ISO/IEC 30107 Standards on PAD

Christoph Busch

Gjøvik University College
http://www.christoph-busch.de

Norwegian Biometrics Laboratory Annual Workshop (NBLAW-2015)

Gjøvik - 2015-03-02

Agenda

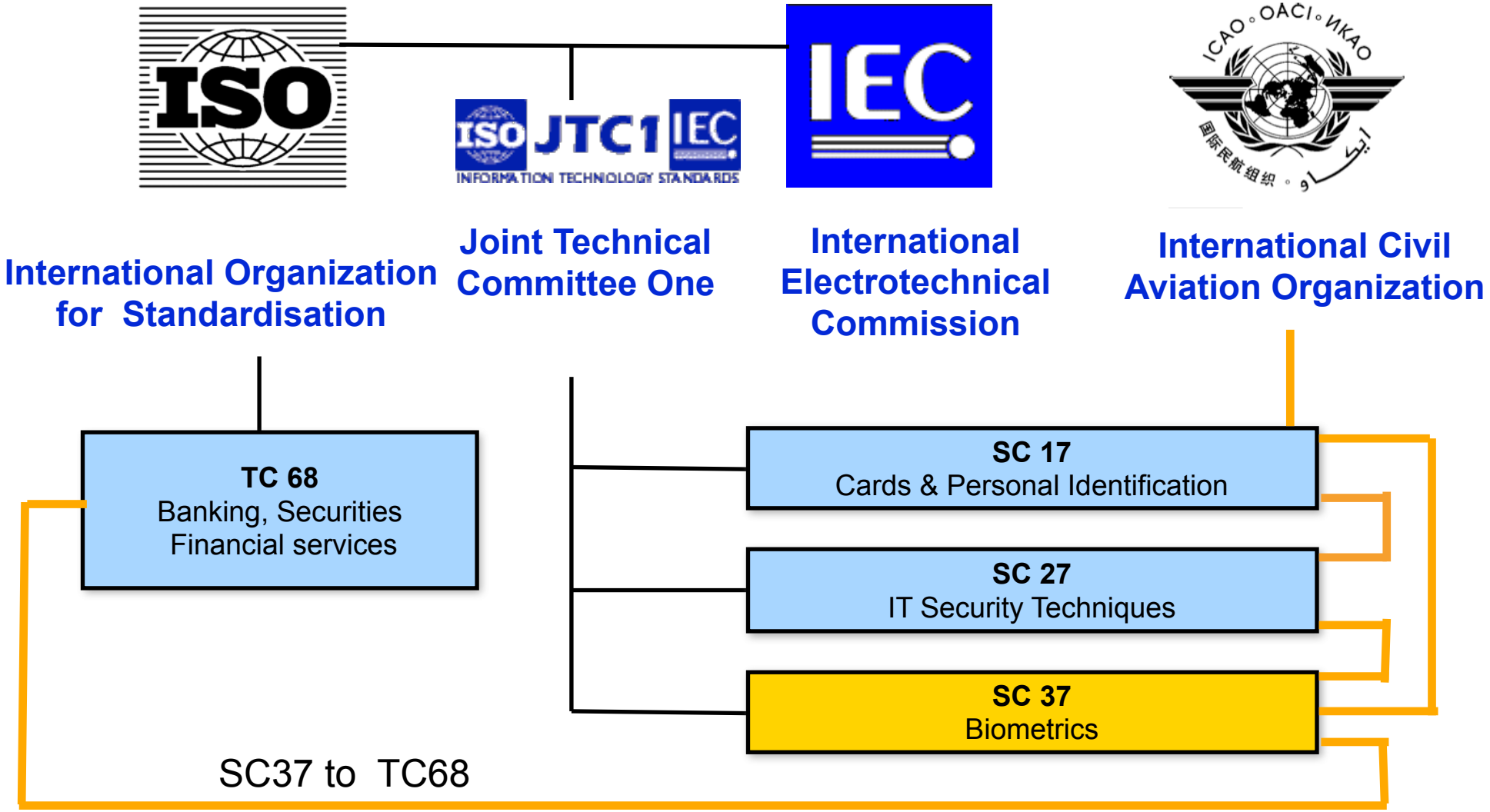
- Certification is important and requested
- Existing International Standardisation
- Performance Testing
- Development of the Presentation Attack Detection Standard
- Conclusion
  - research needs standardisation
  - standardisation needs resarch

International Standardisation

Biometric Standardisation

How does standardisation work?

