Standardisierung Presentation Attack Detection

Christoph Busch

- ISO/IEC JTC1/SC37 WG3 Convenor -

TTT AG Biometrie
Darmstadt
2016-03-22

Presentation Attack Detection

Outline

- Introduction to Standardisation and PAD
- ISO/IEC 30107
- ISO/IEC 19989
- Application areas for these standards

Fingerprint Spoof - James Bond

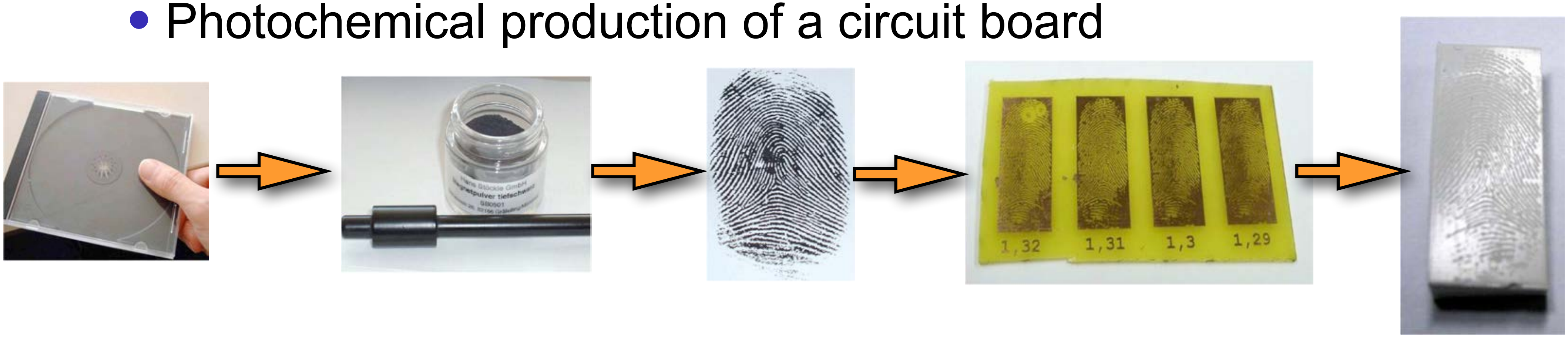
Attack without support of an enroled individual

- 1971: Diamonds Are Forever

Gummy Finger Production in 2000 !

Attack without support of an enroled individual

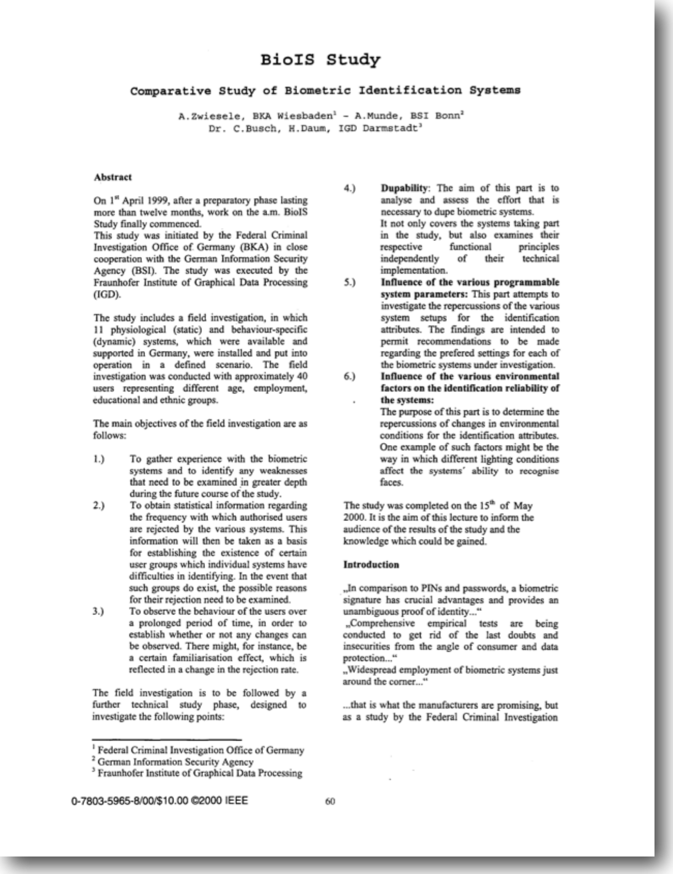
- Recording of an analog fingerprint from flat surface material
  - z.B. glass, CD-cover, etc.
    with iron powder and tape
- Scanning and post processing:
  - Correction of scanning errors
  - Closing of ridge lines (as needed)
  - Image inversion
- Print on transparent slide
- Photochemical production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



Gummy Finger Production in 2000 !

Reported in a publication by the German Federal Police

- 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)



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...“

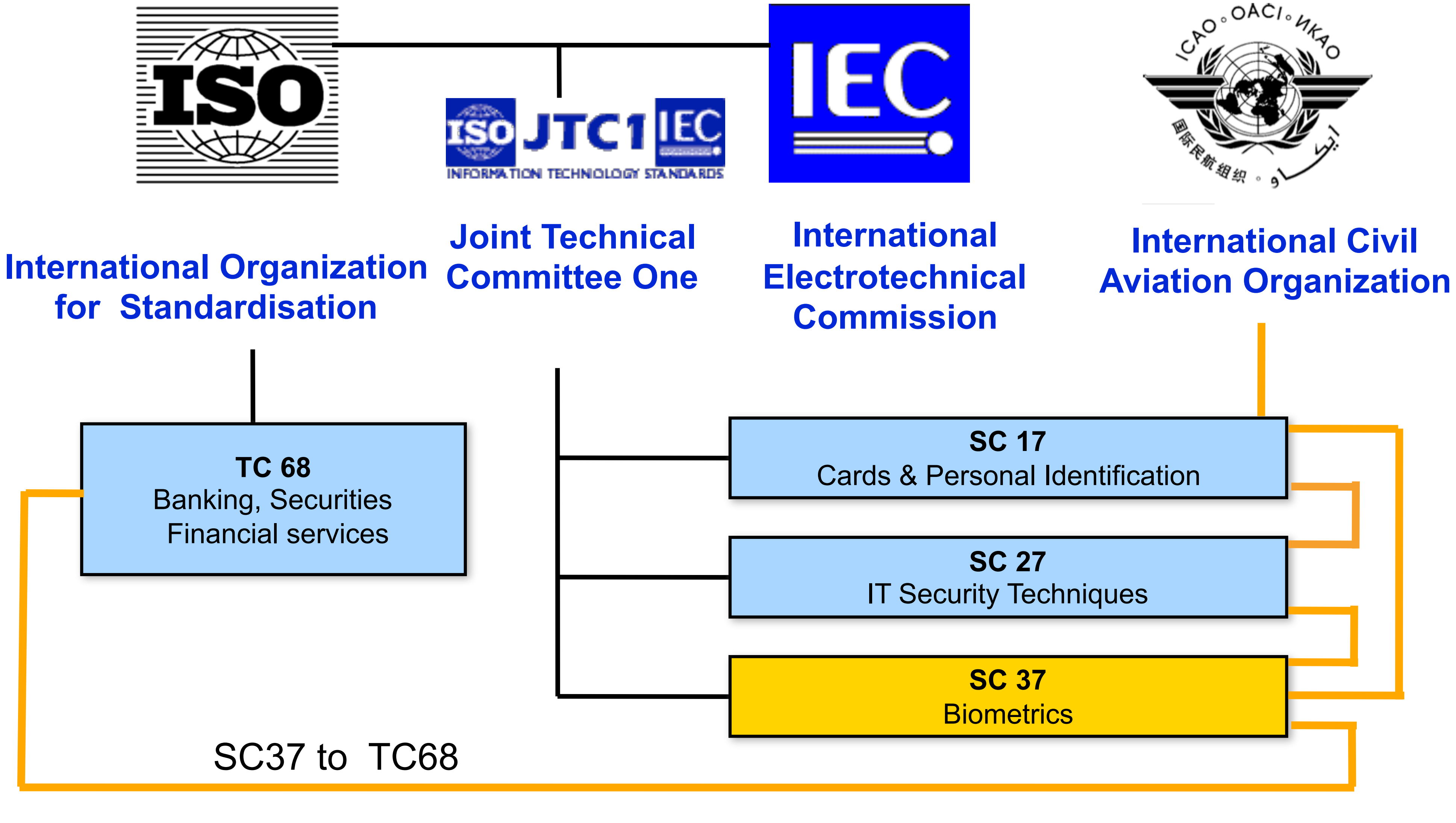
...that is what the manufacturers are promising, but as a study by the Federal Criminal Investigation

[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

60

Biometric Standardisation


International Organization for Standardisation
Joint Technical Committee One
International Electrotechnical Commission
International Civil Aviation Organization
TC 68
Banking, Securities Financial services
SC 17
Cards & Personal Identification
SC 27
IT Security Techniques
SC 37
Biometrics
SC37 to TC68

