimal RIAPAR

b) Decision threshold with optimized RIAPAR

comparison scores

Source: ISO/IEC 30107-3:2023

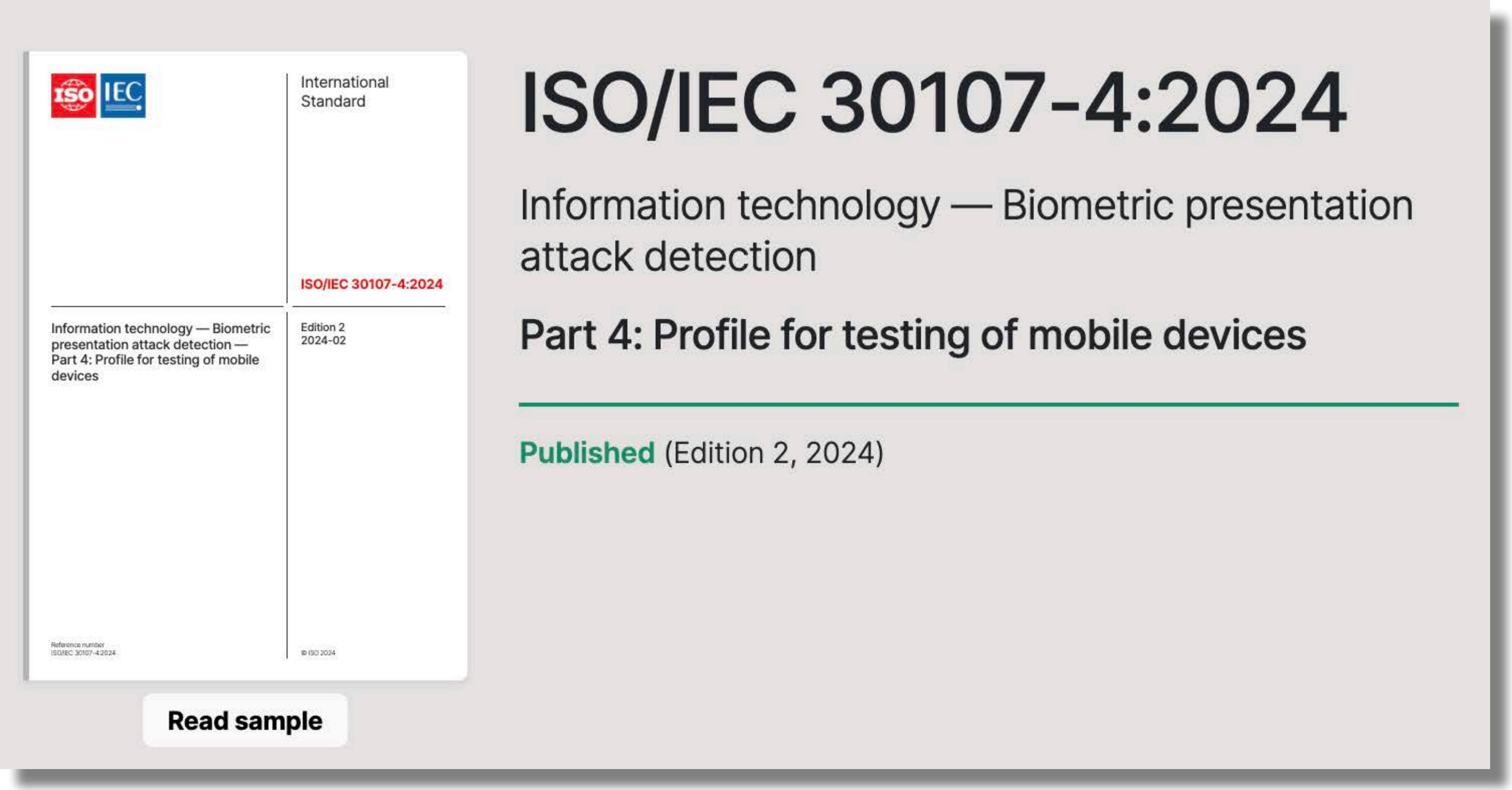
Source: U. Scherhag et al.: "Biometric Systems under Morphing Attacks: Assessment of Morphing Techniques and Vulnerability Reporting", in Proceedings of the IEEE 16th International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, (2017)

PAD and FIDO

Presentation Attack Detection - Testing

ISO/IEC 30107-4:2024

- Provides the testing methodology



International Standard

ISO/IEC 30107-4:2024

Information technology — Biometric presentation attack detection — Part 4: Profile for testing of mobile devices