Biometric Standardisation



ISO/IEC SC37 Biometrics

Established by JTC 1 in June 2002 to ensure

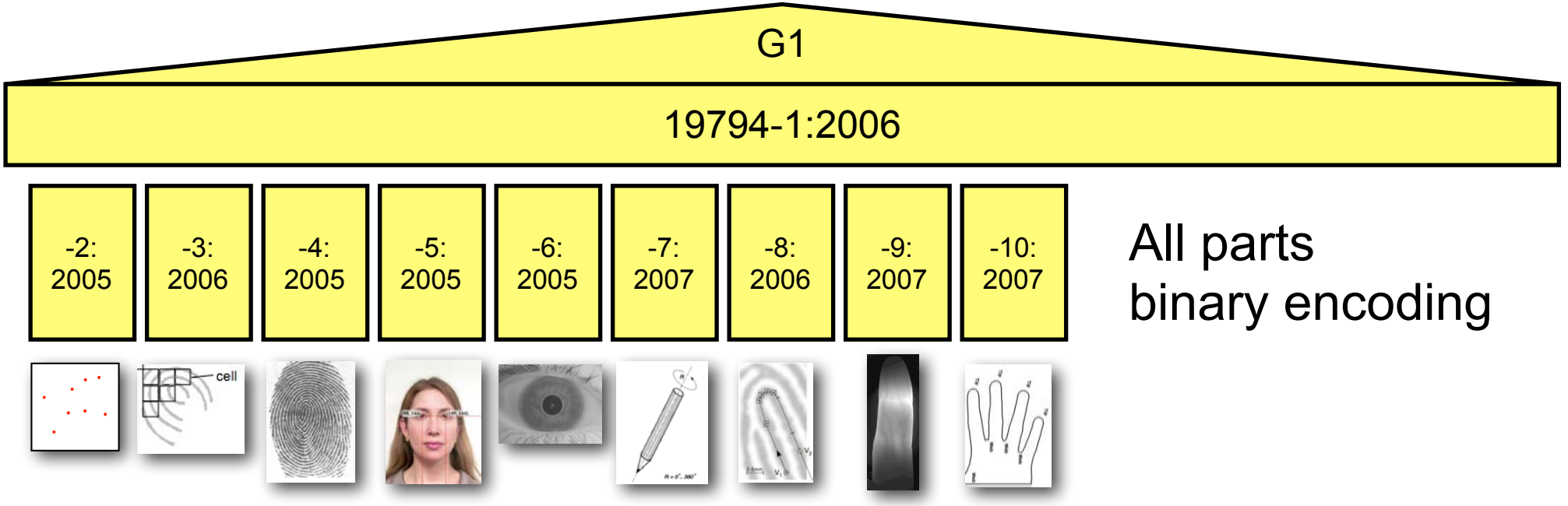
- a high-priority, focused and comprehensive approach worldwide for the rapid development of formal generic biometric standards

