Requirements of Liveliness and Fake Finger Detection Test

Views from industry and discussion

Aashish Banati

22 December 2015

Threats to Biometric System

- Artificially created biometrics: e.g. image of a face or iris, lifted latent fingerprints, artificial fingers, high quality voice recordings, etc.
- Attacking via input port.
- Attacking the biometric database.
- Spoofing: “ The process of defeating a biometric system through the introduction of fake biometric samples.”

Vulnerability Testing

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

Presentation Attack Detection

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

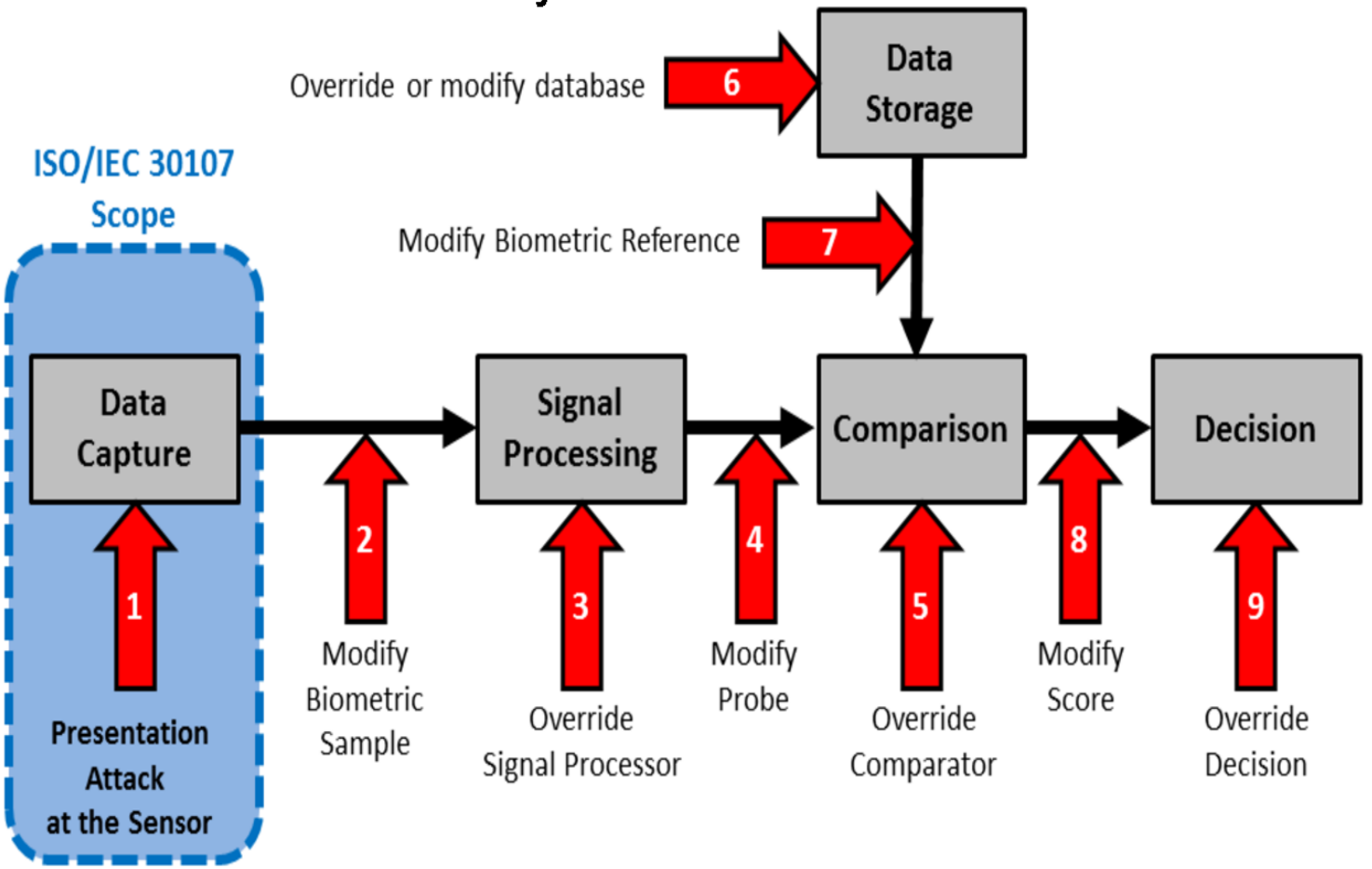
Scope

- 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



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

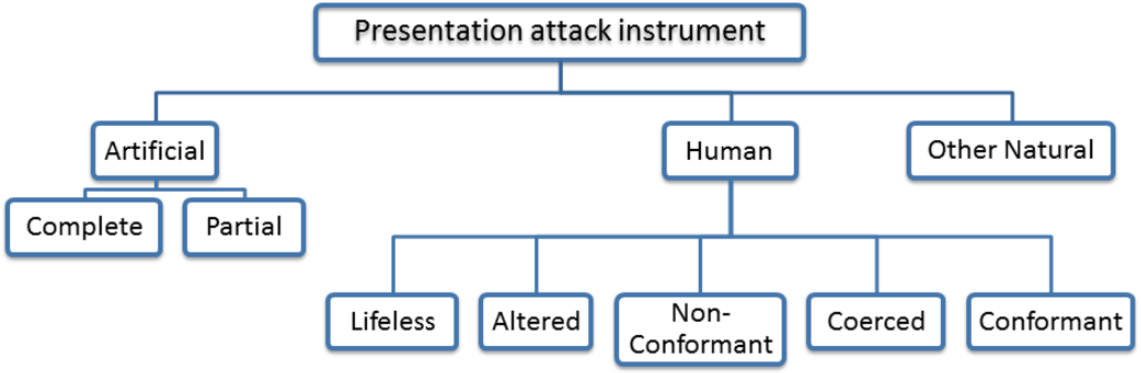
- **presentation attack instrument (PAI)**
  biometric characteristic or object used in a presentation attack
- **artefact**
  artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks

(General Noun)

