CEN/TC 224/WG 18 **N 971**

CEN/TC 224/WG 18 "Biometrics"
WG Secretariat: **AFNOR**
Convenor: **Gacon Pierre M.**

NP TS_injection_attack_WD10

Document type	Related content	Document date	Expected action
Meeting / Document for discussion	Meeting: Helsinki (Finland) 13 Mar 2024 Project: 00224273 - -	2024-01-25	**COMMENT/REPLY** by 2024-02-21

CEN/TC 224

Date: 2022 -01

prEN XXXXX: XXXX

Secretariat: AFNOR

Biometric data injection attack detection

Détection d'attaques par injection de données biométriques

ICS:

CCMC will prepare and attach the official title page.

Contents

European foreword

This document (prEN XXXX:XXXX) has been prepared by Technical Committee CEN/TC 224 “Machine-readable cards, related device interfaces and operations”, the secretariat of which is held by AFNOR.

This document is a working document.

Introduction

A biometric technology is used to identify or verify individuals thanks to their physiological or behavioural characteristics. Therefore, biometric technologies are often used nowadays as component of a security system. In a security system, biometrics is usually used to recognise people in order to check if they are known or not from the system.

From the very beginning in the use of biometrics, potential attacks against such recognition systems were widely acknowledged by the community. This has risen the development of attack detection solutions, to defeat subversive recognition attempts.

ISO/IEC 30107-1 describes nine points of attacks onto a biometric system, as shown in Figure 1. But ISO/IEC 30107 series deals only with Type 1 attacks, i.e. presentations to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system. But ISO/IEC 30107 series do not consider within its scope those attacks that are applied outside the front end of the acquisition system, i.e., those attacks which are not physically presented to the embedded capture device."

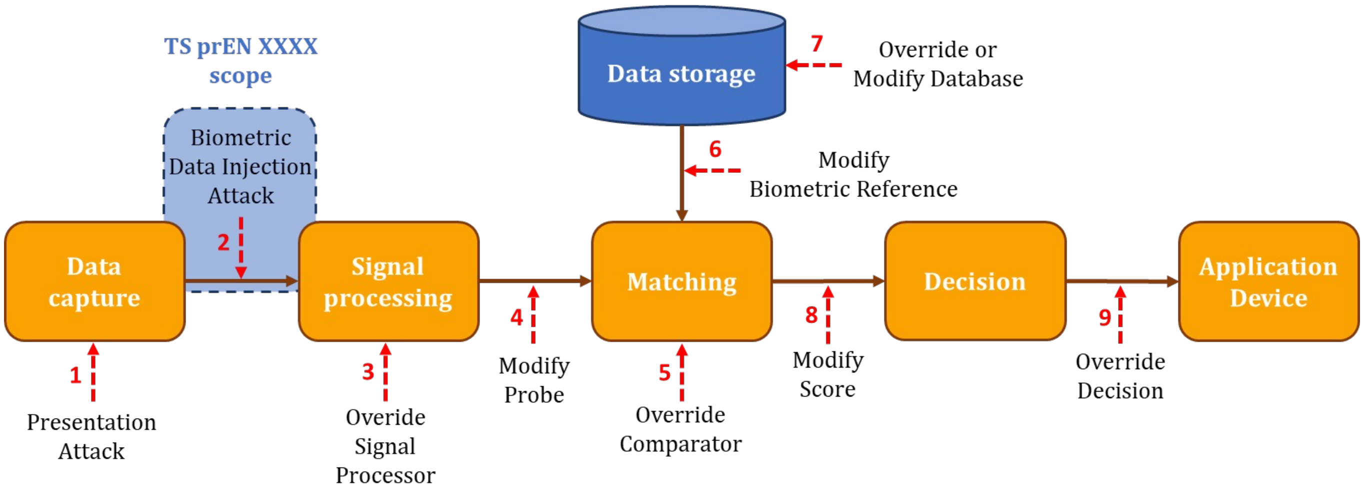

Figure 1 Examples of points of attack in a biometric system [4]

The emergence of remote identity verification solutions based on biometric (such as facial) recognition and using mobile applications or web browser applications may provide new means of attacking the recognition process. One of these attacks is the Type-2 attack (see Figure 1), which is based on the attacker modifying the data flow.