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: June 2015 in Gjøvik

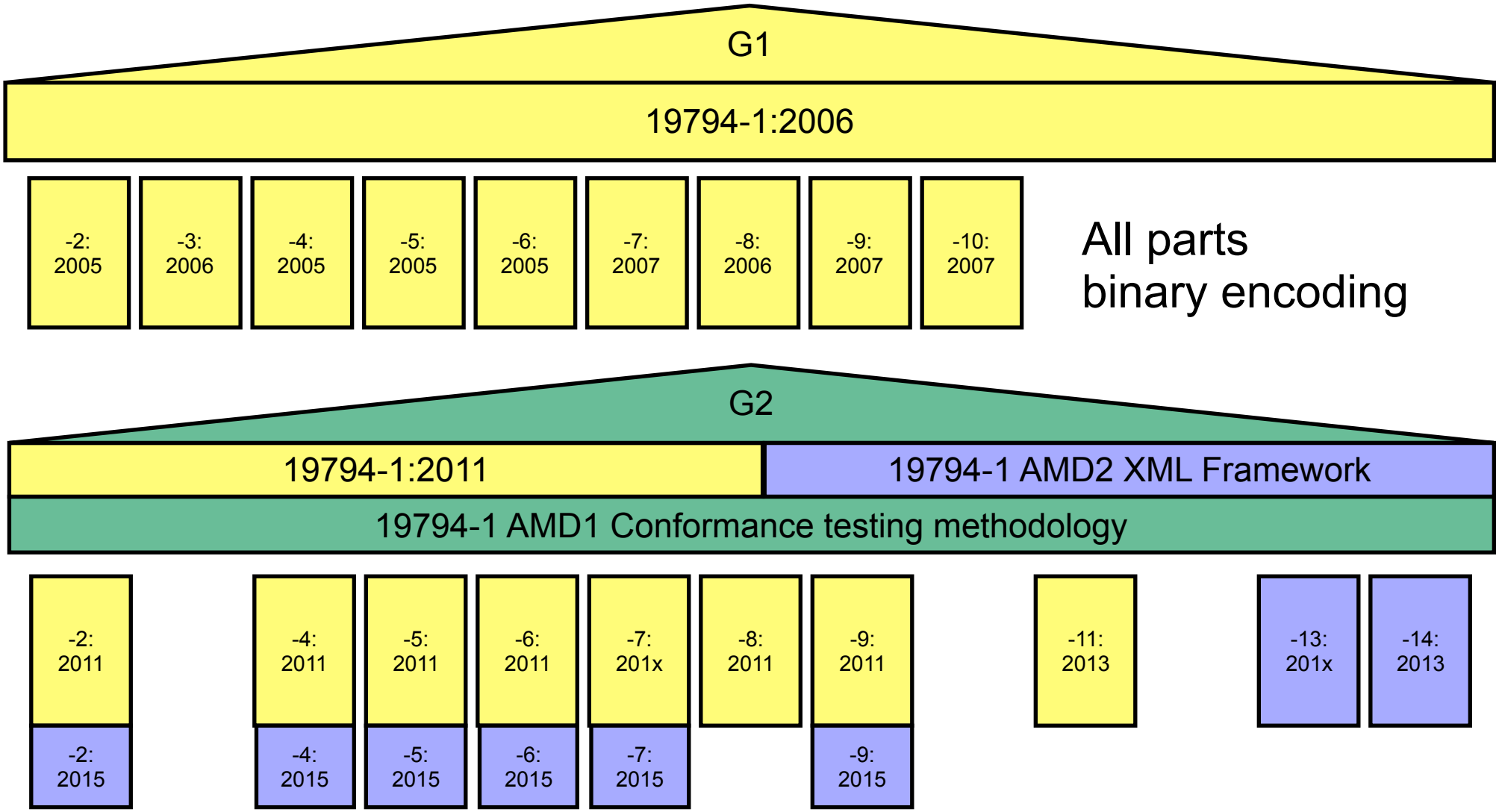
ISO/IEC Interchange Format Standards



All parts
binary encoding

The 19794-Family: Biometric data interchange formats

Generation 2 of ISO/IEC 19794



the semantic is equivalent for binary encoded and XML encoded records

Biometric Performance Testing
ISO/IEC 19795-1:2006

Biometric Performance Testing Standard

ISO/IEC 19795-x, Information technology - Biometric performance testing and reporting

- Part 1: Principles & Framework
  - Guidance applicable to the broad range of tests
- Part 2: Testing Methodologies for Technology and Scenario Evaluation
  - Multiple visits, habituation, enrolment
- Part 3: Modality-Specific Testing
  - Modality (& application) specific methodologies
- Part 4: Interoperability Performance Testing
  - Performance on other vendors data
- Part 5: Framework for biometric device performance evaluation for access control
- Part 6: Testing Methodologies for Operational Evaluation