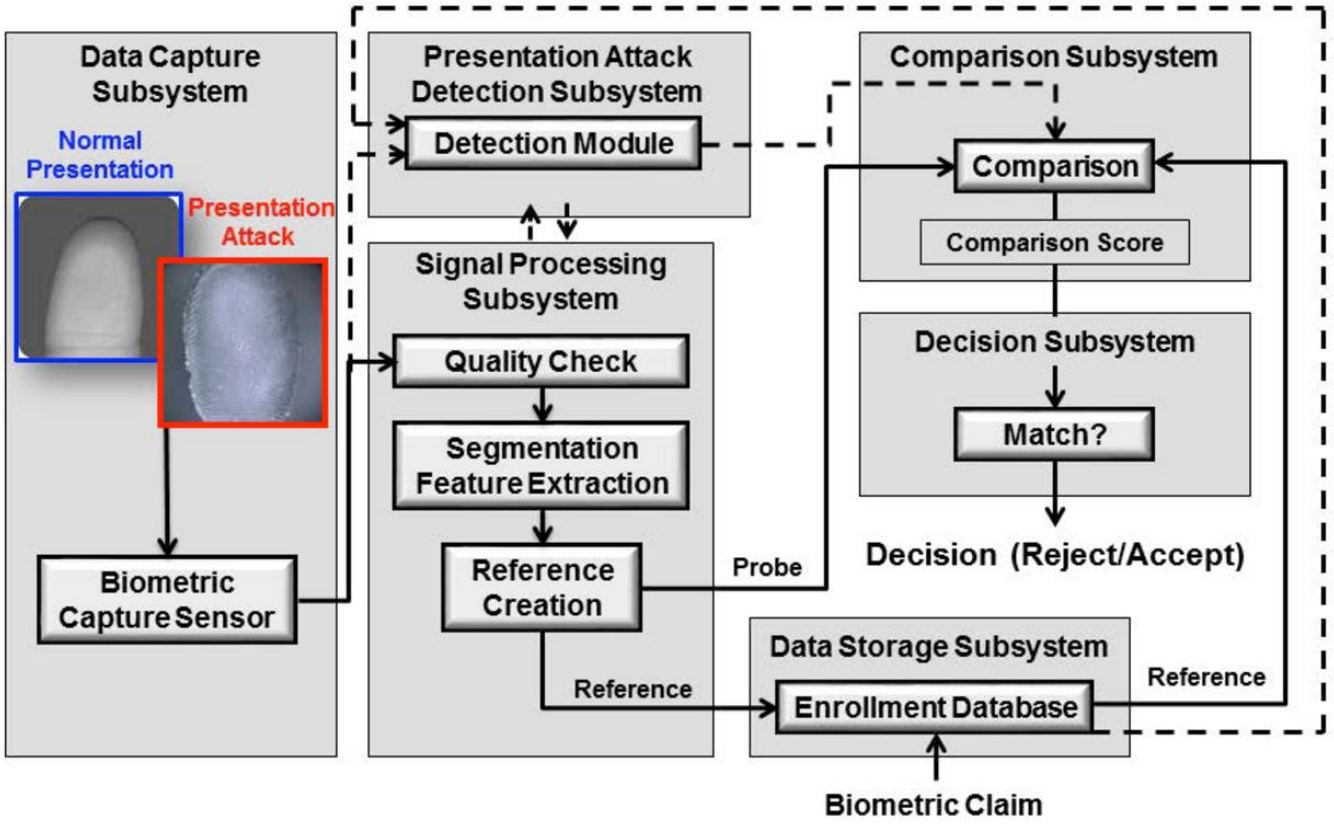
(Adjectives describing categories)

(Qualifying adjectives)



Presentation Attack Detection

Biometric framework with PAD



Conclusion

- Liveness enhances the security of the biometric system by only considering the "real" features.
- Liveness is a major attribute in individuals' feature space but has very low specificity by itself: it is dichotomy of the feature space into live and non-living.
- Liveness detection reads claimant's physiological signs of life.
- Liveness detection in multi-modal biometric devices has the potential to enhance security, reliability and effectiveness.
- Although biometric authentication devices can be susceptible to spoof attacks, different anti-spoofing techniques can be developed and implemented.
- It requires some **software enhancement** of the biometric system
  eg. Fingerprint : perspiration.
  Face : head movements.
- **Hardware enhancements**

eg.
Fingerprint : temperature sensing, detection of pulse on fingertip
Voice: matching the lip movement (video) to the audio.

Fake Finger Detection

- The use of a Fake Finger is a potential vulnerability on biometric systems; primarily in an unsupervised environment.

- Countermeasures exist, either software based or hardware based (various publication on this aspect describe such countermeasures based on research)
  - Security should not be immutable - devices shall be able to adopt to a new fraud quickly when it is discovered

- Whatever the solution, increasing security impacts False Reject Rate (FRR). Therefore
  - Security level and service rate must be balanced before implementing fake finger counter measures.
  - These should be intended for sensitive applications.

