TABULA RASA

Trusted Biometrics under Spoofing Attacks

http://www.TABULA RASA-euproject.org/

Funded under the 7th FP (Seventh Framework Programme)
Theme ICT-2009.1.4
[Trustworthy Information and Communication Technologies]

D5.7: Standards for security evaluation under spoofing attacks

Due date: 28/02/2014
Submission date: 31/03/2014
Project start date: 01/11/2010
Duration: 42 months
WP Manager: Gian Luca Marcialis (UNICA), Fabio Roli (UNICA)
Revision:

Author(s): S. Revelin (MORPHO)

Project funded by the European Commission in the 7th Framework Programme (2008-2010)		
Dissemination Level		
PU	Public	No
RE	Restricted to a group specified by the consortium (includes Commission Services)	Yes
CO	Confidential, only for members of the consortium (includes Commission Services)	No

Content

1. Introduction

Biometric technologies are used to recognize individuals based on biological and behavioural traits and, consequently, are often used as a component in security systems. A biometric technology assisted security system may attempt to recognize persons who are known as either friends or foes, or may attempt to recognize persons who are unknown to the system as either.

Since the beginnings of these technologies, the possibility of subversion of recognition by determined adversaries has been widely acknowledged, as has the need for countermeasures to detect and defeat subversive recognition attempts, or spoofing attacks. Subversion of the intended function of a biometric technology can take place at any point within a security system and by any actor, whether a system insider or an external adversary.

However, in a context of increasing use of security solutions in ICT systems based on biometrics, the resistance of biometric systems to direct spoofing attacks is a critical issue. Techniques for the automated detection of direct attacks need to be tested and evaluated. A common methodology and best practises to assess the resistance level of a biometric sensor is required for a proper comparison of the performances between different systems. The definition of standards and norms for security evaluation of biometric product facing spoofing attack will increase the trust of the users in the biometric technologies.

The purpose of this document is to describe the current (and not necessarily aligned) initiatives and work at the international and European level towards the adoption of standards for the security evaluation of biometric products when facing direct attacks.

2. From standards to certification: the advantage

Adoption of international standard or norm for security evaluation of biometric sensors would lead to the establishment of recognised certification label (granted, in Europe, by independent European Certification Bodies).

Certification of biometric products is a way to guarantee their resistance up to a certain level and then will rapidly become a critical issue for biometric actors to create trust to their customers. The generalization of evaluation scheme to biometrics devices would offer to European industry a service for valorising its know-how in the development of secure systems

European Certification Bodies always pushed for high quality certification methodologies for security product. France, especially, through the French Certification Scheme, has often been a leader in the evaluation of Security Components. It has always promoted the idea of a strong technical content of evaluations giving to the Certificates a real added value both from the developers and the users.

Biometric solutions manufacturers and sellers would benefit from the enhancement of security provided by the establishment of a standardised certification methodology. They would introduce in their portfolio evaluated biometric products exhibiting a security certification label. This label has a significant interest for industries because it will act as a differentiator between biometrics products with apparently identical features but different level of performance. Certified products will then contribute to enhance the image of companies proposing high quality sensors.

Common Criteria (CC) methodology, a certification norm used worldwide (for smart cards security evaluation for instance), is often pointed out as a possible reference for biometric sensors evaluation and certification. The advantage to rely an international well-known standard is that the methodology already proved to be efficient and reliable and can accelerate its wide adoption by the international biometric community. Nonetheless, other standards based on different methodologies are under study.

3. The ISO initiative

3.1 ISO organisation

ISO (International Organization for Standardization) is the world's largest developer of voluntary International Standards. International Standards give state of the art specifications for products, services and good practice, helping to make industry more efficient and effective. Developed through global consensus, they help to break down barriers to international trade.

ISO develops International Standards. The ISO story began in 1946 when delegates from 25 countries met at the Institute of Civil Engineers in London and decided to create a new international organization 'to facilitate the international coordination and unification of industrial standards'. In February 1947 the new organisation, ISO, officially began operations.

Since then, ISO has published over 19 500 International Standards covering almost all aspects of technology, business and manufacturing. From food safety to computers, and agriculture to healthcare, ISO International Standards impact all our lives.