- Part 7: Testing of ISO/IEC 7816-based Verification Algorithms

Performance Metrics

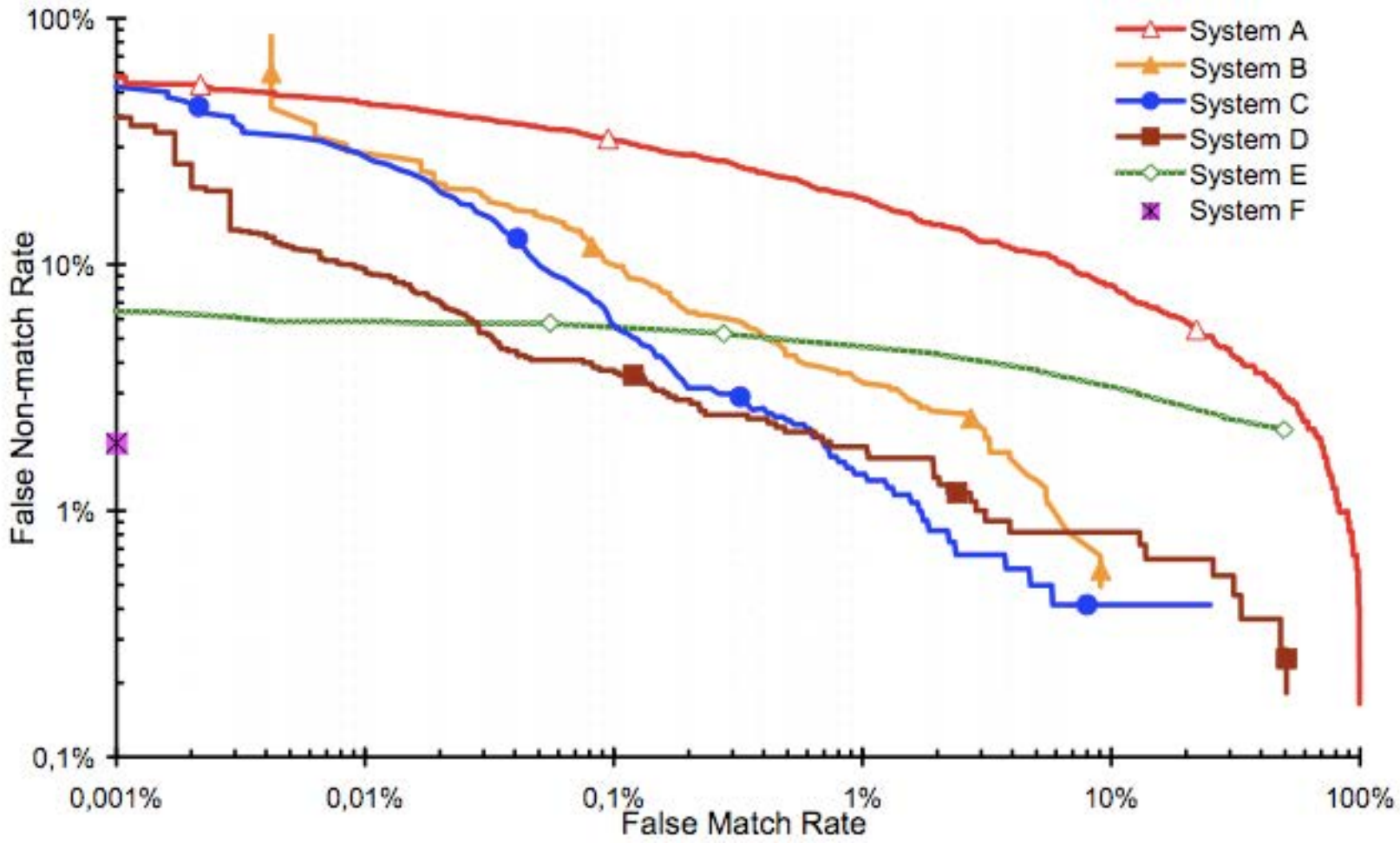
Categorization

- Technology testing
  - Algorithmic level verfication error
    - False-Match-Rate (FMR) - algorithm accepts „zero-effort“ imposter
    - False-Non-Match-Rate (FNMR) - algorithm rejects true identity
- Scenario testing and operartional testing
  - System level verification error
    - False-Accept-Rate (FAR)
    - False-Reject-Rate (FRR)
  - System level error requires observation of:
    - Sample generation: Failure-to-Capture (FTC)
    - Enrolment: Failure-to-Enrol (FTE) - no reference for this subject
    - Verification: Failure-to-Acquire (FTA) - no probe feature vector

Graphical Presentation

DET curve (detection error trade-off curve)

- modified ROC curve which plots error rates on both axes (false positives on the x-axis and false negatives on the y-axis)



Vulnerability Testing has a History

Gummy Finger Production in 2000 !