— SC 37 Formal Liaisons

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, 2016

First Generation Format Standards

G1

19794-1:2006

-2: 2005

-3: 2006

-4: 2005

-5: 2005

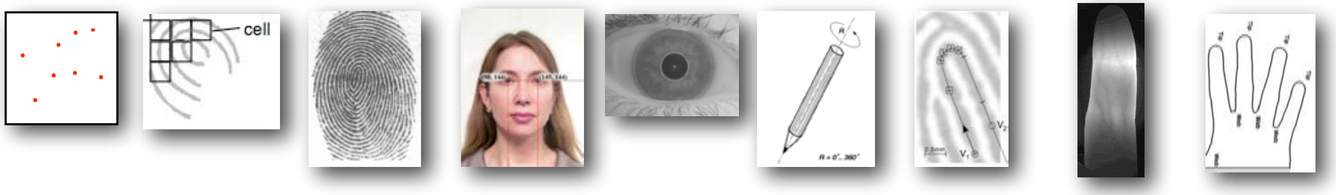
-6: 2005

-7: 2007

-8: 2006

-9: 2007

-10: 2007



All parts
binary encoding

The 19794-Family: Biometric data interchange formats

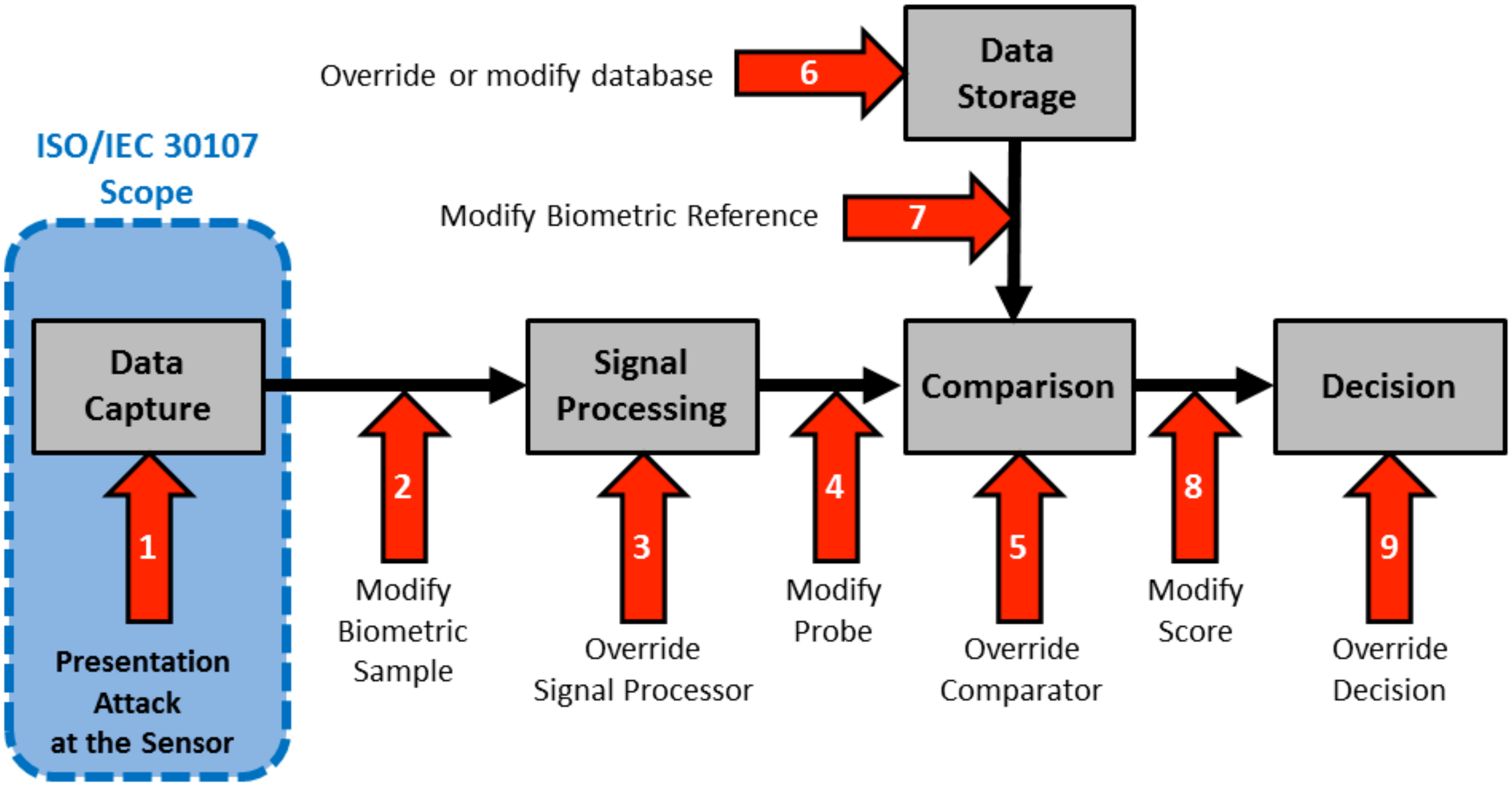
Presentation Attack Detection

ISO/IEC 30107

Liveness Detection

ISO/IEC 30107-1:2016 Presentation Attack Detection

- Attacks on Biometric Systems



Source: ISO/IEC 30107-1
nspired 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).

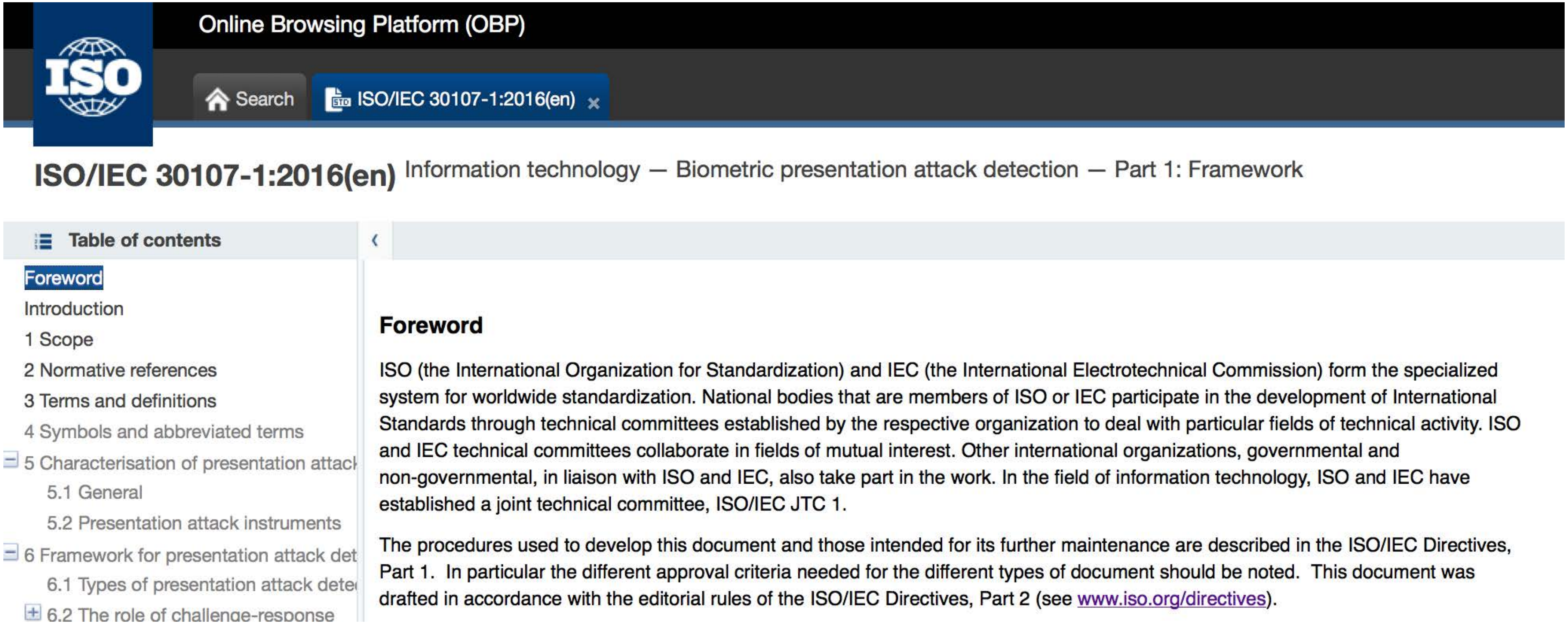
Outside the scope are

- 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 IS 30107-1 Standard

- **now available in the ISO-Portal**
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53227
- SC37 has initiated to make this standard freely available