This Technical Specification is focused on such Type-2 attacks, called Biometric Data Injection Attacks. Such an injection attack consists in the action of interfering with the biometric system by replacing the original data sample provided by the user at the biometric data capture device, with another biometric sample, before the execution of the feature extraction process.

EXAMPLE An injection attack can be the injection of fingerprint image/video in a fingerprint contactless system.

The feasibility of such digital attacks has been identified by several agencies such as:

- French ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) in remote identity verification referential called P.V.I.D. [1]

- European Standards Organization ETSI (European Telecommunications Standards Institute) in their TS 119 461 which deals with remote identity verification. [2]

- European Union Agency for Cybesecurity (ENISA) in “Remote Identity Proofing: Attacks and Countermeasures” report. [3]
- German BSI (Bundesamt für Sicherheit in der Informationstechnik) in the Technical Guideline TR-03147 Assurance Level Assessment of Procedures for Identity Verification of Natural Persons. [4]
- Spanish CCN Security Guide for ITC products – Annex F.11: Videoidentification tools [12]

Yet, there is no national or international standard for biometric data injection attacks as there is for presentation attacks with the already available ISO/IEC 30107 standards or for generic biometric systems with the ISO/IEC 19792 standard [22].

This standard activity could be a common base for the work undertaken by French ANSSI, Spanish CCN and ETSI. This standardisation gap has also been identified by ENISA (European Network and Information Security Agency) which has written a report on the vulnerability landscape of the remote digital identity service providers using biometrics [3].

Thus, this Technical Specification will provide a foundation for Injection Attack Detection through defining terms and establishing a framework through which biometric data injection attack events can be specified and detected so that they can be categorized, detailed and communicated for subsequent biometric system decision making and performance assessment activities.

Secure elements and any other cryptographic security features are not covered by this technical specification.

1 Scope

This technical specification provides overview on:

- Definitions on Biometric Data Injection Attack.
- Biometric Data Injection Attack use case on main biometric system hardware for enrolment and verification
- Injection Attack Instruments on systems using one or several biometric modalities.

This technical specification provides guidance on:

- System for the detection of Injection Attack Instruments.
- Appropriate mitigation risk of Injection Attack Instruments.
- Creation of test plan for the evaluation of Injection Attack Detection system

If presentation attacks testing is out of scope of this technical specification, note that these two characteristics are in the scope of this document:

- Presentation Attack Detection systems which can be used as injection attack instrument defence mechanism and/or injection attack method defence mechanism. Yet, no presentation attack testing will be performed by the laboratory to be compliant with this TS (out of scope).
- Bona Fide Presentation testing in order to test the ability of the Target Of Evaluation to correctly classify legitimate users.

The following aspects are out of scope:

- Presentation Attack testing (as they are covered into ISO/IEC 30107 standards)
- Biometric attacks which are not classified as type 2 attacks (see Figure 1).
- Evaluation of implementation of cryptographic mechanisms like secure elements.
- Injection Attack Instruments rejected due to quality issues.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

Here are the normative references of this Technical Specification:

- ISO/IEC 2382-37
- ISO/IEC 19795-1
- ISO/IEC 30107-1
- ISO/IEC 30107-3

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37, ISO/IEC 19795-1 and ISO/IEC 30107 serie, and the following apply.

3.1

attack type

combination of injection attack method and injection attack instrument species

3.2

biometric data injection

replacement of a biometric sample.

3.3

biometric data injection attack

action of using an injection attack method (3.15) to interfere with the biometric system by replacing the original data sample captured by the data capture component by an injection attack instrument (IAI), before the execution of the feature extraction process.

NOTE To avoid too long sentences in the rest of this document, we will use the term “injection attacks” to talk about “biometric data injection attacks”.

EXAMPLE An injection attack can be the injection through a virtual (fake) webcam of a deepfake video representing the face of a victim onto the head of an attacker in order to impersonate the identity of a victim during a remote identity verification transaction using face recognition [1,7].

3.4

enrolment evaluation

measure the ability of a biometric system to correctly detect injection attacks and classify bona fide presentations at enrolment phase.

3.5

full system

a system which includes both biometric comparison and IAD subsystems.