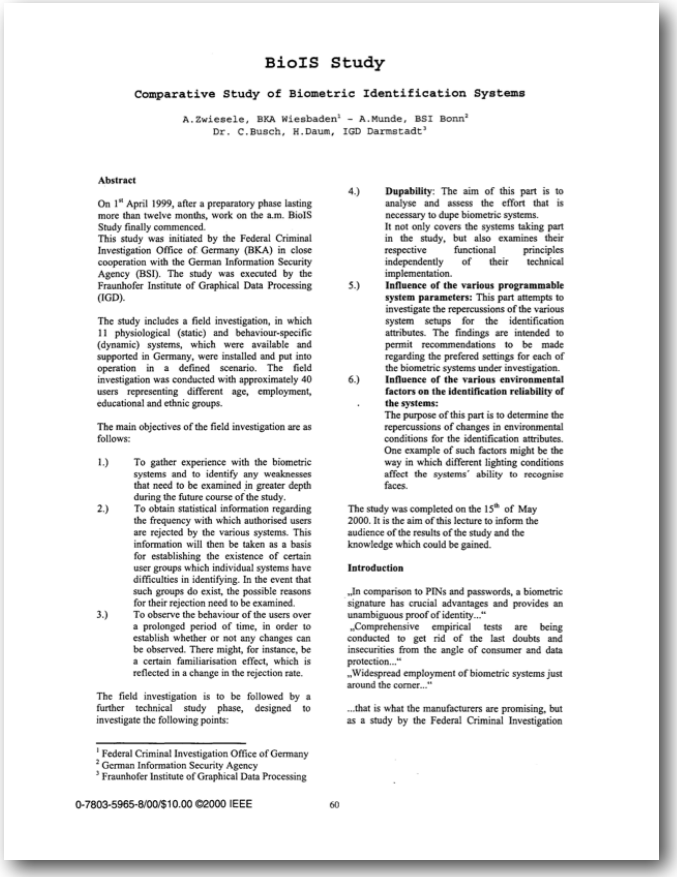
Attack without support of an enroled individual

- 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 platine

Gummy Finger Production in 2000 !

Reported in a publication by BKA

- 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 appoximately 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..."

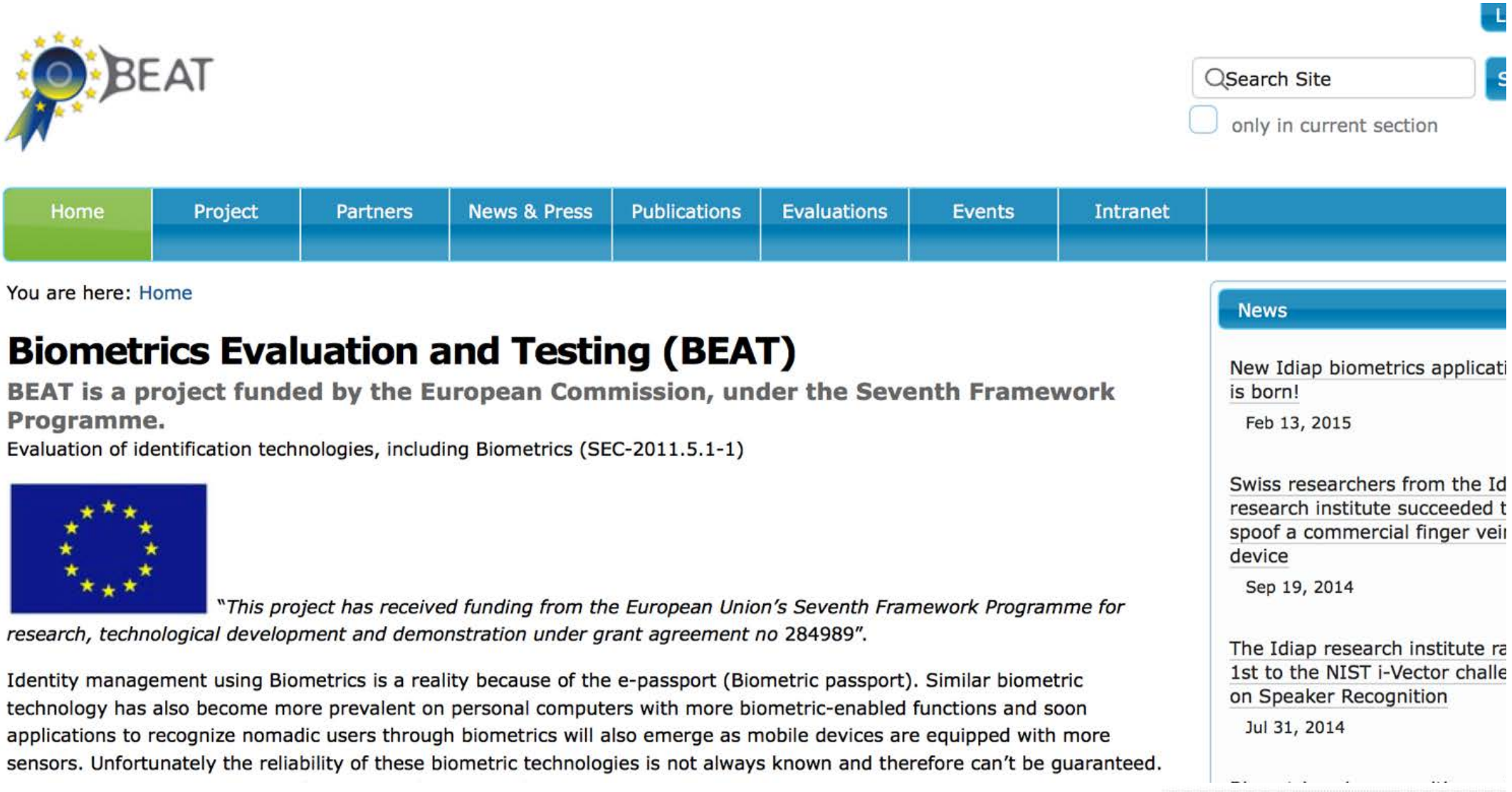
...that is what the manufacturers are promising, but as a study by the Federal Criminal Investigation