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

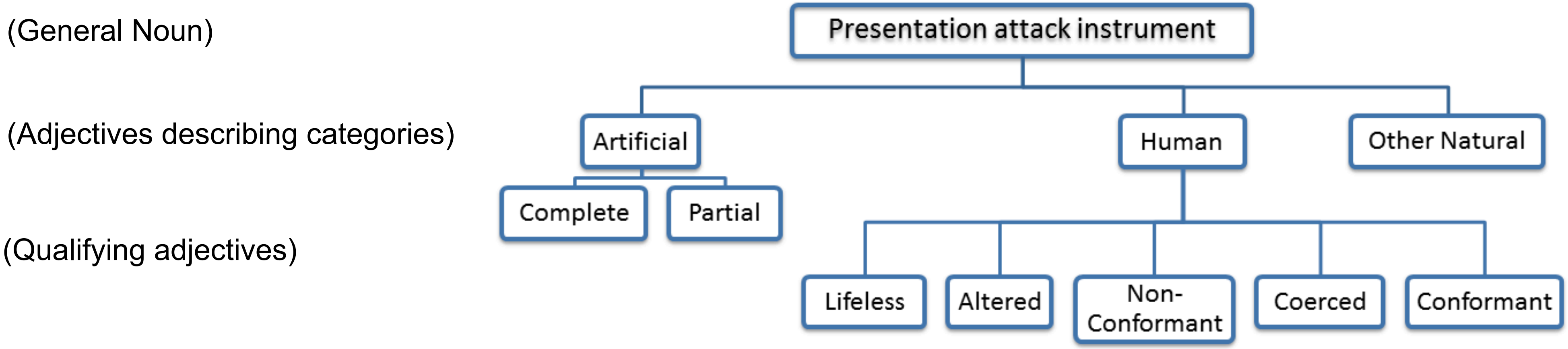
- **impostor**
  subversive biometric capture subject who attempts to being matched to someone else's biometric reference
- **identity concealer**
  subversive biometric capture subject who attempts to avoid being matched to their own biometric reference

Presentation Attack Detection

ISO/IEC 30107 - 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)

Presentation attack instrument

Artificial

Complete

Partial

Human

Lifeless

Altered

Non-Conformant

Coerced

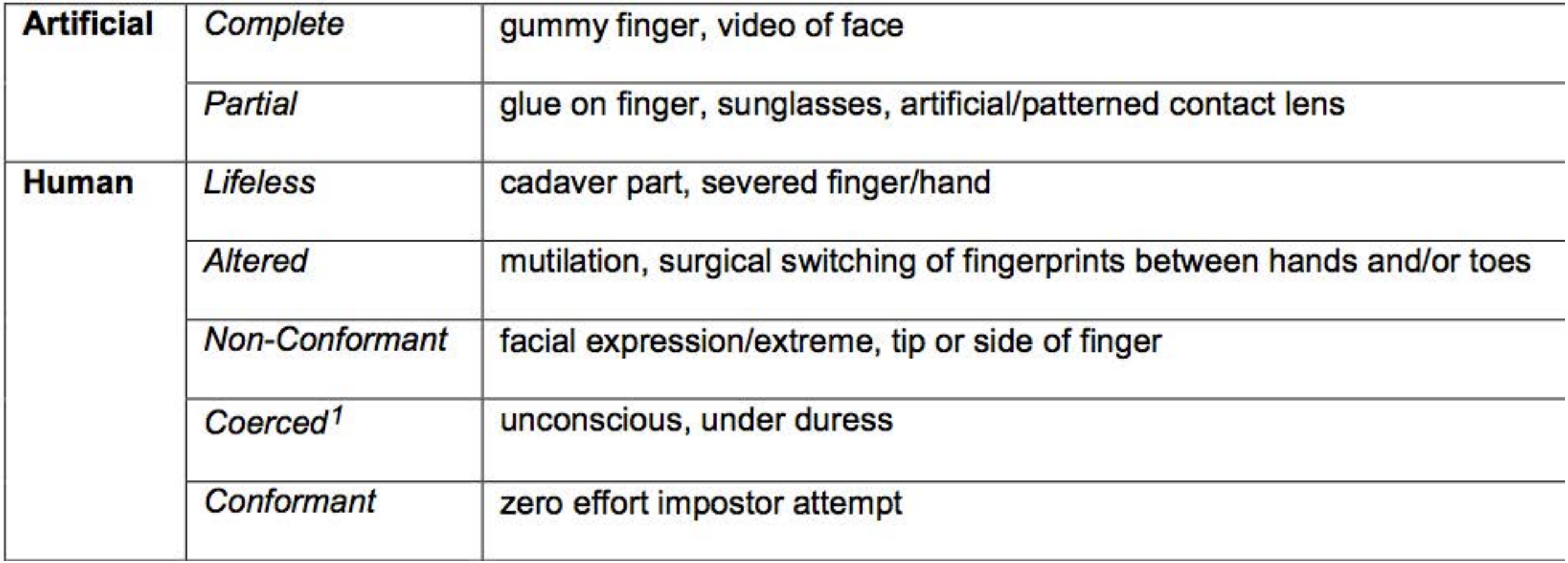
Conformant

Other Natural

Source: ISO/IEC 30107-1

Presentation Attack Detection

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



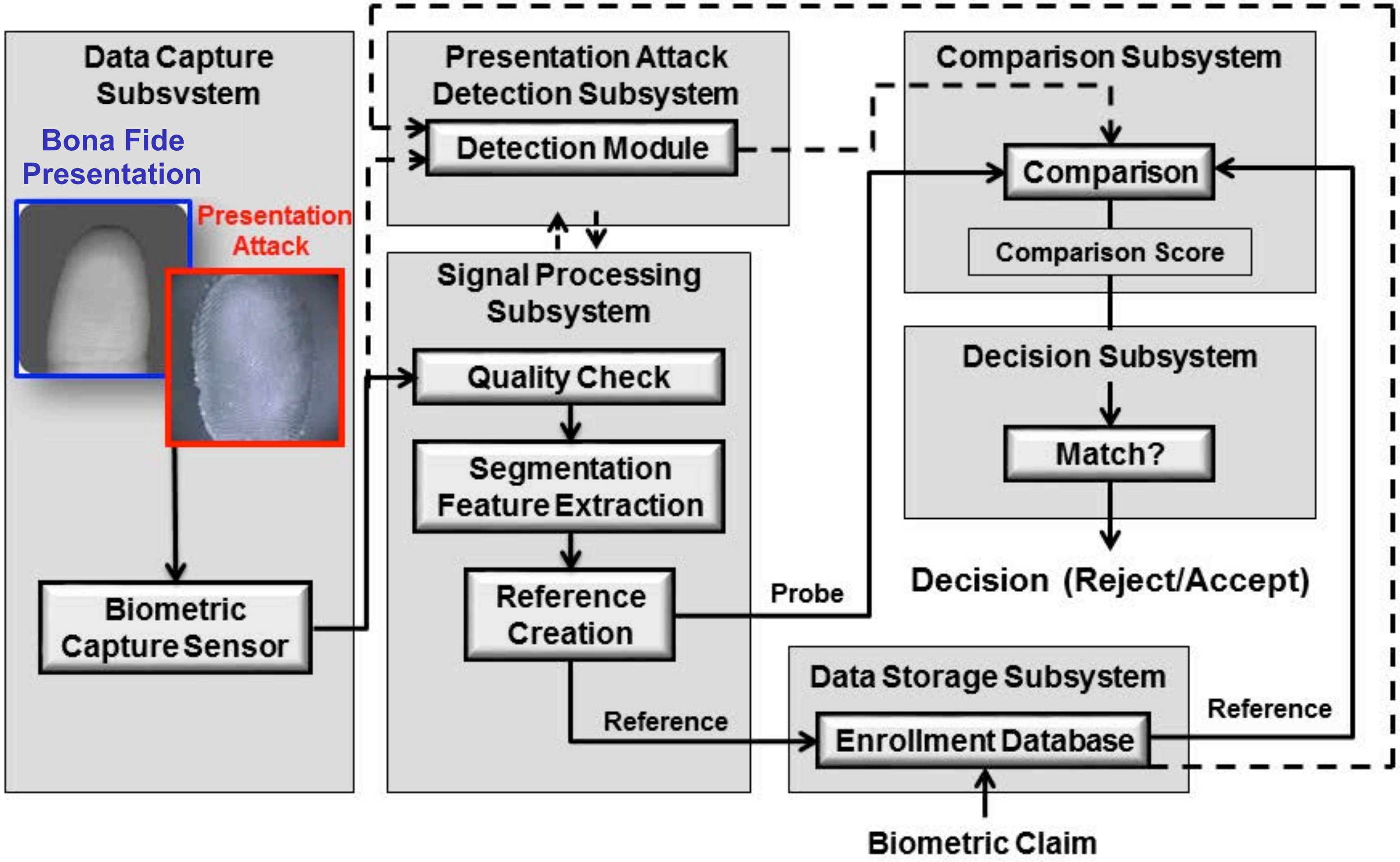
Artificial	*Complete*	gummy finger, video of face
	Partial	glue on finger, sunglasses, artificial/patterned contact lens
Human	*Lifeless*	cadaver part, severed finger/hand
	Altered	mutilation, surgical switching of fingerprints between hands and/or toes
	Non-Conformant	facial expression/extreme, tip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