3.6

full system evaluation

measure the ability of the full system to correctly detect injection attacks and classify bona fide presentations.

3.7

hook

operation where function calls are intercepted by a program to modify their behavior.

3.8

injection

modification of a data flow by modifying the data source or overwritting the data.

3.9

injection attack detection

IAD

automated determination of a biometric data injection attack.

NOTE: IAD can include injection attack method defence mechanisms (3.16) and injection attack instrument defence mechanism (3.13)

3.10

injection attack detection subsystem

IAD subsystem

hardware and/or software that implements an IAD mechanism and makes an explicit declaration regarding the detection of injection attacks.

3.11

injection attack detection subsystem evaluation

IAD subsystem evaluation

measure the ability of the IAD subsystem to correctly classify both injection attacks and bona fide presentations.

3.12

injection attack instrument

IAI

biometric sample, which may be a modified biometric sample, used in a biometric data injection attack.

3.13

injection attack instrument defence mechanism

IAIDM

biometric defence mechanisms aiming at making a biometric system resistant to injection attack instruments.

3.14

IAI species

class of injection attack instruments created using a common production method and based on different biometric characteristics

EXAMPLE 1 A set of face deepfakes videos made with the same software.

3.15

injection attack method (IAM)

methodology to interfere with the biometric system in order to replace the original data sample captured by the data capture component.

3.16

injection attack method defence mechanism (IAMDM)

biometric defence mechanisms aiming at making a biometric system resistant to injection attack methods.

3.17

modified biometric sample

biometric sample modified, through edition or alteration, by an attacker in order to impersonate a victim's identity or to hide original biometric sample characteristics.

3.18

operating system read-only memory

OS ROM

Read-only memory, or ROM, is a type of computer storage containing non-volatile, permanent data that, normally, can only be read, not written to. ROM contains the programming that allows a computer to start up or regenerate each time it is turned on. The OS ROM is a ROM which contains the Operating System of the device, which are all the programs which manage resources of the device.

3.19

security target

document which defines the assets protected by the TOE, the threats which will be taken into account during the evaluation and the security functions implemented by the TOE to prevent the threats.

3.20

target of evaluation

TOE

the product that is the subject of the evaluation.

3.21

threat

injection attack scenario used by the attacker to bypass the IAD mechanism.

NOTE For the other terms not defined here, see their definition in the normative references.

4 Symbols and abbreviations

For the purposes of this document, the symbols and abbreviations given in ISO/IEC 2382-37, ISO/IEC 19795-1, ISO/IEC 30107-1, ISO/IEC 30107-3, and the following apply:

AI Artificial Intelligence

API	Application Programming Interface
BPCER	Bona fide Presentation Classification Error Rate
FNMR	False Non-Match Rate
IAD	Injection Attack Detection
IAI	Injection Attack Instrument
IAIDM	Injection Attack Instrument Defence Mechanism
IAM	Injection Attack Method
IAMDM	Injection Attack Method Defence Mechanism
IT	Information Technology
PAD	Presentation Attack Detection
ROM	Read-Only Memory
TOE	Target Of Evaluation

5 Conformance

To conform to this document, an evaluation of IAD mechanisms shall be planned, executed and reported in accordance with the mandatory requirements as follows:

- Clauses 6 to 13
- Annex A

6 Characterisation of biometric data injection attacks

6.1 Injection Attack Methods

Although attacks of a biometric system can occur anywhere and be instantiated by any actor, as described in [5], this Technical Specification only focuses on biometric-based attacks after the data capture subsystem by replacing the captured biometric sample. Attacks by other actors and at other points of the system are out of scope of this TS.

Figure 1 (see Introduction) illustrates several generic attacks against a biometric system. This document only focuses on type 2 attacks.

Injection attacks are usually carried out by biometric impostors who intend to be recognised as a specific individual known to the system.

In order to achieve a biometric data injection attack, the attacker needs to have a partial control over the device to perform the replacement, as the replacement may need to prepare the device or to use specific software installed on the device. This means that the device used to perform the attack is unsupervised.

Thus, there are different types of devices on which a biometric data injection attack is possible:

- a computer,
- a mobile device,
- other smart devices (e.g., IoT device equipped with a camera).