ISO is a network of national standards bodies. These national standards bodies make up the ISO membership and they represent ISO in their country. Today the organisation has members from 161 countries and 3 368 technical bodies to take care of standard development. More than 150 people work full time for ISO's Central Secretariat in Geneva, Switzerland.

ISO International Standards ensure that products and services are safe, reliable and of good quality. For business, they are strategic tools that reduce costs by minimizing waste and errors and increasing productivity. They help companies to access new markets, level the playing field for developing countries and facilitate free and fair global trade.

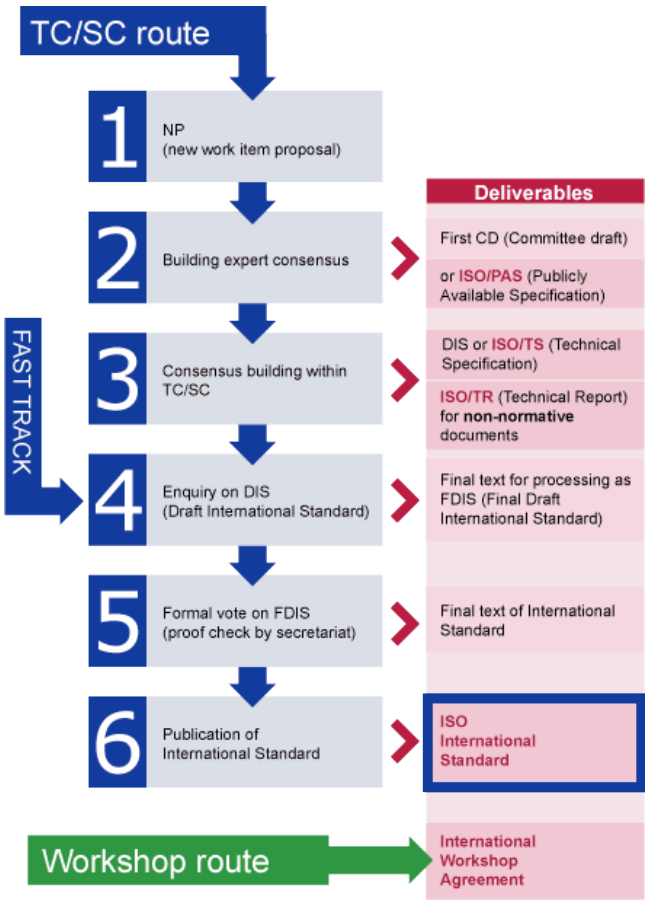
ISO Standards are developed by the people needing them, through a consensus process. Experts from all over the world develop the standards that are required by their sector. This means they reflect a wealth of international experience and knowledge.

3.2 ISO Standard

This is a normative document, developed according to consensus procedures, which has been approved by the ISO membership and participating members (P-members) of the responsible committee in accordance with Part 1 of the ISO/IEC Directives as a draft International Standard and/or as a final draft International Standard and which has been published by the ISO Central Secretariat.

A text corresponding to an approved work item is developed as necessary through the preparatory and/or the committee stages until consensus is reached in the committee. (In case of doubt, approval by 2/3 of the P-members voting may be considered to constitute consensus.) The text is submitted to all ISO member bodies for a five-month vote as a draft International Standard (DIS) and is approved if two-thirds of the P-members vote affirmatively and not more than a quarter of all votes cast are negative. A final text is prepared taking into account member body comments on the DIS and this text is issued for

formal vote as a final draft International Standard (FDIS). If the text is again approved by two-thirds of the P-members voting and if not more than a quarter of all votes cast are negative, then the text is approved and the Central Secretariat publishes the International Standard.



An ISO standard is an international recommendation but the implementation of this standard is not mandatory.

3.3 ISO and biometrics

In June 2002, JTC 1 established a new Subcommittee 37 on Biometrics. The goal of this JTC 1 SC is to ensure a high priority, focused, and comprehensive approach worldwide for the rapid development and approval of formal international biometric standards. These standards are necessary to support the rapid deployment of significantly better, open systems standard-based security solutions for purposes such as homeland defence and the prevention of ID theft.