Source: ISO/IEC 30107-1

Presentation Attack Detection

Bona Fide Presentation

Biometric framework with PAD

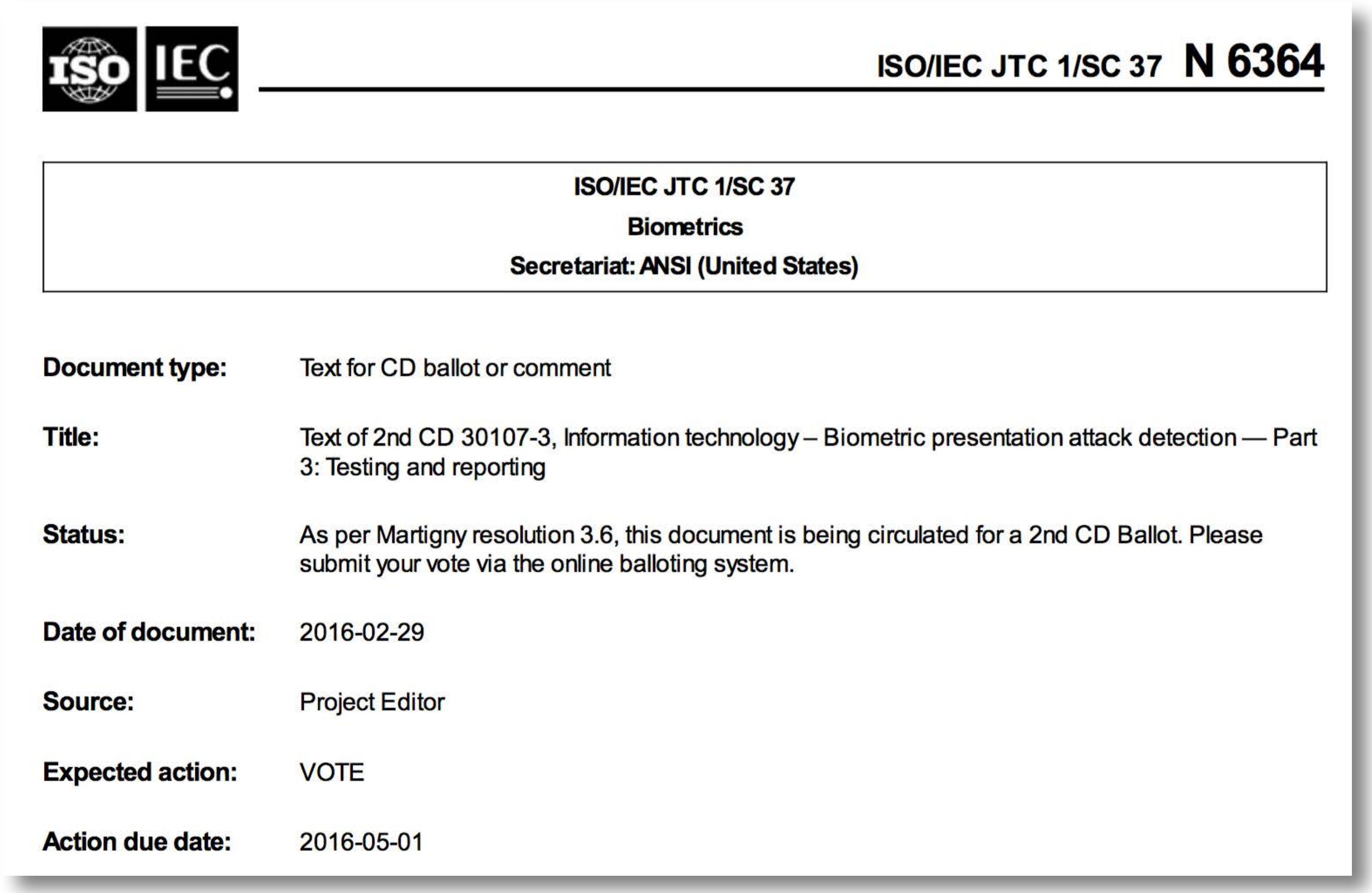


Source: ISO/IEC 30107-1

Presentation Attack Detection - Metrics

ISO/IEC CD 30107-3

- available as draft
  http://isotc.iso.org/livelink/livelink?func=ll&objId=17578675&objAction=Open&viewType=1



ISO/IEC JTC 1/SC 37 **N 6364**

ISO/IEC JTC 1/SC 37
Biometrics
Secretariat: ANSI (United States)

Document type:	Text for CD ballot or comment
Title:	Text of 2nd CD 30107-3, Information technology – Biometric presentation attack detection — Part 3: Testing and reporting
Status:	As per Martigny resolution 3.6, this document is being circulated for a 2nd CD Ballot. Please submit your vote via the online balloting system.
Date of document:	2016-02-29
Source:	Project Editor
Expected action:	VOTE
Action due date:	2016-05-01

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

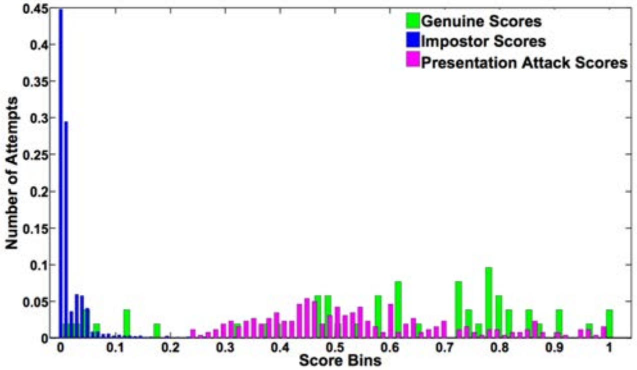
- Testing the full system:

- **Attack presentation match rate (APMR)**
  in a full-system evaluation of a verification system, the proportion of presentation attacks in which the target reference is matched

Source: ISO/IEC 30107-3

- **Attack presentation non-match rate (APNMR)**
  in a full-system evaluation of a verification system, the proportion of presentation attacks in which the target reference is not matched.

Source: ISO/IEC 30107-3



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

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem:
- **Attack presentation non-response rate (APNRR)**
  proportion of presentation attacks 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 PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem:

- **Attack presentation classification error rate (APCER)**
  proportion of attack presentations incorrectly classified as Bona Fide presentations at the component level
  in a specific scenario

- **Bona Fide presentation classification error rate (BPCER)**
  proportion of Bona Fide presentations incorrectly classified as attack presentations at the component level
  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 effort to be expended in attacking a TOE, expressed in terms of an attacker's expertise, resources and motivation

- **target of evaluation (TOE)**
  within Common Criteria, the product or system 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 incorrectly classified as Bona Fide presentations at the component level
  in a specific scenario

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

Source: ISO/IEC 30107-3

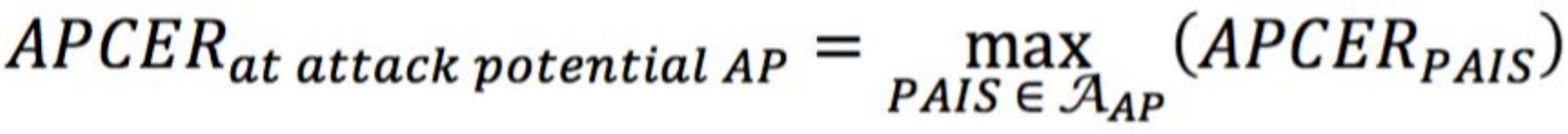
- *N_{PAIS} is the number of attack presentations for the given PAI species*
- *Res_i takes value 1 if the i^{th} presentation is classified as an attack presentation, and value 0 if classified as a bona fide presentation*

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

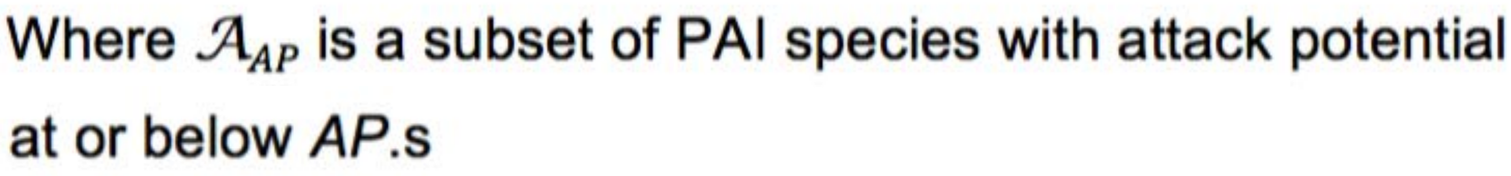
- Testing the PAD subsystem with different species:

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



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

Source: ISO/IEC 30107-3



Where $\mathcal{A}_{AP}$ is a subset of PAI species with attack potential at or below *AP*.s

Presentation Attack Detection - Testing

Definition of PAD metrics in ISO/IEC 30107-3

- Testing the PAD subsystem with different species:

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

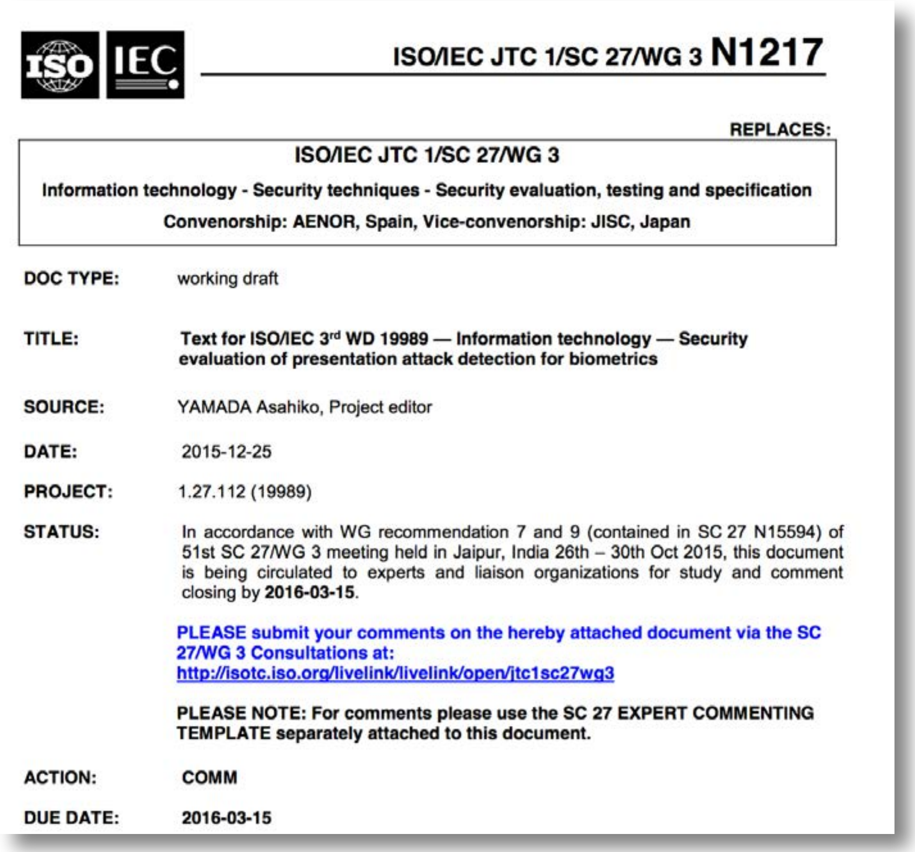
Presentation Attack Detection

ISO/IEC 19989

Presentation Attack Detection - Security

ISO/IEC WD 19989

- Security evaluation, testing and specification
- available as draft
  http://isotc.iso.org/livelink/livelink?func=ll&objId=17501054&objAction=Open&viewType=1



ISO/IEC JTC 1/SC 27/WG 3 **N1217**

REPLACES:

ISO/IEC JTC 1/SC 27/WG 3

Information technology - Security techniques - Security evaluation, testing and specification

Convenorship: AENOR, Spain, Vice-convenorship: JISC, Japan

DOC TYPE:	working draft
TITLE:	**Text for ISO/IEC 3rd WD 19989 — Information technology — Security evaluation of presentation attack detection for biometrics**
SOURCE:	YAMADA Asahiko, Project editor
DATE:	2015-12-25
PROJECT:	1.27.112 (19989)
STATUS:	In accordance with WG recommendation 7 and 9 (contained in SC 27 N15594) of 51st SC 27/WG 3 meeting held in Jaipur, India 26th – 30th Oct 2015, this document is being circulated to experts and liaison organizations for study and comment closing by **2016-03-15**. **PLEASE submit your comments on the hereby attached document via the SC 27/WG 3 Consultations at: http://isotc.iso.org/livelink/livelink/open/jtc1sc27wg3** **PLEASE NOTE: For comments please use the SC 27 EXPERT COMMENTING TEMPLATE separately attached to this document.**
ACTION:	**COMM**
DUE DATE:	**2016-03-15**

Presentation Attack Detection - Security

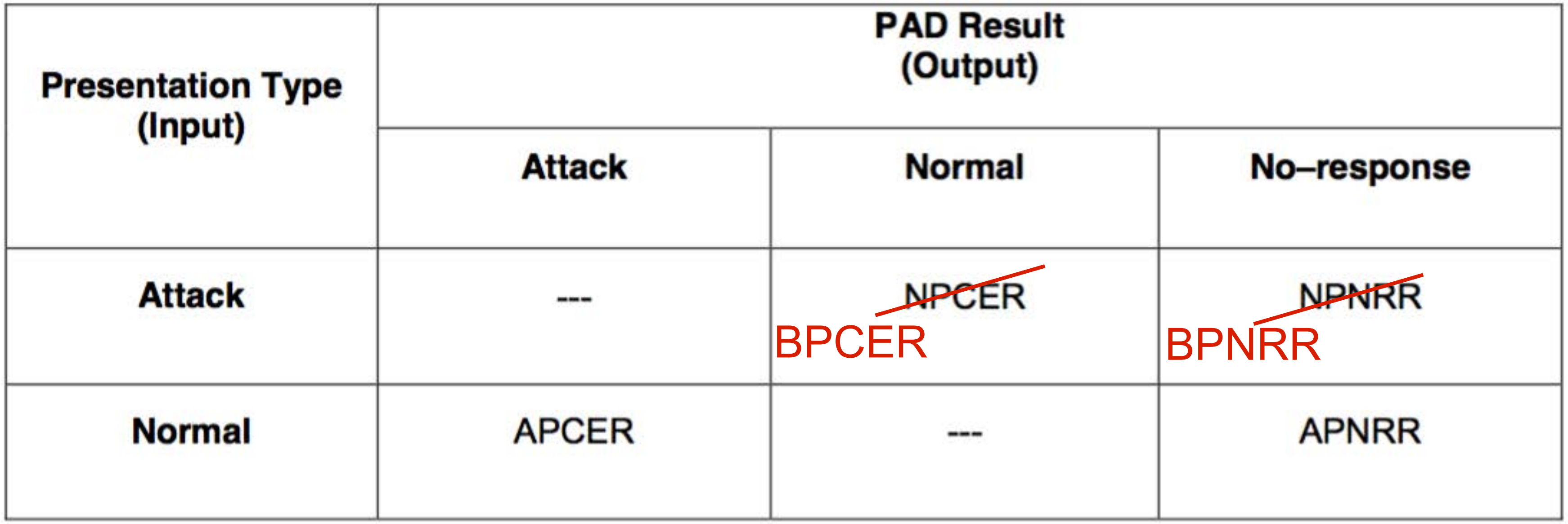
ISO/IEC WD 19989

- Common Criteria testing of Biometric Sensors
- Scope:
  For security evaluation of presentation attack detection for biometrics, this International Standard specifies:
  - *Extended security functional component to Class FPT: Protection of the TSF specified in ISO/IEC 15408-2,*
  - *Extended security assurance component to Class AVA_VAN: Vulnerability assessment specified in ISO/IEC 15408-3, and*
  - *Complements to methodology specified in ISO/IEC 18045 for Class APE, Class ASE, Class ADV, Class AGD, Class ALC, Class ATE, and Class AVA of ISO/IEC 15408-3.*

Presentation Attack Detection - Security

ISO/IEC WD 19989

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



Presentation Type (Input)	PAD Result (Output)		
	Attack	Normal	No–response
Attack	---	~~NPCER~~ BPCER	~~NPNRR~~ BPNRR
Normal	APCER	---	APNRR