[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

Diversity of Testing Methodologies

Testing Projects 2009 - 2015



Diversity of Testing Methodologies

Confusion about concepts and terminology

- Examples: *Gummyfinger, anti-spoofing, artefact detection, spoof detection, fake detection, sensor robustness, imposter detection, liveness detection, fingerprint alteration detection, ... ???*

Diversity of Testing Methodologies

Confusion about concepts and terminology

- Examples: *Gummyfinger, anti-spoofing, artefact detection, spoof detection, fake detection, sensor robustness, imposter detection, liveness detection, fingerprint alteration detection, ... ???*

Diversity of Testing Methodologies

Confusion about concepts and terminology

- Examples: *Gummyfinger, anti-spoofing, artefact detection, spoof detection, fake detection, sensor robustness, imposter detection, liveness detection, fingerprint alteration detection, ... ???*

Confusion about metrics

- for security testing
- for technology testing
- Examples: *FAR/FRR, Fcorrlive, Fcorrfake, Ferrlive, Ferrfake, FalseReal, TrueFake, FalseFake, TrueReal, OverallFAR ???*

- Without a common understanding and common metrics we can not benchmark different technological approaches

Standards on PAD -
The mutlipart standard ISO/IEC 30107

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

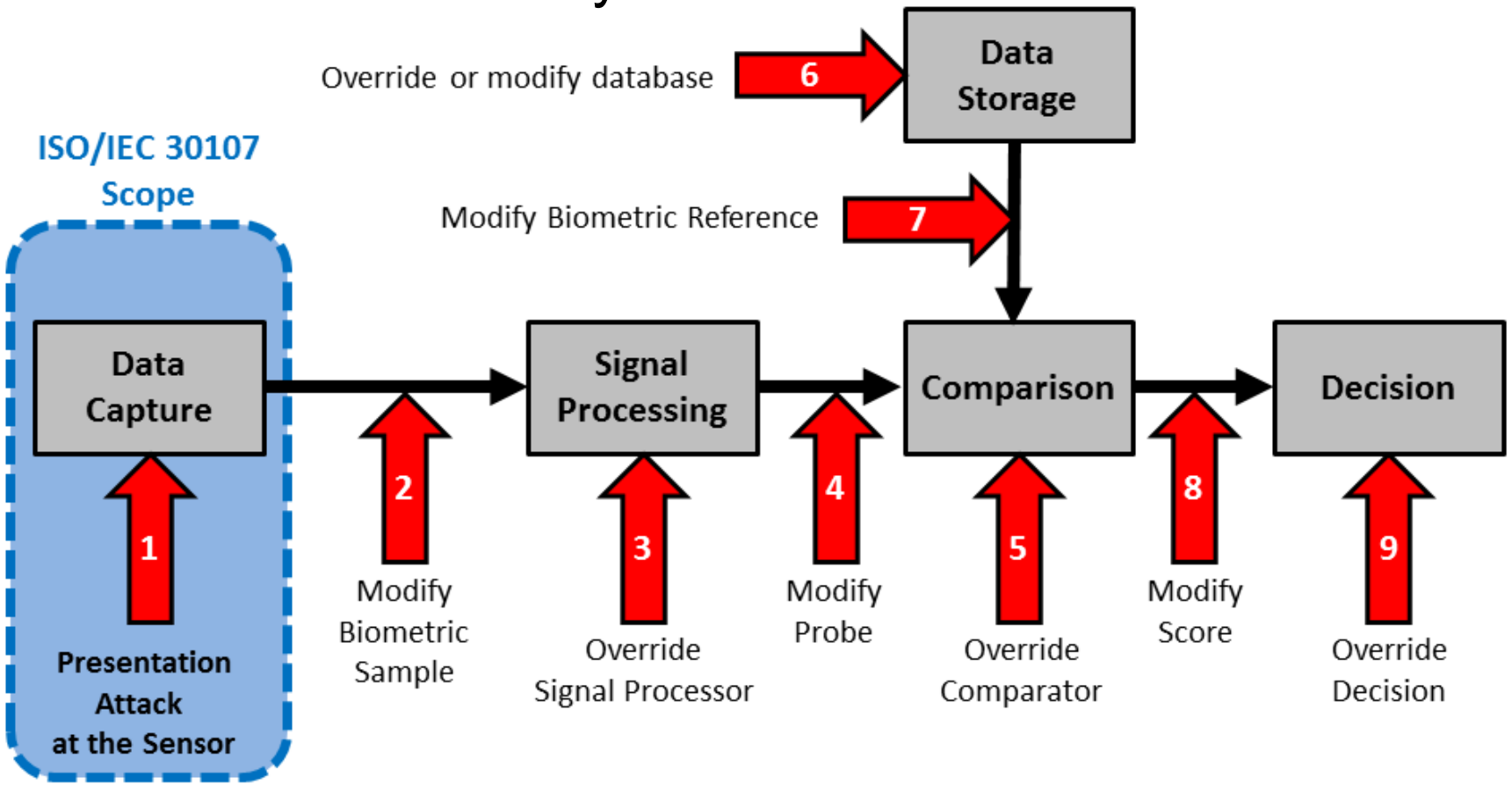
Outside the scope are

- 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.

Liveness Detection

ISO/IEC DIS 30107-1 - 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

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
Examples of Artificial and Human Attack Presentation

Artificial	*Complete*	gummy finger, video of face
	Partial	glue on finger, sunglasses, artificial/patterned contact lens, non-permanent make up
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

ISO/IEC 30107 - Definitions

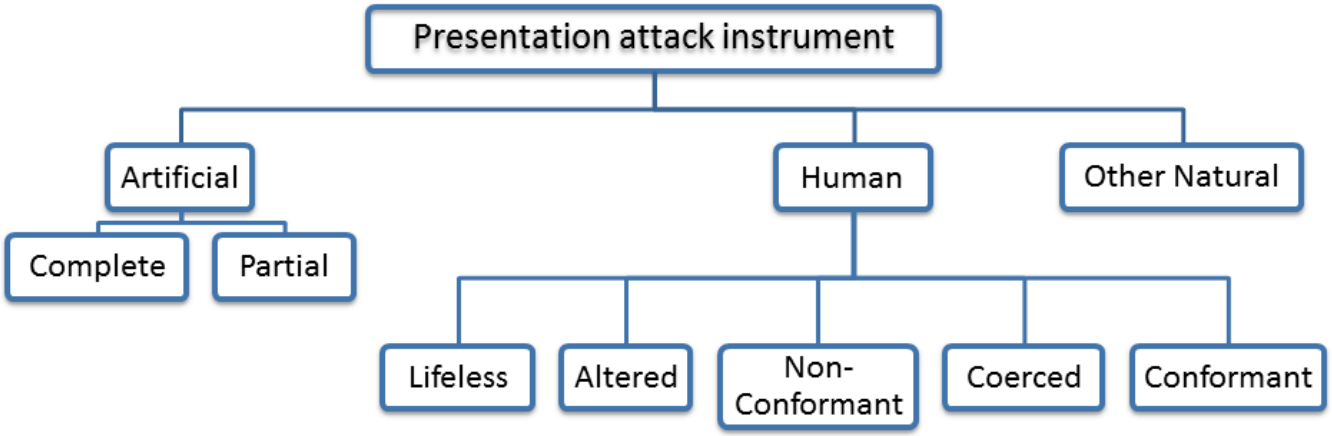
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

(Adjectives describing categories)