The JTC 1/SC 37 is responsible for the standardisation of biometric technologies pertaining to human beings to support interoperability and data interchange among applications and systems. There are 6 working groups:

- JTC 1/SC 37/WG 1 Harmonized biometric vocabulary
- JTC 1/SC 37/WG 2 Biometric technical interfaces
- JTC 1/SC 37/WG 3 Biometric data interchange formats
- JTC 1/SC 37/WG 4 Biometric functional architecture and related profiles

- JTC 1/SC 37/WG 5 Biometric testing and reporting
- JTC 1/SC 37/WG 6 Cross-Jurisdictional and Societal Aspects of Biometrics

As at July 2012, there are 79 ISO standards published under the direct responsibility of JTC 1/SC 37.

3.4 ISO initiative for anti-spoofing

3.4.1 Scope

In recent years, since 2011, ISO is interested in spoofing attacks for biometric systems. In this direction, ISO has started the working draft ISO/IEC 30107 for Presentation Attack Detection (PAD).

ISO/IEC 30107 was prepared by Technical Committee ISO/TC JTC1, Information Technology, Subcommittee SC 37, Biometrics, WG3. Morpho, who is participating actively in SC37, is naturally involved in this standard development.

This International Standard aims to establish:

- 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

- Standardisation of specific PAD detection methods;
- Detailed information about countermeasures (i.e. anti-spoofing techniques), algorithms, or sensors; and
- Overall system-level security or vulnerability assessment.

The attacks to be considered in this standard are taking place at the sensor during the presentation and collection of the biometric characteristics. Any other attacks are considered outside the scope of this standard.

Although attacks on a biometric system can occur anywhere and be instantiated by any actor, this International Standard will focus on biometric-based attacks on the capture sub-system by data capture subjects intending to subvert the intended operation of the system. Attacks by other actors and at other points of the system have previously been considered in documents. This standard will not address protecting the sensor itself from modification, replacement, or removal from, or its communication with, the biometric system. The term

attack points to what can be done with a biometric presentation, not what can be done to a sensor or other hardware or software component of the biometric system.

Where appropriate, the biometric capture subsystem should be ideally able to detect a biometric attack presentation characteristic, and in some applications take further actions to counter such an attack. Presentation attacks can be of two basic types; An Active Imposter Presentation Attack is where the subversive data capture subject intends to be recognized as an individual other than him/herself. An Identity Concealer Presentation Attack is where the subversive data capture subject intends not to be recognized as any individual known to the system.

Of the first type of attack, there are two sub-types. In the first sub-type, the subversive data subject intends to be recognized as a specific individual known to the system. In the second sub-type, the subversive data subject intents to be recognized as any individual known to the system, without specification as to which.

Of the second type of attack, as opposed to modelling the characteristics of known individuals, the subversive data capture subject will be seeking to conceal his/her own biometric characteristics, e.g., using an artefact or through disguise or alteration of natural biometric characteristics. This type of attack also is decomposable into two subtypes: one in which the attacker will seek later repeatability of the disguised or altered biometric characteristic and one in which the attacker will seek no later use of the characteristic (a "one-time" deception).

Figure 1 illustrates several generic attacks against a biometric system. This document will only focus on attacks pointed out by arrow "1," in which a biometric sample is presented to a sensor which is operating properly within a biometric system.