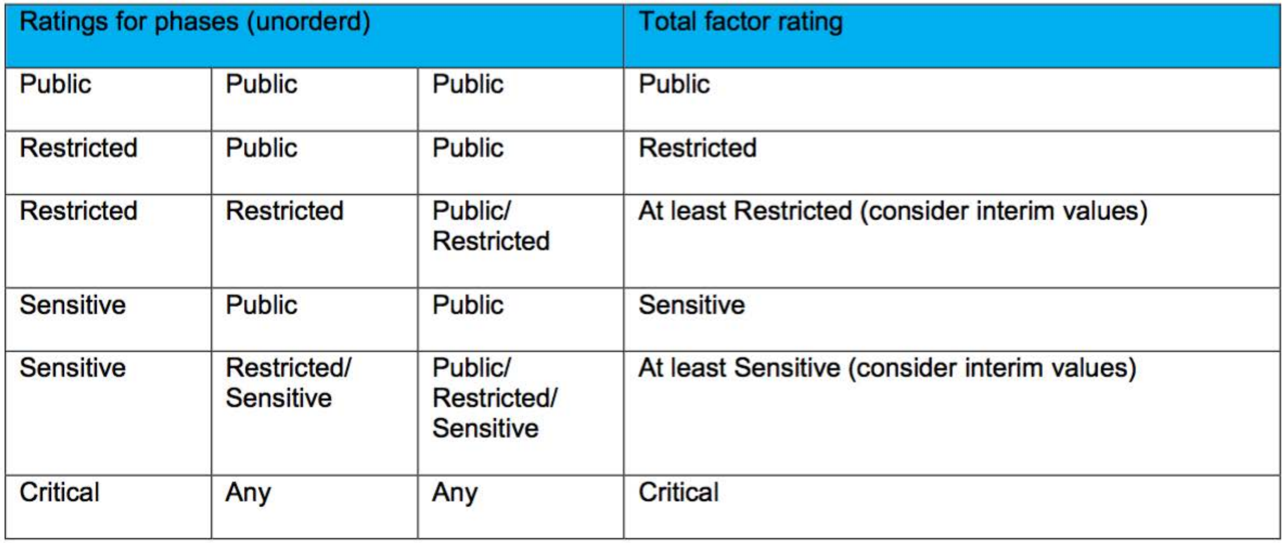
Source: ISO/IEC WD 19989

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

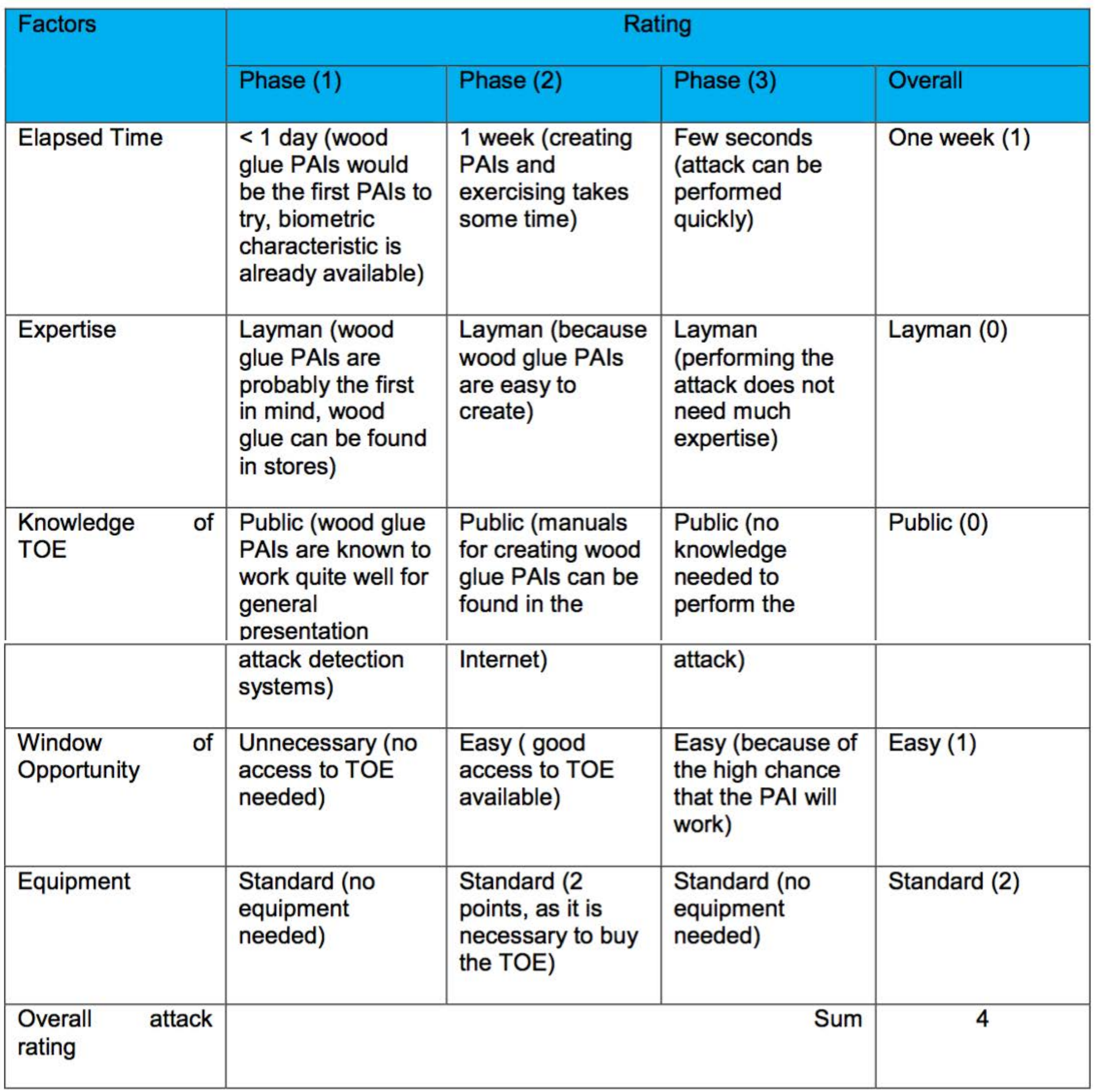
Presentation Attack Detection - Security

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

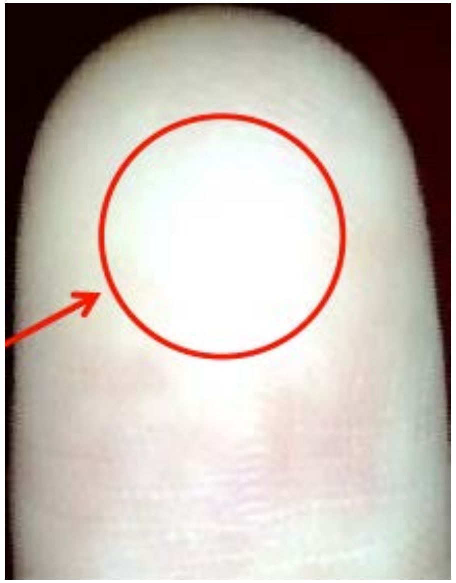
Presentation Attack Detection

Application areas

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



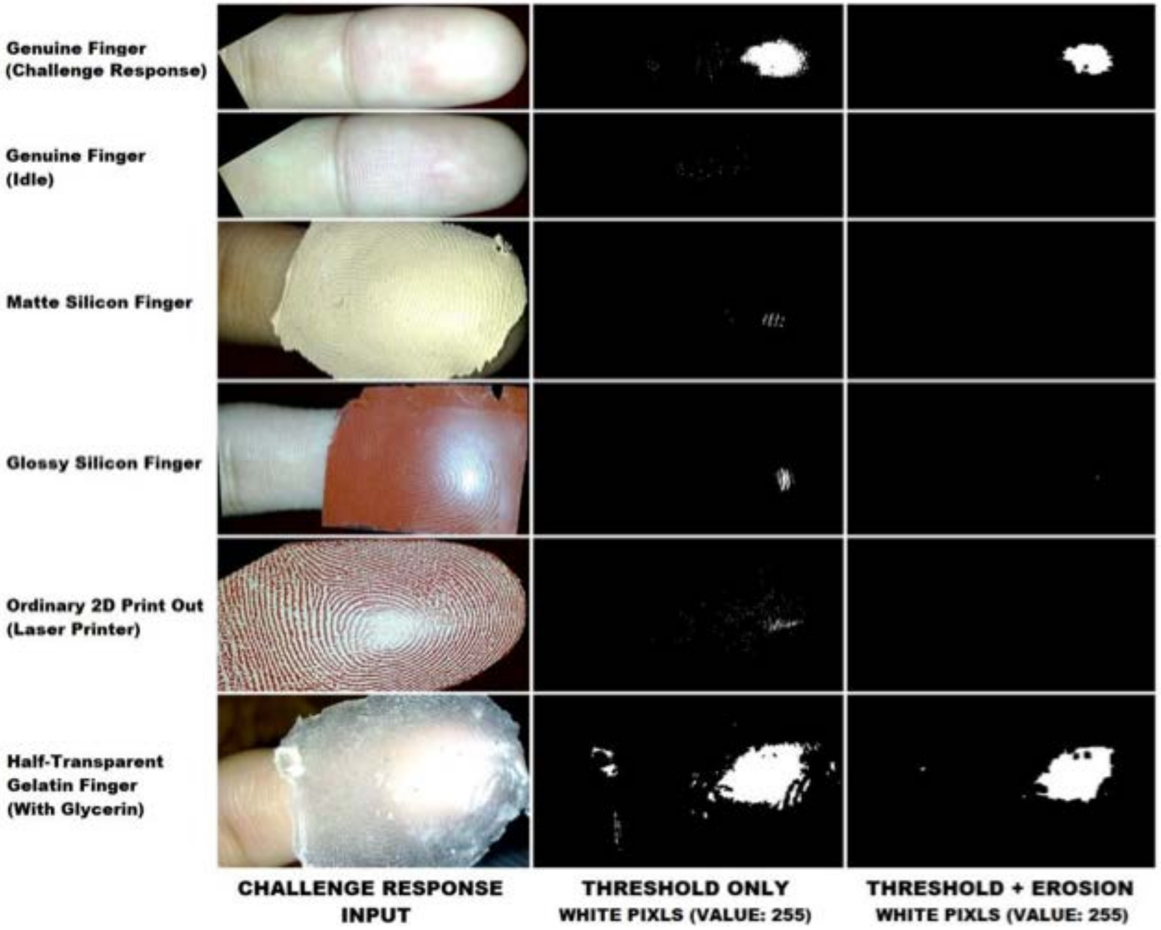
- Attack detection, as light reflection differs from artefacts to Bona Fide fingers

[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)