Figure 2 shows how injection attacks are done on a biometric system used via a web app or a computer app. Figure 3 gives an illustration of an attack performed through hooking process.

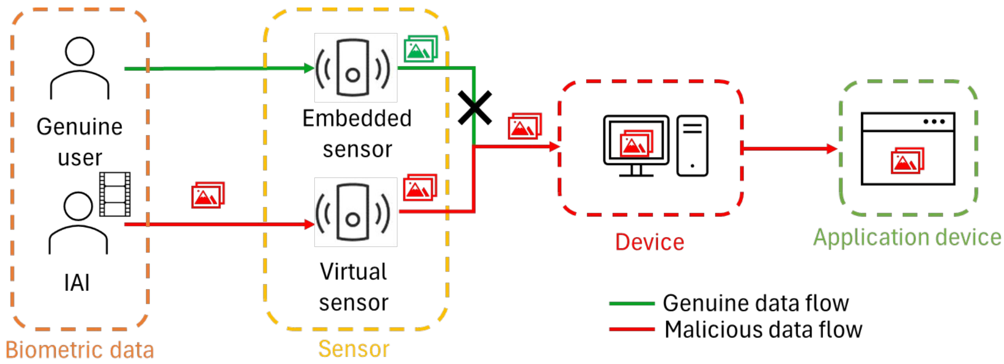

Figure 2 Principle of a biometric data injection attack through virtual sensor used in a standard device [7]

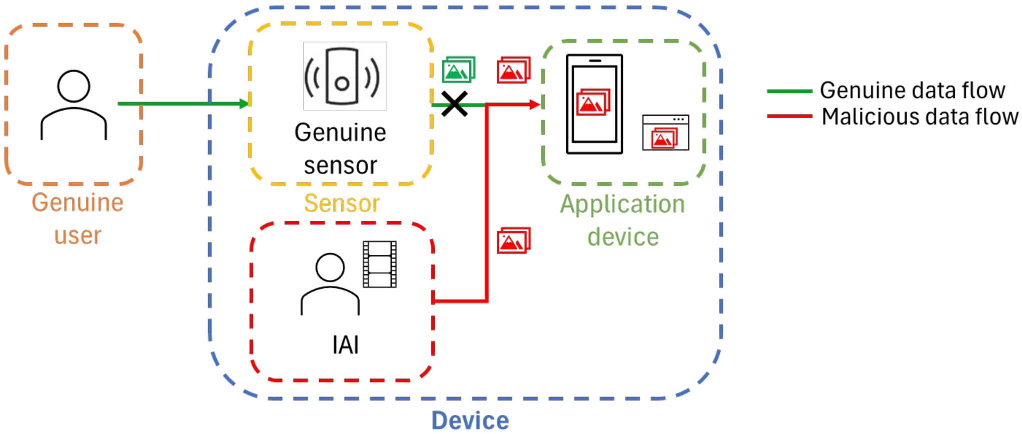

Figure 3 Biometric Data Injection Attack made with hooking process [14]

Of course, the difficulty to achieve the attack will depend on the device that is used to perform the attack, but also on the way the device is used. Because using a computer can give access to plenty of different software that will give to the impostor the possibility to mimic the biometric capture device (as a virtual camera for face recognition or virtual microphone for voice recognition for instance) or to intercept data sent by the capture device.

Nevertheless, for instance, as of today it is more difficult, but not impossible, to install a virtual capture device on a mobile device. Thus, it means that the injection attack may require the use of a rooted device and requires the attacker to have expertise in mobile application reverse engineering and penetration testing in order to make a hook of the biometric capture device API called by the mobile application and replace the data taken by the capture device with malicious data.

NOTE For specific devices, it might be possible for attackers to find custom ROM with virtual camera on the internet and thus, the attacker only needs to root his phone and then to install the custom ROM.

Figure 4 gives an illustration of what the hooking process looks like.