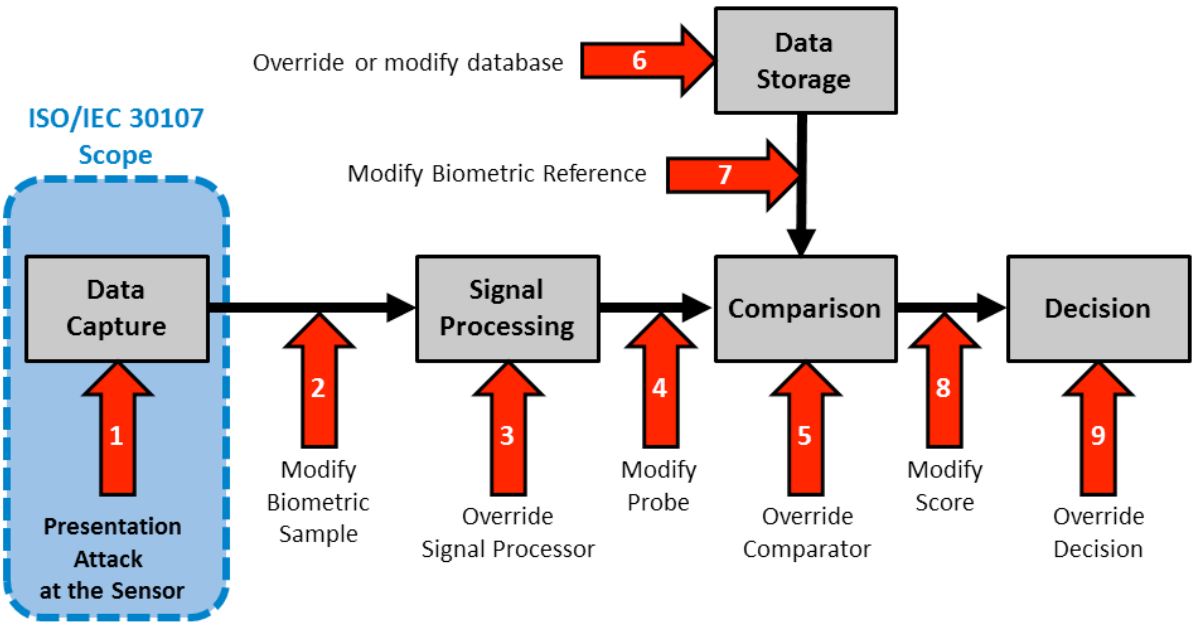


Figure 1: Generic attacks againts a biometric system

Therefore, the scope of the ISO/IEC 30107 standards is perfectly consistent with the Tabula Rasa project' scope.

3.4.2 Status

The ISO/IEC 30107 working draft is driven by the NIST organisation (USA). Until end of 2013, there was little progress on the document due to strong disagreements between participating members, especially between USA, Japan and Europe. Discussions and comments were numerous, thus leading to the production of many working draft, slowing down the writing of the standard.

It was recently decided in January 2014 to split up the document in three parts to facilitate the progress of the standard development:

Project #			
30107		Presentation Attack Detection	
IS 30107-1 (Clauses 1 to 6) IS 30107-2 (clause 7) IS 30107-3 (Annexes A and C (the latter to become a clause))		Presentation Attack Detection - Framework - Data formats - Testing, reporting and classification of attacks	

The first part (Framework) is currently in Committee Draft (CD) stage for review. The targeted date of publication is September 10, 2016. This part is still under NIST editorship. (Elaine Newton)

The second part deals with data formats, in other words, how to shape the information coming from the sensors to be readable in a standard way by any potential system. This part is under editorship of Fraunhofer IGD (Germany). (Olaf Henniger)

The main contribution of Tabula rasa for this standard is expected on part 3, dealing with testing, reporting and classification of attacks. This 3rd part will define the metrics to be used in order to quantify the acquisition quality, and potentially to take a decision whether the capture is valid or not. This part of the standard is currently in “first working draft” stage and the publication of a Committee draft is estimated for July 2015 at best. This part is still under NIST editorship (Michael Thieme)

For all 3 parts, Europeans are involved, either on the editorship (Part 2), or in the co-editorship (Part1 and Part 3).

4. CEN Working Group

4.1 CEN description

CEN, the European Committee for Standardization, is an association that brings together the National Standardization Bodies of 33 European countries.

CEN is one of three European Standardization Organizations (together with CENELEC and ETSI) that have been officially recognized by the European Union and by the European Free Trade Association (EFTA) as being responsible for developing and defining voluntary standards at European level.

CEN provides a platform for the development of European Standards and other technical documents in relation to various kinds of products, materials, services and processes.

CEN supports standardization activities in relation to a wide range of fields and sectors including: air and space, chemicals, construction, consumer products, defence and security, energy, the environment, food and feed, health and safety, healthcare, ICT, machinery, materials, pressure equipment, services, smart living, transport and packaging.

CEN is composed of many groups, working on all key areas for Europe (https://www.cen.eu/Pages/default.aspx).