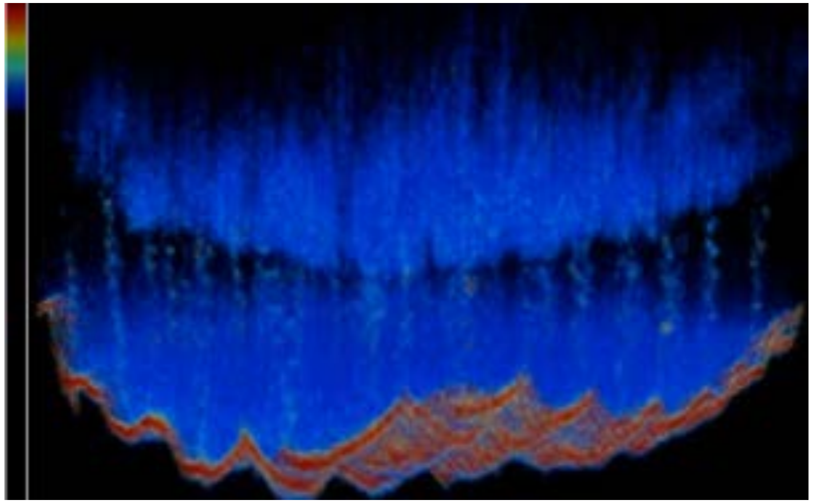


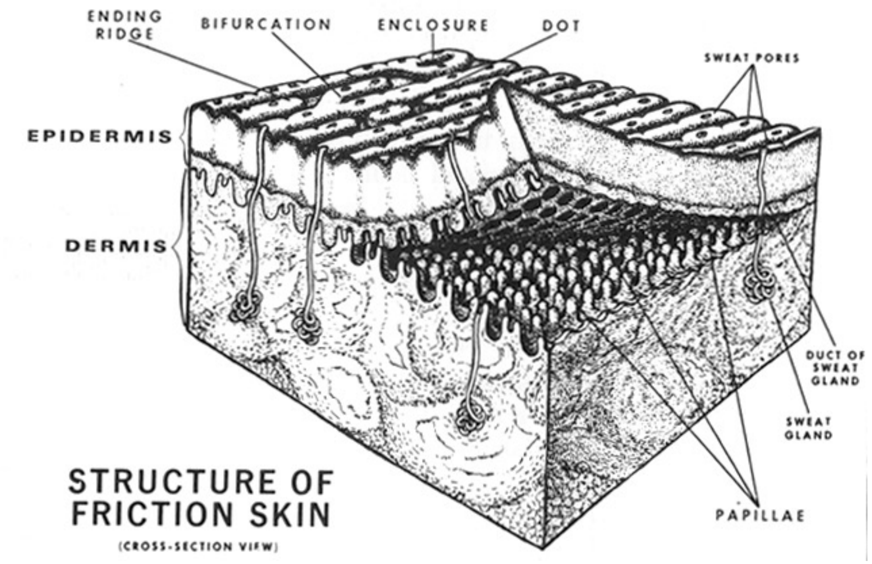
- Conclusion:
  better Presentation Attack Detection than capacitive sensors

Fingerprint Sensor Security

Countermeasures

- Observation of the live skin properties
- Observation of the sweat glandes
- Sensors
  - Optical Coherence Tomography (OCT)

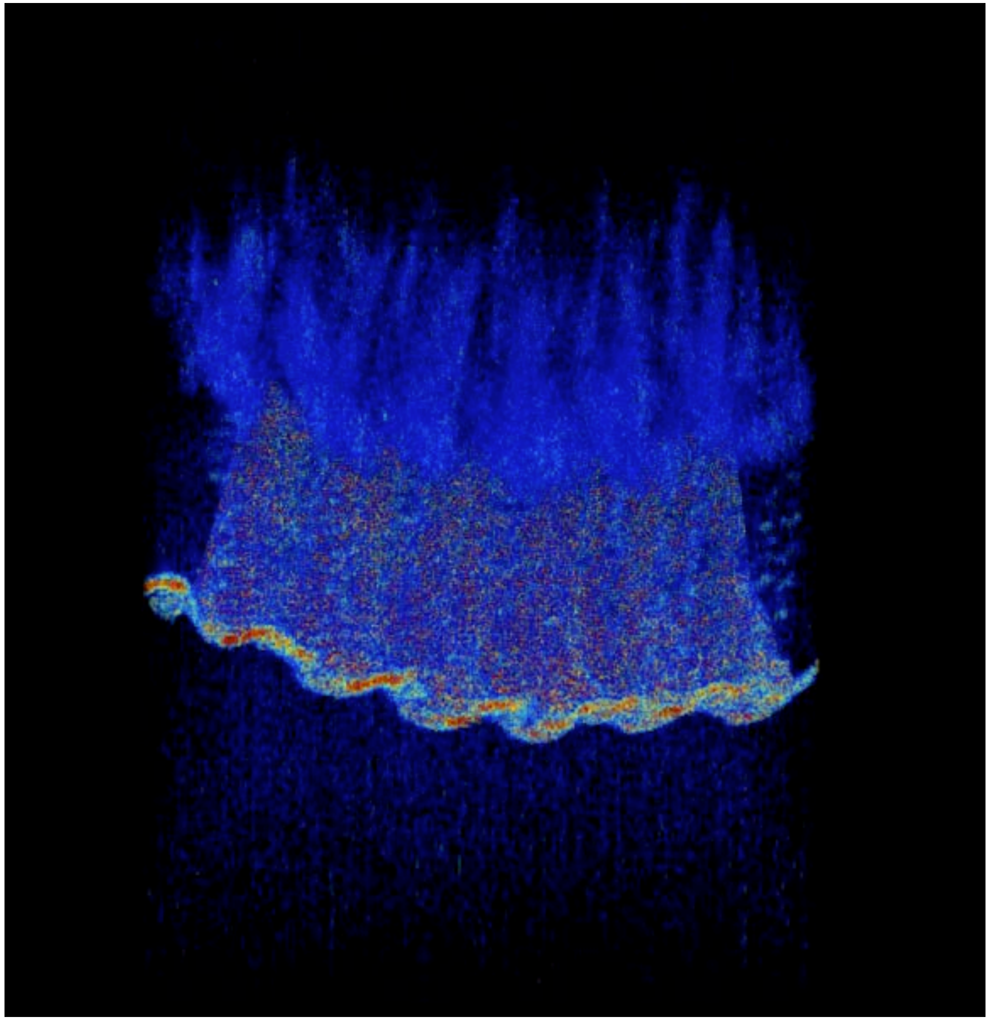




Fingerprint Sensor Security

OCT

- Visualization of sweat glands
  - good scan



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

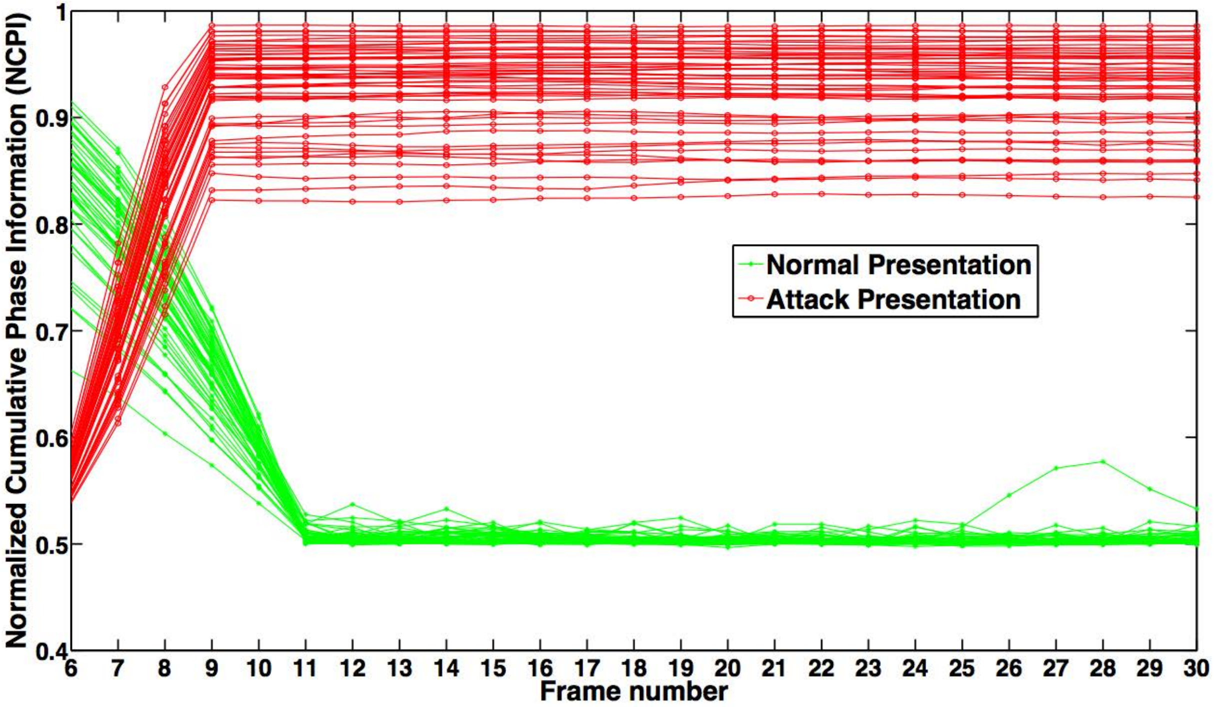
Method based on Eulerian Video Magnification (EVM)