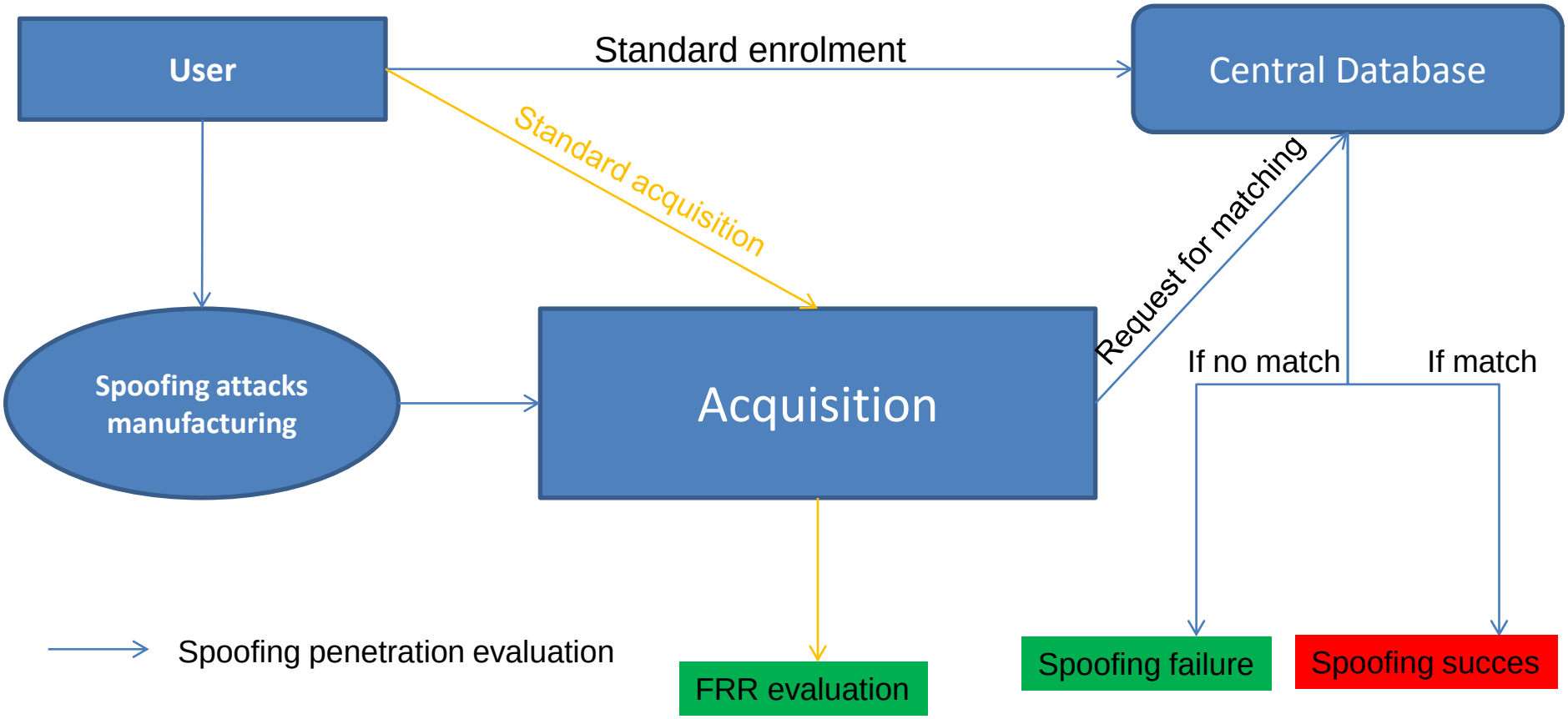
- Security of the whole biometric system is an important factor for system design and spoof prevention is only one part of the security system.

STQC Proposal for Measurement of Fake Finger Detection capability

- Basic Principle
  - Different type of fingerprint sensor use different type of acquisition technologies, so measurement must consider a fully representative set of fakes to account for all such technologies

- Fake finger detection is basically robustness evaluation against fake finger. Therefore,
  - A device is considered robust if it offers 90% average protection over all attacks, than 99% on one kind of attack and 0% on another, because that vulnerability will quickly be known and fraudsters will know they take absolutely NO RISK of being detected while using it. The deterrent effect of the anti-spoofing technology could be quickly nullified.

TEST PROCEDURE



FAR and FRR for FFD tests

- False Acceptance Rate : number of times an impostor using a fake (or using his own fingers) successfully identified as someone he is not divided by number of attacks. Define a minimum acceptation rate to be accepted FOR ALL MATERIALS.