CEN members are separated into 3 categories:

- **Members**: all EU M.S., plus Iceland, Norway, Switzerland, Macedonia and Turkey.
- **Affiliates**: Albania, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Egypt, Georgia, Israel, Jordan, Lebanon, Libya, Moldova, Montenegro, Morocco, Serbia, Tunisia and Ukraine
- **Partners**: Australia, Mongolia, Kyrgyzstan

The standardization system in Europe is based on the national pillars, which are the National Standardization Bodies or the members of CEN. A National Standardization Body is the one stop shop for all stakeholders and is the main focal point of access to the concerted system, which comprises regional (European) and international (ISO) standardization. It is the responsibility of the CEN National Members to implement European Standards as national standards. The National Standardization Bodies distribute and sell the implemented European Standard and have to withdraw any conflicting national standards.

CEN is composed of Technical Committee (TC) and Project Committee (PC). Those committees are further composed of Sub-Committee (SC), Working Group (WG), and Technical Boards (BT).

4.2 Developing a European Standard

The development of a European Standard (EN) is governed by the principles of consensus, openness, transparency, national commitment and technical coherence and follows several steps:

Proposal to develop an EN

Any interested party can introduce a proposal for new work in CEN. Most standardization work is proposed through the National Standardization Bodies.

Acceptance of the proposal

Once a project to develop an EN is accepted by the relevant CEN Technical Body, or by the CEN Technical Board (in case the proposal is related to a new field of standardization activity), the member countries shall put all national activity within the scope of the project on hold. This means that they do not initiate new projects, nor revise existing standards at national level. This obligation is called 'standstill' and allows efforts to be focused on the development of the EN.

Drafting

The EN is developed by experts within a Technical Body.

CEN Enquiry – Public comment at national level

Once the draft of an EN is prepared, it is released for public comment, a process known in CEN as the 'CEN Enquiry'. During this public commenting stage, everyone who has an interest (e.g. manufacturers, public authorities, consumers, etc.) may comment on the draft. These views are collated by the CEN national members and analysed by the CEN Technical Body.

Adoption by weighted vote

Taking into account the comments resulting from the CEN Enquiry, a final version is drafted, which is then submitted to the CEN national members for a weighted formal vote.

Publication of the EN

After its publication, a European Standard must be given the status of national standard in all CEN member countries, which also have the obligation to withdraw any national standards that would conflict with it. This guarantees that a manufacturer has easier access to the market of all these European countries when applying European Standards and applies whether the manufacturer is based in the CEN territory or not.

Review of the EN

To ensure that a European Standard is still current, it is reviewed at least within five years from its publication. This review results in the confirmation, modification, revision or withdrawal of the EN.

Unlike ISO standard, a European Standard (EN) automatically becomes a national standard and therefore is included in the standards catalogue of CEN's Members, the National Standardization Organizations in 33 countries. Additionally, CEN is producing two other types of document:

- TR (Technical Recommendations): provide information and advice

- TS (Technical Specifications): strong recommendation

Implementation of EN in Members States is mandatory while implementation of TR and TS is not.

4.3 Biometrics working group and planned initiative

TC224 is specifically working on "Personal Identification, Electronic Signature, Cards and their related systems". TC224 is composed of 7 active working groups, ranging from user interface to European citizen card, and of course, interoperability of biometric recorded data.

TC 224/WG18, "Interoperability of Biometric Recorded Data" has been created in 2010, chaired by Morpho, and was based on 2 main wishes:

First one was to prolong the work previously carried within the focus group on Biometrics, and the second is the willingness of the European Commission to work on 2 main documents.

The first document is dedicated to the Best practices for Slap Ten Print Captures, and is focusing on recommendations for hardware of fingerprint sensor and its deployment, user guidance, enrolment process, processing, compression and coding of the acquired fingerprint image, operational issues and data logging. This document has been published as a "TS" in October 2012, based on the wishes of the commission to release a standard to guide border guard for the European Visa system. This document will soon be published as an ISO Standard.

The second document is a recommendation for using biometrics in European Automated Border Control. This document focuses on ensuring a comprehensive and continuous security for Automates Border Control (ABC) deployment; increase efficiency of border control processes, improved experience for traveller, ergonomics, etc. This document has been aligned with the Frontex document on the general guideline for ABC deployment. This document will soon be published as "TS", and is the next candidate for adoption at the ISO level.

The group is actively working on other topics such as:

- Environmental influence on European ABC System (a derivation of the ISO 29197),
- Managing identity with portable devices (focuses on law enforcement and border authorities), and
- Translating the on-going ISO work on the detection of suspicious biometric samples for European ABC.