[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

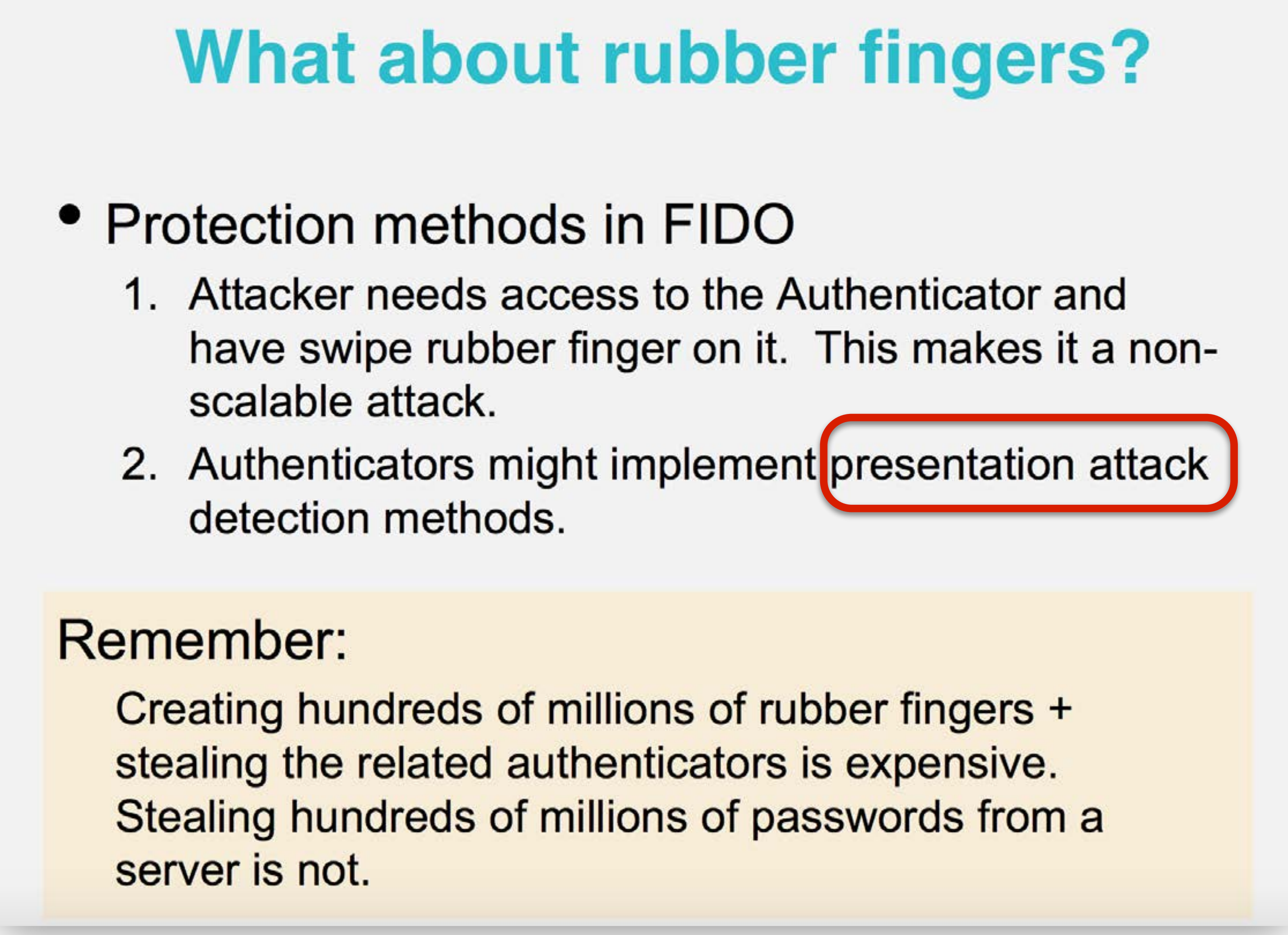


- Zero Error Rates:
  - APCER = 0 %
  - BPCER = 0 %

[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 - on 9th September 2015



What about rubber fingers?

- Protection methods in FIDO
  1. Attacker needs access to the Authenticator and have swipe rubber finger on it. This makes it a non-scalable attack.
  2. Authenticators might implement presentation attack detection methods.

Remember:

Creating hundreds of millions of rubber fingers + stealing the related authenticators is expensive. Stealing hundreds of millions of passwords from a server is not.

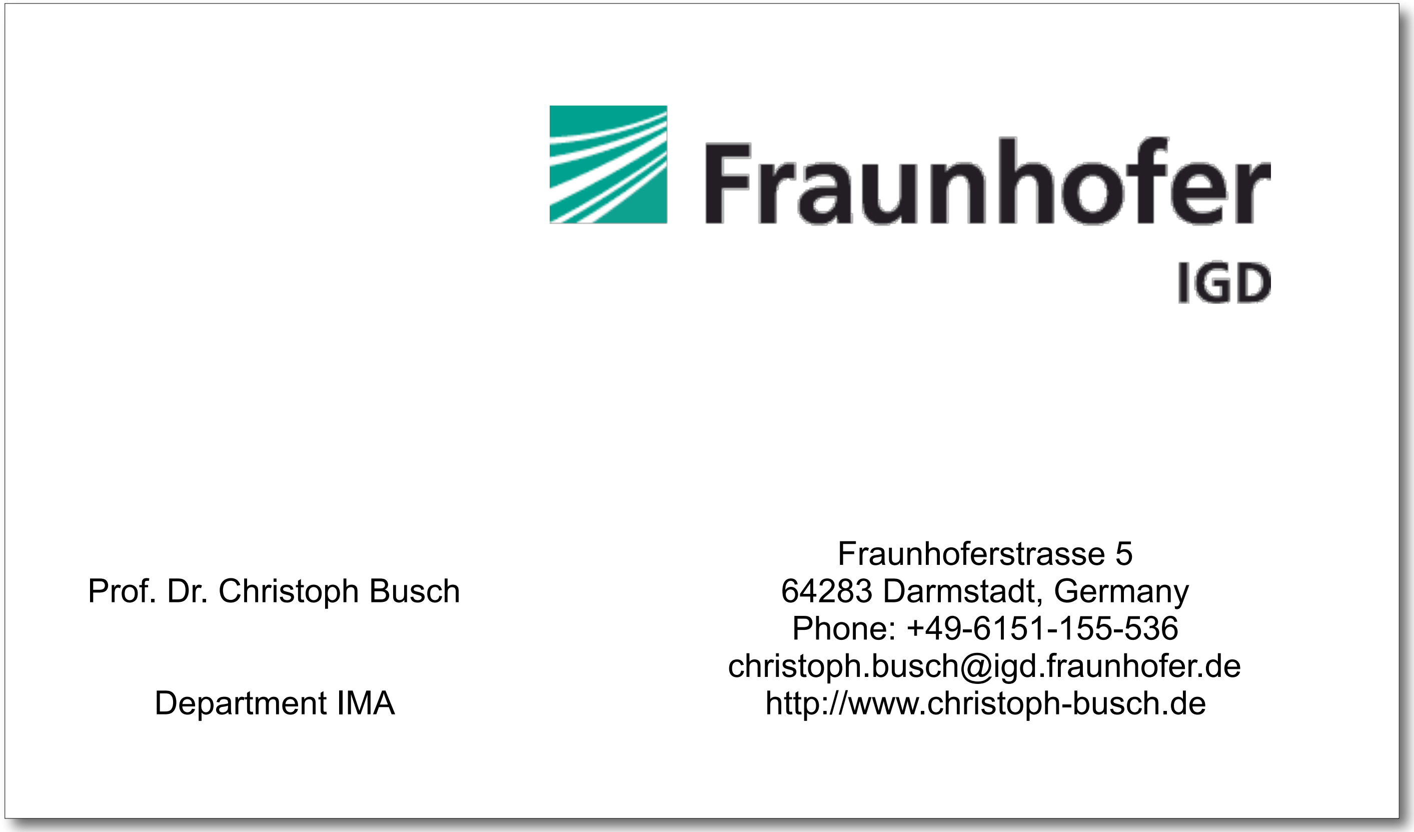
Source: R. Lindemann (NokNok) - 2015

References

Web

- Convenors website with latest news and slides
  http://www.christoph-busch.de/standards-sc37wg3.html
- ISO/IEC JTC SC37
  http://isotc.iso.org/livelink/livelink?func=ll&objId=2262372&objAction=browse&sort=name
- Published ISO/IEC Standards
  http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on

Contact



Fraunhofer

IGD

Prof. Dr. Christoph Busch

Department IMA

Fraunhoferstrasse 5
64283 Darmstadt, Germany
Phone: +49-6151-155-536
christoph.busch@igd.fraunhofer.de
http://www.christoph-busch.de