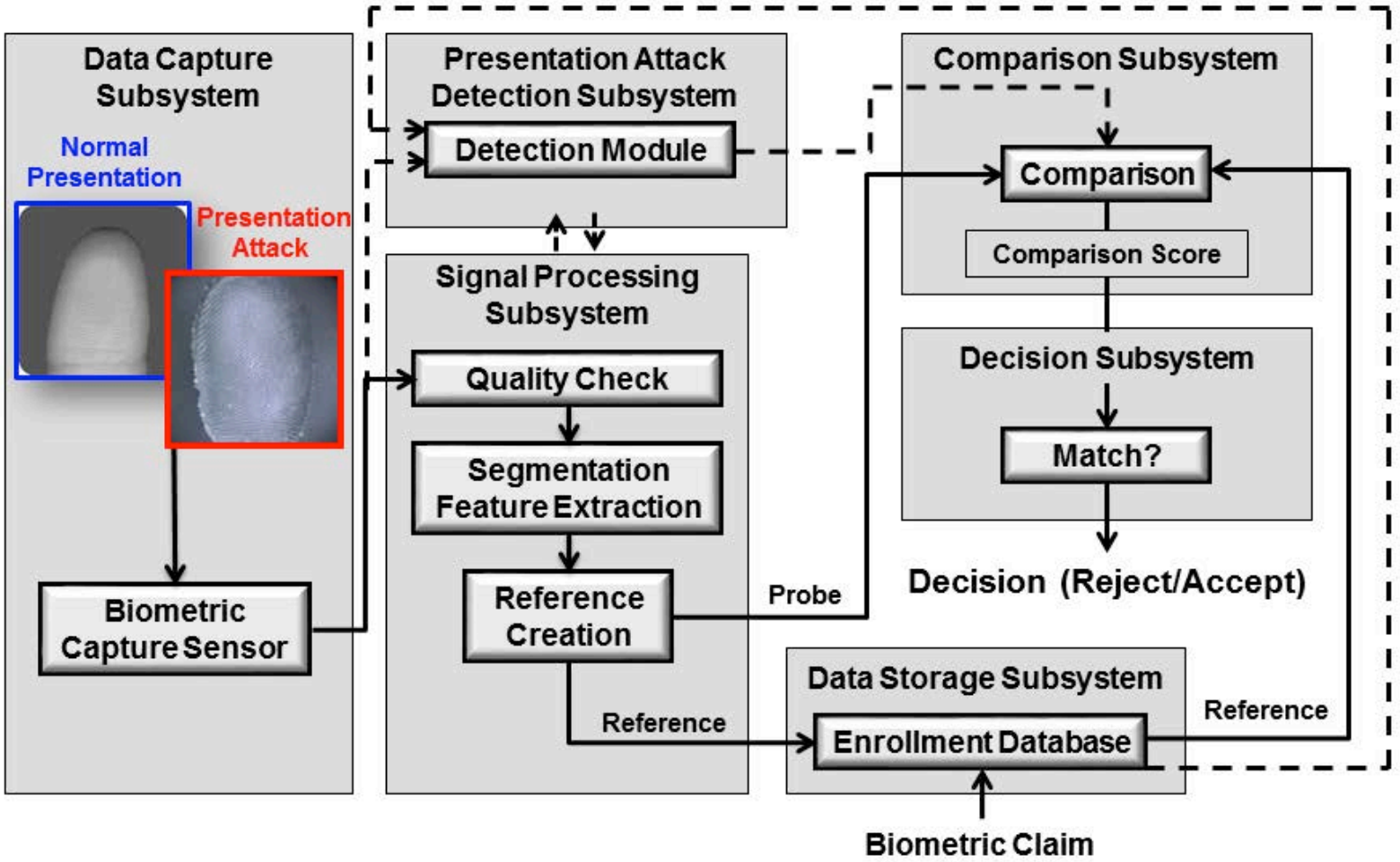
(Qualifying adjectives)



Source: ISO/IEC 30107-1

Presentation Attack Detection

Biometric framework with PAD



Source: ISO/IEC 30107-1

Reporting about the PAD using ISO/IEC 30107-3

PAD-Standard

Methodology in ISO/IEC 30107 Presentation Attack Detection - Part 3: Testing and reporting

- Security Evaluation
  - for evaluations using the Common Criteria Framework
  - Protection Profile (PP) (e.g. from German BSI)
  - Security Target (ST)
  - Evaluation Assurance Level (EAL)
  - Assessment of the attack potential
  - *„if there is at least one aretefact that can reproducibly successful attack the PAD-component - then the PAD failed the test“*
- Other approaches
  - for evaluations in academic and technology development
  - tolerating the limited statistical significance of small test set
    - the statistical distribution is unknown and for sure not normal
  - *„ a score based metric can tell us, if the method improved“*

PAD-Standard

Definition of harmonized metrics in ISO/IEC 30107-3

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

- **Normal presentation classification error rate (NPCER)**
  proportion of normal presentations incorrectly classified as attack presentations at the component level in a specific scenario

PAD-Standard

Assessment of the attack potential in ISO/IEC 30107-3

- **Attack potential**
  attribute of a biometric presentation attack expressing the effort expended in the preparation and execution of the attack in terms of elapsed time, expertise, knowledge about the capture device being attacked, window of opportunity and equipment, graded as Basic, Enhanced-Basic, Moderate, High, or Beyond High

Current ISO/IEC 30107-3 Metrics

Suggested metrics in ISO/IEC 30107-3

- The APCER shall be calculated as follows:

$$APCER = \max_{AS \in \mathcal{A}^{AP}} \frac{1}{N_{AS}} \sum_{i=1}^{N_{AS}} RES_i$$

N_{AS}	number of presentation attack instruments (PAI) (i.e. artefact species) in the corpus
RES_i	result of attack with ith PAI {0 for detected attack, 1 for successful attack}
A^{AP}	set of artefacts species with the same attack potential (this is subset of all artefact species)

Current ISO/IEC 30107-3 Metrics

Suggested metrics in ISO/IEC 30107-3

- The NPCER shall be calculated as follows:

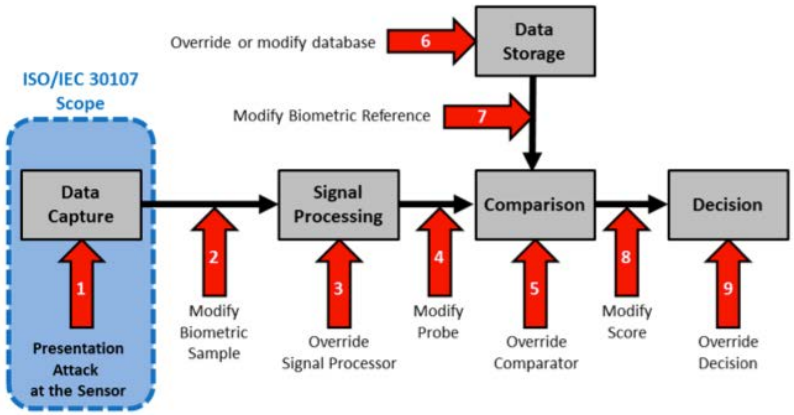
$$NPCER = \frac{\sum_{i=1}^{N_{GPA}} RES_i}{N_{GPA}}$$

N_{GPA}	number of normal presentations from a genuine subject
RES_i	result of presentation detection component for the ith attempt {0 for no detected attack, 1 for false alarm}

Conclusion

The standardisation process is an open process

- Register and contribute to ISO/IEC 30107 Presentation Attack Detection
- Open question:
  - are the metrics sound?
  - should PAD metrics and performance metrics be merged ?