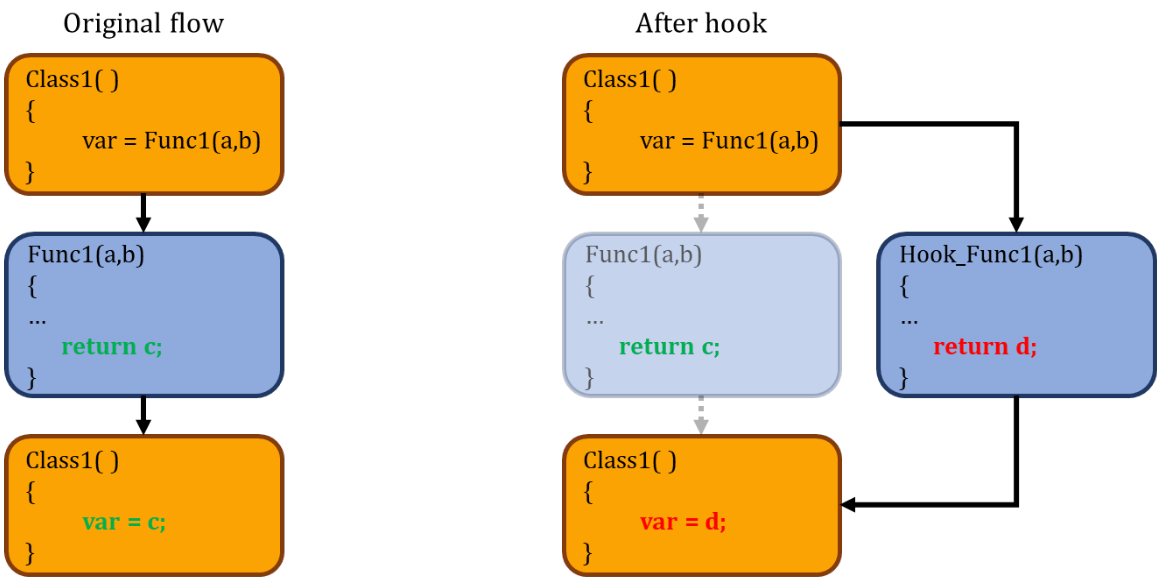

Figure 4 Hooking process [14]

Moreover, note that the environment and the context of the attack can affect its feasibility. Indeed, if the TOE is supervised or attended, it may be more difficult for the attacker to achieve the attack.

Eventually, the success of a biometric data injection attack is highly related to the IAI that is used by the attacker. It is important to notice that creating a high quality IAI can rely on the expertise of the attacker and/or the quality of the biometric source.

6.2 Injection Attack Instruments

An Injection Attack Instrument is a fully synthetic, a modified or unmodified biometric sample used by an attacker to replace the genuine biometric sample in a biometric security solution in order to fool it. Data used for attacks just after the capture device falls into three distinct categories: unmodified data, modified data and artificial data.

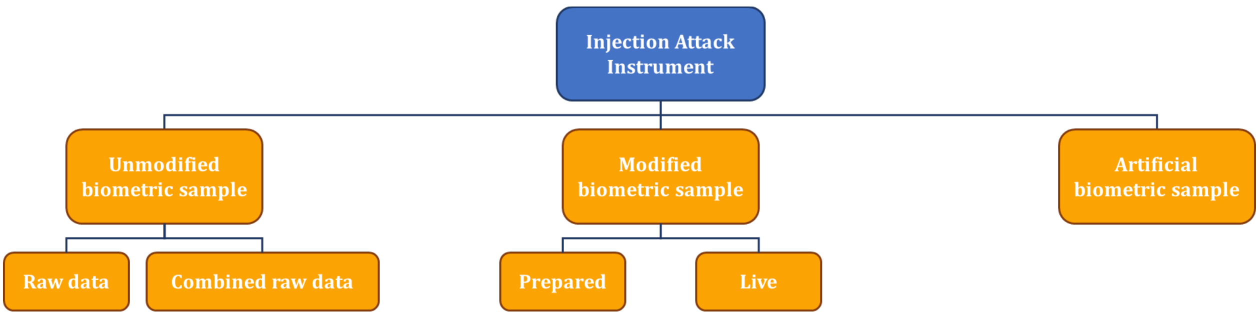

Figure 5 Types of injection attack instruments

Figure 5 gives a detailed description of these categories. Table 1 gives examples of each specific IAI type in the bottom tier of Figure 5.