- False Rejection Rate : number of times a genuine user got rejected (based on fake detection OR unsuccessful biometric verification) divided by number of genuine tests. Define a maximum False Reject rate as a very efficient countermeasures can hide a trap : increase considerably the rejection of real finger which will penalize the common user;

Error Rates in ISO/IEC 30107

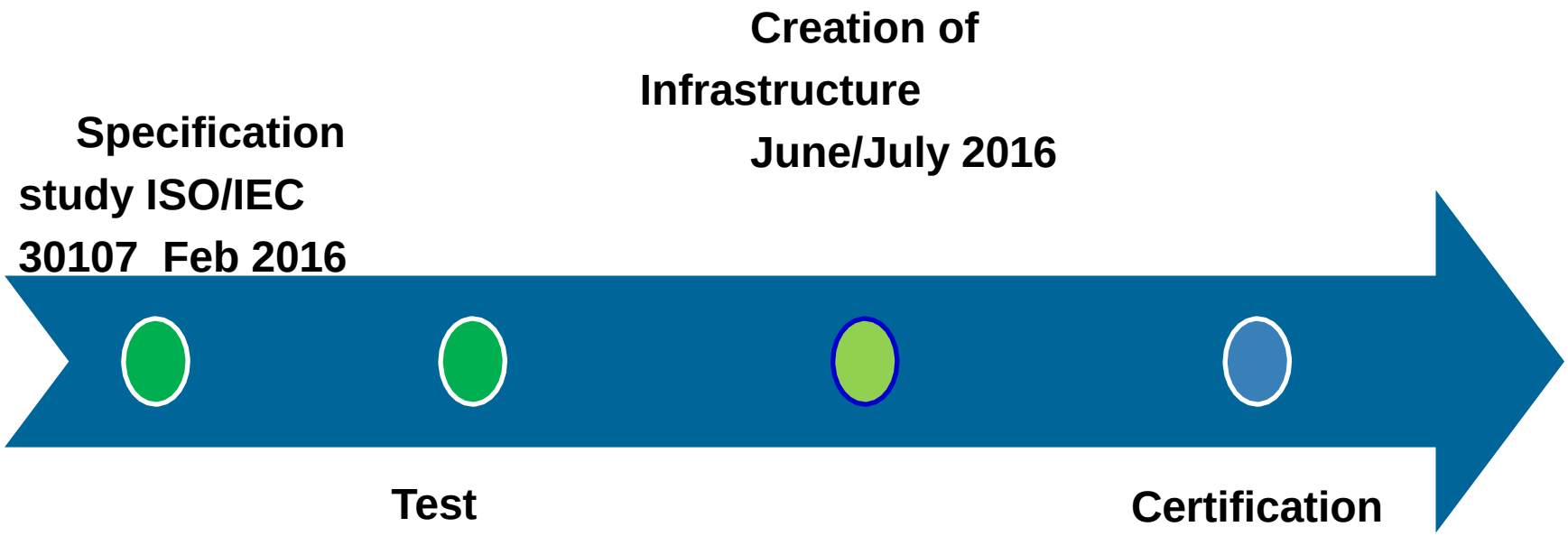
- Detection might result in errors

- ‣presentation attack detection rate (PADR)
  - „proportion of presentation attacks with a defined level of difficulty detected by a system.“

- ‣presentation attack non-detection rate (PA-NDR)
  - „proportion of presentation attacks with a defined level of difficulty not detected by a system.“

- **Note of caution: <u>For security assessment rates are irrelevant, if there exists a single artefact that can break the system</u>**
- ‣presentation attack detection-power level:
  - „level of difficulty of biometric presentation attacks above which the biometric system is not able to detect them.“

Road Map


Specification study ISO/IEC 30107 Feb 2016
Creation of Infrastructure June/July 2016
Test Methodology Standardization April 2016
Certification

THANKS