- Research needs standardisation
- Standardisation needs resarch

References

Web

- WG3 onvenors website with latest news
  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
- Wikipedia
  http://en.wikipedia.org/wiki/ISO/IEC_JTC_1/SC_37
- Published ISO Standards
  http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=313770&published=on&development=on

- ISO/IEC 19795-1:2006, Biometric performance testing and reporting - Part 1:Principles and framework
- ISO/IEC DIS 30107-1, Biometric presentation attack detection - Part 1: Framework
- ISO/IEC WD 30107-3, Biometric presentation attack detection - Part 3: Testing and reporting

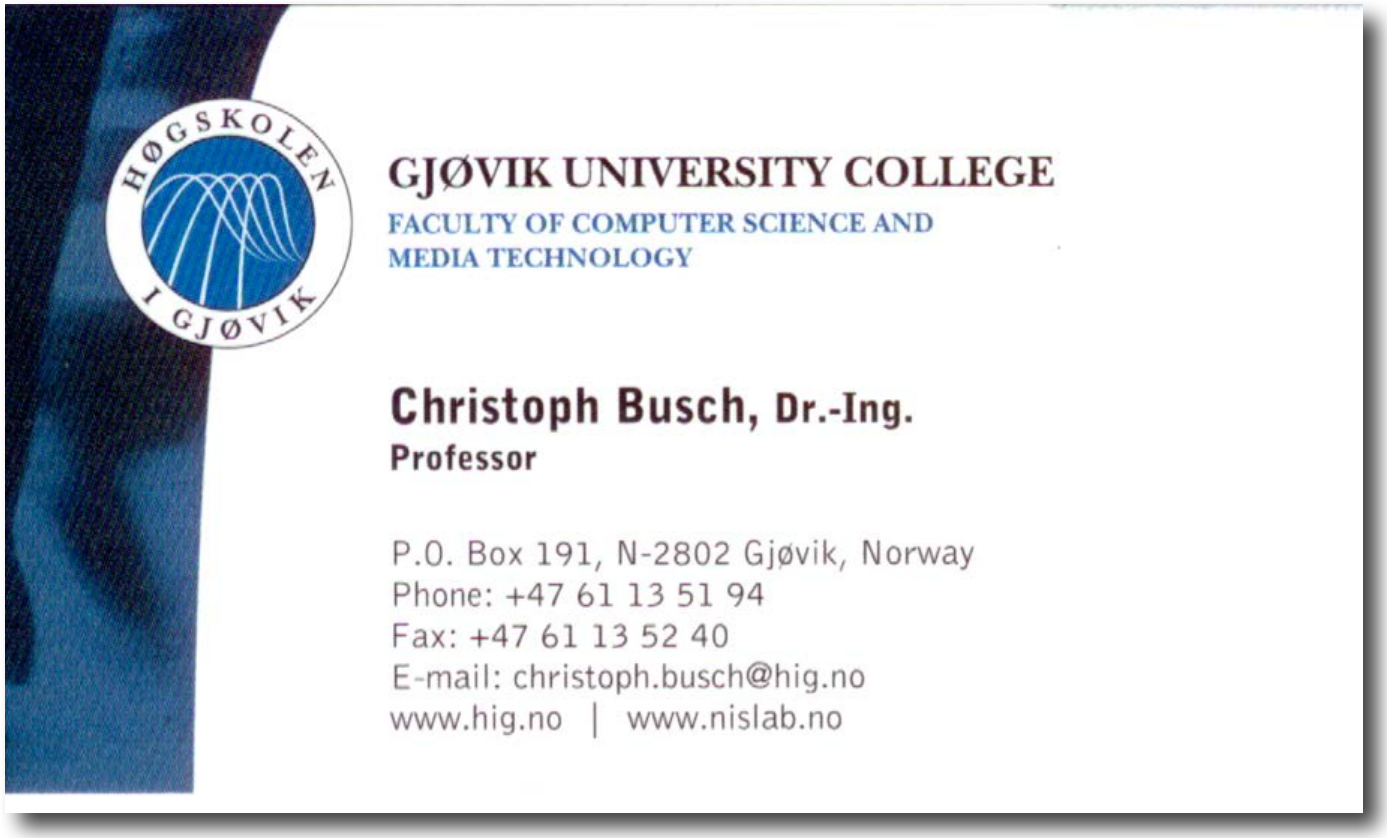
Visit Gjøvik again in 2015

ISO/IEC JTC1 SC37 Conference

- Working Group Meetings
- June 22 to 26, 2015 in GUC
- Standards Norge http://www.standard.no/sc37

We are seeking Sponsors for the SC37 - conference

Contact


HØGSKOLEN I GJØVIK
GJØVIK UNIVERSITY COLLEGE
FACULTY OF COMPUTER SCIENCE AND MEDIA TECHNOLOGY
Christoph Busch, Dr.-Ing.
Professor
P.O. Box 191, N-2802 Gjøvik, Norway
Phone: +47 61 13 51 94
Fax: +47 61 13 52 40
E-mail: christoph.busch@hig.no
www.hig.no | www.nislab.no