This last point will be proposed as a new work item during the next meeting, and will translate the ISO 30107:1 Framework in order to create a set of requirements for managing anti-spoofing for ABC gates. **Tabula Rasa** (and Beat) coordinator already made a presentation of the European projects results, with the willingness to carry those results at the CEN level, potentially to push them forward to ISO.

CEN TC224/WG18 is composed of eight Member States and two European Union organizations (Frontex, ANEC), with various contributors, industries, non-profit, and academics. The group is meeting 4 times per year, and try to harmonize European decision in order to push a common vision at the ISO international level.

5. The Common Criteria standard

5.1 Description

Common Criteria (CC) is a norm, appeared in the early 2000, for the evaluation of security products. It has been submitted to ISO under the reference ISO 15408. It is composed of various documents describing requirements for the developers submitting a product to the evaluation and evaluation methodology for the evaluators. The basic ideas of a security product evaluation can be summarized as follows:

- The security of the product (Security objectives, its environment, the resistance level) is described in a document called "Security target"
- For applications classes, a generic "security target" is proposed and is called a "Protection Profile". Protections profiles can be seen as security specifications for future products.
- The role of the evaluator is double: firstly to verify the consistency of the claims of the developer, secondly to perform an independent vulnerability analysis (including attacks and testing) to confirm the claimed resistance level.
- Common Criteria define a kind of Common language (Security requirements, Assurance components, etc) both for the developer to express the Security features of its product, and for the evaluator to express its evaluation work.

In addition to the norm and the methodology, a cooperation structure has been set up through what's called CCRA (Common Criteria Recognition Arrangements) to enable a wide recognition of Certificates emitted by the signing countries. Major rules are:

- The evaluation / Certification are organized in National Certification Schemes. Each Scheme is managed by a **public** Certification Body (CB), the only authority able to emit Certificates.
- Evaluations are performed by specific laboratories (called ITSEF: Information Technology Security Evaluation Facilities or CLEF: Common Criteria Laboratory Evaluation Facilities) delivering an ETR (Evaluation Technical Report) to the CB. Competences of ITSEF are checked, through a formal accreditation process, by the CBs.
- CCRA is managing the evolution of the Common Criteria.

Today, 26 countries over the world (European countries, USA, Canada, Australia, Japan, Korea, China, etc) have signed the CCRA arrangements.

The existence of a norm and mainly the organization built around Common Criteria make them a key element for the evaluation and certification of Security Products.

However, as a generic norm available for any kind of Security Products, Common Criteria are imperfect for all the applications. Interpretations, adaptations are required to make them efficient in specific areas.

The *Smartcards Example* is pointed out today in the Common Criteria context as the way to follow for using CC in specific context. The stakeholders group is called a "Technical Committee" and a structure to receive proposed documents, analyse and validate them, and derive normative documents is defined.

"Protection Profiles":

Protection Profiles (PP) are a tool enabling to define a common evaluation practice for different products targeting the same application. However, to be efficient, they need to be shared by all the stakeholders. If not, a multiplication of slightly varying PPs and the "mine is better" reflex for choosing one, drives to the opposite target (no comparison nor common understanding). A real standardization could not just rely on producing a new PP but must take into account the way to reach a global acceptance of this proposal.

PPs are evaluated and certified, but this certification only states that they are conform to the CC criteria and not that they are efficient and well adapted to a specific area.

The resistance of a given product is checked through 2 axes:

- The Strength of Functions (SOF) corresponding to the theoretical resistance of the mechanisms (for example key length for cryptographic algorithms). This is checked independently of the implementation and is defined at the national level (with international recognition). 3 levels are defined: BASIC, MEDIUM and HIGH. For example, a simple DES is considered as MEDIUM, triple DES is HIGH, RSA 1024 are for some years HIGH but will be reduced to MEDIUM in the future, AES 256 is HIGH, …
- The resistance to an attacker (Vulnerability analysis, VLA or VAN). For this task, the implementation is checked and the attacker is free to play with the environmental conditions (including specific test benchs). The attack potential is rated as LOW, MEDIUM and HIGH. These ratings are defined by tables using various criteria to describe the complexity of the attack (time, expertise, access to the product, knowledge of the design, etc). For some product families, specific tables have been developed by the industry, such as smartcards.