Table 1 Examples of biometric samples used during a biometric data injection attack

Category	Type	Examples

Unmodified biometric sample	raw data	video of a face, photo of an iris
	combined raw data	combination of videos, combination of voice records
Modified biometric sample	prepared	deepfake video, synthetised voice record, or a combination of both.
	live	live deepfake video, live synthesized voice, or a combination of both.
Artificial biometric sample	generated artificial data	face image generated with AI, fingerprint image generated with AI

7 Framework for injection attack detection mechanisms

7.1 Overview of different types of injection attack detection

The biometric data injection method is neither dependent from the integration nor of the capture system in the device (e.g., integrated webcam or USB webcam on a computer), which means that an injection attack can be performed on both architectures.

There are different types of Injection Attack Detection (IAD) mechanisms:

- IAMDM designed to counter an IAM
- IAIDM designed to classify IAI as artefacts

It is recommended that systems implement both types of IAD mechanisms so that the attacker has to identify an effective injection method and to build injection instruments able to not be classified as such. Yet, some systems can choose to implement only one type of IAD mechanisms.

As there is no way possible to be sure that data received by the application device (whether it is a mobile or computer application) is from the trusted biometric capture device, mechanisms countering an IAM usually depend on cryptographic security solutions, while mechanisms concerned with IAI may be similar to PAD mechanisms or introduce randomness during data capture (see subclauses 7.3.1 and 7.3.2).

For Injection Attack Method Defence Mechanisms, the techniques can be based on system changes detection, injection detection, IT countermeasures or device authentication. On the other hand, the techniques for Injection Attack Instrument Defence Mechanisms can be based on challenge-response or artifact detection.

Table 2 proposes different methods for detecting biometric data injection attacks and gives different implementation's examples.

Table 2 Examples of methods for detecting or countering biometric data injection attacks

Category	**Type**	**Examples**
Injection attack method defence mechanism	System changes detection	Detection of changes from normal use by the attacker. For example, it can be a proxy detection, a root detection or an emulator detection for mobile devices.
	Injection detection	Detection of a data injection during the usage of the device. For example, it can be a virtual camera detection system.
	IT countermeasures	Security implemented by the developer to

		waste the attacker's time or hide sensitive information. For example, it can be the use of counters or code obfuscation.
	Device authentication and secure messaging	The biometric sample transferred to the signal-processing subsystem is protected with respect to authenticity and integrity by applying appropriate cryptographic primitives [13].
Injection attack instrument defence mechanism	Challenge-response	Detection of expected response after a specific challenge has been requested by the IAD system. Challenges can be performed by the users themselves or executed by the device capture, and they can then be observable on the sample. For instance, the IAD system may ask the users to perform specific actions (active challenge-response), such as moving their head in facial biometrics systems or reading some random code for voice biometric ones. Or it may command the device capture system to execute certain instructions (passive challenge-response). Other useful information can be used, directly extracted from the device capture to detect normal usage. For instance, using the mobile's accelerometer to check if the device is moving.
	Artifact detection	Detection of features that are indicative of an artifact. For example, detection of abnormal cuts in the voice flow in a synthetic voice made of copy-and-paste or speech concatenation; detection of an abnormal blur around the mouth or the eyes in synthetic videos…

7.2 Injection Attack Method Defence Mechanisms

7.2.1 Virtual sensor detection

As noted in 6.1, an attacker can use a virtual webcam, which can be configured to display real pre-recorded videos or a video stream and which will have similar behavior than a real camera. Similarly, using a smartphone simulator or emulator permits to an attacker to use a desktop environment and simulate or emulate a smartphone device. The simulated smartphone camera can for example be fed with a real pre-recorded video or dynamic deep fake.

Mechanisms that mitigate the presence of such virtual sensors shall be in place.

7.2.2 Secure channel mechanisms

An attacker shall not be able to intercept and modify the images / video / liveness answer or any instruction during their transit. Cryptographic securities shall be used to protect the whole digital channel between the capture device and the biometric system against injection. It can include digital encryption, digital signature or any mechanisms to insure integrity and authenticity.

7.3 Injection Attack Instrument Defence Mechanisms

7.3.1 Challenge-response

The concept of challenge-response is widely used in authentication schemes, some of which include biometric aspects and others with no biometric contribution. This part will focus in more detail on the implementation of challenge-response into biometric systems.
The framework for categorizing all aspects of challenge-response related to liveness is shown in Table 3.