Edition 2
2024-02

Reference number
ISO/IEC 30107-4:2024

© ISO 2024

ISO/IEC 30107-4:2024

Information technology — Biometric presentation attack detection

Part 4: Profile for testing of mobile devices

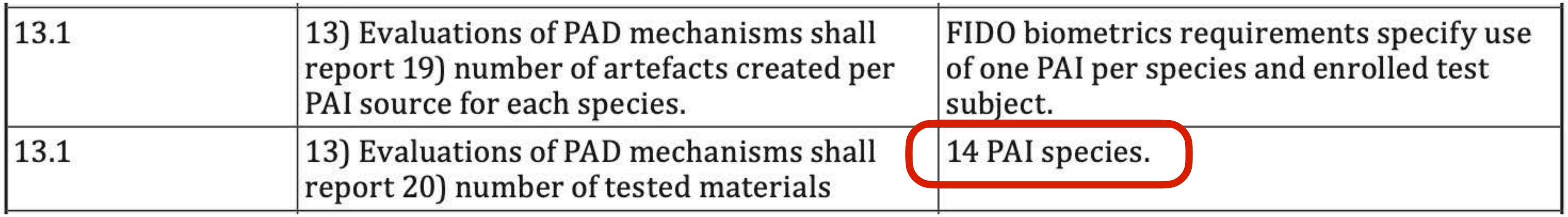
Published (Edition 2, 2024)

Read the sample text:
https://www.iso.org/obp/ui/en/#iso:std:iso-iec:30107:-4:ed-2:v1:en

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-4

- Scope: *This document is a profile that specifies requirements for testing biometric presentation attack detection (PAD) mechanisms on mobile devices with local biometric recognition.*



13.1	13) Evaluations of PAD mechanisms shall report 19) number of artefacts created per PAI source for each species.	FIDO biometrics requirements specify use of one PAI per species and enrolled test subject.
13.1	13) Evaluations of PAD mechanisms shall report 20) number of tested materials	14 PAI species.

Summary

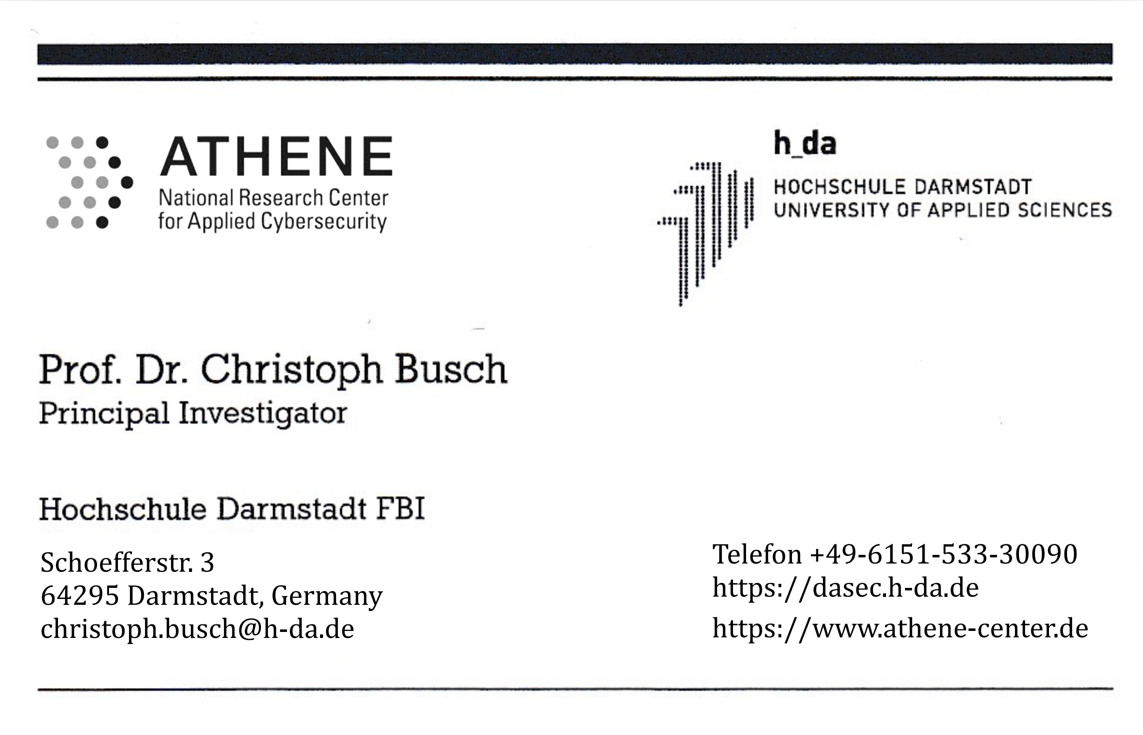
The ISO/IEC 30107 series

- Part 1: Framework
  https://www.iso.org/standard/83828.html
- Part 2: Data formats
  https://www.iso.org/standard/67380.html
- Part 3: Testing and reporting
  https://www.iso.org/standard/79520.html
- Part 4: Profile for testing of mobile devices
  https://www.iso.org/standard/82584.html

Further information on PAD:

- PAD for face recognition systems:
  https://christoph-busch.de/files/Raghavendra-FacePAD-survey-ACM-2017.pdf
- PAD for fingerprint recognition systems:
  http://digital-library.theiet.org/deliver/fulltext/iet-bmt/3/4/IET-BMT.2013.0020.pdf?itemId=/content/journals/10.1049/iet-bmt.2013.0020&mimeType=pdf&isFastTrackArticle=

Contact



ATHENE
National Research Center
for Applied Cybersecurity

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

Prof. Dr. Christoph Busch
Principal Investigator

Hochschule Darmstadt FBI

Schoefferstr. 3
64295 Darmstadt, Germany
christoph.busch@h-da.de

Telefon +49-6151-533-30090
https://dasec.h-da.de
https://www.athene-center.de