The basic idea of a Common Criteria evaluation is that the developer has to claim a security level (then a resistance level), to justify its claim through documentation, internal procedures and testing, and for the evaluator to check the consistency of the given elements and to perform independent testing to validate the results.

For example, the CC norm is used worldwide for the certification of smartcard products. Today, every provider of smartcards is certifying them at the highest level of security, as this is a minimal and mandatory requirement from customers.

5.2 Common Criteria applied to biometrics

For biometrics systems, the first type of resistance can be defined as evaluating the FAR (False Acceptance Rate) and the FRR (False Reject rate) factors. The main difficulties reside in the fact that huge databases are required, theoretically independent for the developer and for the evaluator. A legal problem often arises, for example, in France, the management of fingerprints databases is subject to the agreement of a National Agency (CNIL). In addition, it is relatively easy to introduce biases to enhance the performances of a specific technology, and validating a database is a complex task.

The second type of resistance covers various types of attacks, specific or not to the biometrics. Spoofing (for example creating false fingers), attacks towards the matching system (hill climbing, synthetic fingerprints images), are attacks specific to the biometric

system. Electronics attacks (tampering the sensors), Side channel like attacks are classical attacks that could be applied to biometrics sensors.

From early 2000, Common Criteria have been proposing some adaptation for the evaluation of fingerprints based systems. BEM ("Biometrics evaluation methodology") was the first reference. It was focused on SOF testing and did not take into account spoofing or electronics attacks. Starting from 2007, the French, German and Spanish national schemes, together with partners including Morpho, have started some studies to cover all the aspects of an evaluation (i.e. including the VLA testing). Today, a CC group, driven by the Spanish Certification Body, CCN, works on the definition of a document for:

- Defining the attacks to be taken into account during an evaluation
- Defining a testing methodology
- Defining a rating table for a quantification of the resistance level

Additionally, the German Certification Body (BSI - Bundesamt Sicherheit Informationstechnik) is already proposing to certify the resistance of fingerprint sensors based on this adapted Common Criteria norm up to EAL2+ level (i.e. Medium), using a defined and large set of fake fingers. Morpho's fingerprint sensor **MorphoSmart™ Optic 301 fingerprint reader** has passed this evaluation, becoming the first ever biometric sensor certified for its resistance against spoofing attacks[1]. This certification by BSI means that the device went through a rigorous analysis and testing process in order to meet the industry's highest standards for spoof detection.

These initiatives toward the use of Common Criteria standard for security evaluation of biometric sensors are strongly pushed by the French, German and Spanish certification bodies. They are for now limited to Fingerprints based systems and still have to be improved. If very little has been initiated, in the Common Criteria context, for other modality, projects have started to adapt the CC norm to face, iris and vein biometrics. The work and results achieved in the Tabula Rasa project can greatly contribute to this study, especially for attacks definition and testing methodology.

Surprisingly, this work on Common Criteria adaptation for biometric evaluation is not aligned with the current ISO initiative. Indeed, ISO has not retained for now Common Criteria as an appropriate methodology for evaluating resistance of biometric systems against direct attacks. However there are still opportunities for the European Certification Bodies to push this methodology at the CEN level in order to reach a consensus and common vision for the security evaluation of biometric products.

[1] Press release: http://www.morpho.com/actualites-et-evenements/presse/morpho-world-s-first-company-to-receive-common-criteria-certification-for-fake-finger-detection?lang=en

6. Conclusion

This document has presented the on-going work at European and international level for the development and the adoption of a standard allowing harmonised security evaluation of biometric products. All these initiatives are focussing on direct spoofing attacks only, i.e. at the sensor level. Unfortunately, a common vision still have to be discussed shared as competing evaluation methodologies are under study in different initiatives.

Tabula Rasa is contributing (or will contribute shortly) to the establishment of theses standards. In particular, the work regarding the definition and characterisation of attacks, the definition of evaluation methodology and the metrics is a valuable and helpful input from the project. This contribution is done through the presentation of the project by the coordinator to the different working groups and the participation of consortium members (e. g. Morpho) and the coordinator to standardisation meetings related to spoofing attacks.