Table 3 Injection Attack Detection utilizing challenge-response as tool

	Passive response	**Active response**
Challenge	Specific commands to the data capture subsystem, whose impact can be observed on the biometric data sample.	Cues (verbal, visual…) asking for a specific action to be made by the user, that will be captured by the biometric system
Response	Natural, involuntary, not controllable by the subject	Based on alive human cognition and voluntarily controlled action
Examples	Expect to detect a changing focus during face capture → the focus on face change according to the pattern given by the system	Cue to turn head right --> head pitch angle changes in the correct direction Cue to read a specific word --> word recognised by the system

The use of challenge-response for IAD can reduce the risk of attacks created from unmodified biometric samples. Indeed, depending on what is being asked as the challenge, unmodified data meeting that exact challenge may be hard (and sometimes impossible) to obtain for the attacker. The more unexpected the type of challenge requested, the harder it is to obtain an unmodified biometric sample meeting this specific challenge. Challenge-response for IAD can also make attacks based on modified data harder to create, in particular if the challenges required from the device or the user are based on "extreme data" (e.g. data that are harder to synthetize) such as unusual angles of the face or invented words. Moreover, if the challenge focuses on known attack flaws, it can increase the time spent and/or the attacker's expertise required to make an attack of sufficient quality.

Challenges, both based on active and passive responses, are particularly interesting in the case of IAD if they are linked to a random factor of challenge appearance, as they make the preparation of the attack more complex to create (need to create data samples for all possible variations and to inject them at the correct moment) - see clause 7.3.2 for more details.

7.3.2 Randomness

The following paragraph only concerns systems based on server-client architecture. To be efficient for preventing injection attacks, it is better that systems perform the analysis of the various challenges on the server side. As the client side is required to capture the necessary information from the user, any challenge request sent to the system or to the user shall be cyphered to prevent the attacker from knowing the challenges in advance.

Incorporating random factors in challenge-response IAD systems to prevent biometric data injection can further increase the difficulty, for an attacker, to fool the system. Random challenge-response systems are based on a set of different challenges or a set of different challenge orders that can be asked at each time to any user. The higher the number of possible challenges or challenge orders, the more robust the system. For instance, on a voluntary facial biometric system, the IAD can ask the user to turn his head right then left, or left then right: this would make two possible variations that can be randomly chosen for each verification. The greater is the entropy, the greater is the time required to create the different orders of challenges to carry out an attack. It means that having a large entropy (for instance more than a hundred challenge orders possible) can prevent the injection attacks prepared in advance, which are the attacks with the highest level of quality as the attacker have all the time he wants to remove or at least to reduce the flaws of his attack.

It is important to notice that if the system is built on client-server architecture, the creation of challenge order shall be done on server side to prevent against challenge order modification from the attacker. In addition, the confidentiality of instruction containing the challenge order shall be protected in the channel between the server and the client, see also clause 7.2.2.

Eventually, it is important to notice that the nature of the device will affect the field of possibilities for the developer. Indeed, the developer would be able to have a best control on the mobile camera from his mobile application than on the webcam from his web-app for instance.

EXAMPLE On an Android mobile device, the developer can have access to raw images (without any algorithms from Image Signal Processor applied).

EXAMPLE 2 On a mobile device, it is possible to get access to data from other sensors like the accelerometer for instance.

7.3.3 Artifact detection

IAIDM mechanisms implementing artifact detection contribute to prevent deepfake attacks and face re-enactment attacks (giving movement to a face photograph according to a specific source video) used against face recognition or robotic voice synthetisation attacks used against voice recognition for example.

EXAMPLE: receiving something with a resolution different than the expected can be evidence of an injection attack, depending on the application.

This kind of automatic attack detection methods are particularly interesting to protect biometric systems against biometric data injection attacks realised in live as this kind of attack usually presents lots of defaults which would be detectable by such solutions.

EXAMPLE 2: a challenge requesting to move an object in front of the biometric source can be used to increase the probability of artefacts.

7.4 Combination of different types of IAD

As each method deals with a specific interest against a specific kind of biometric data injection attack, the best way to guard a biometric system is to combine different types of IAD subsystems. For instance, having an IAD solution which combines Injection Attack Method Detection Mechanism (e.g., log-in attempt counters) with Injection Attack Instrument Defense Mechanisms (e.g., challenge-response and artifact detection) will help to detect most of injection attacks.

7.5 Security vs general public use

The combination of different security solutions is interesting if such solutions are simple and easily understandable by the user. Enforcing a high level of security can impact the convenience of the system.

Thus, it is important to test the system and report the different performances to be sure that the security level does not reduce the usability of the solution (trade-off between the false acceptance rate, i.e., representing the security level, and the false rejection rate).

8 Evaluation of IAD systems

8.1 Overview

The system which is evaluated in conformance with this TS is called Target Of Evaluation (TOE). The evaluation of the TOE consists of assessing the resistance of the security functions established by the TOE against injection attacks. These security functions will be described in a document called security target (the security target structure is defined in Clause 8.2.2). The security target contains the description of threats taken into account by the evaluator to develop its injection attacks. The threat model corresponds to the risk analysis performed by the TOE developer. The TOE can be evaluated according to two different types of evaluation:

- IAD subsystem evaluation
- Full system evaluation

Evaluations of IAD mechanisms that are part of the TOE and resulting evaluation reports shall specify the applicable evaluation level, whether IAD subsystem or full system.

This TS does not cover the PAD testing. However, it is recommended to carry out, in addition to a conformity assessment with this TS, a conformity assessment with ISO/IEC 30107-3 if the TOE is a full-system product to identify all possible existing vulnerabilities of the TOE.

8.2 General principle of evaluation

8.2.1 General principles

First of all, the evaluator shall validate the security target in order to ensure that it takes into account all existing threats against the product under evaluation.

The evaluation of the TOE shall cover a defined variety of threats which will be defined in the security target. The threats will be covered by the evaluator thanks to a representative set of IAI species.

Moreover, the evaluator shall use a representative set of bona fide capture subjects in order to ensure the proper functioning of the TOE. With this set of bona fide capture subjects, the evaluator shall realise legitimate transactions in order to ensure that the bona fide presentation rate (BPCER for IAD subsystem evaluation and FNMR for full system evaluation) is close to the one given by the TOE developer in the security target.

Once the threats are defined in the security target document, the number of injection attack instruments species and injection attack methods used by the evaluator to set up the threat should be specified in the report. Establishing whether a specific IAI species reproducibly succeeds does not require a very large number of injections or subjects. The evaluator will be able to identify a vulnerability once an attack has bypassed the system once (identification phase, see Clause 10) and to exploit the vulnerability when the attack has been reproduced at least once (exploitation phase, see Clause 10).

A representative set of bona fide capture subjects is required to determine the frequency with which the TOE incorrectly classifies bona fide presentations. This is a critical part of the TOE testing since an IAD mechanism could erroneously classify bona fide presentations as injection attacks. A high classification error rate for bona fide capture subjects would reduce system usability and would not allow the evaluator to give a positive result in the report if the BPCER (or FNMR) is too high (for instance if it exceeds 15%). It needs to be clarified in the ST document.

8.2.2 Evaluation framework

At beginning of the assessment, the evaluator needs to have access to the security target of the TOE. The security target is a document in which the evaluator describes the TOE and the perimeter of the evaluation: the assets protected by the TOE, the threats taken into account during evaluation and the security functions implemented by the developer to prevent the threats. The security target will give information about the TOE to the evaluator and will influence the attack rating if an attack bypasses the TOE (see Clause 10). The security target shall have this structure:

1. Synthesis
   Identification of the product to be evaluated
2. Argument
   General description of the product to be evaluated
   Description of the use of the product to be evaluated
   Description of the intended use environment
   Description of dependencies
   Description of typical users
   Description of the TOE
3. Description of the technical operating environment
4. Asset to protect by the TOE
5. Description of threats
6. Description of the security functions of the TOE
7. Threats coverage

The security target can be written by the evaluator with the support of the developer, or can be provided to the evaluator by the developer.

Once the evaluator has validated the security target, the evaluation can begin. In order to get a conformance with this Technical Specification, the evaluator shall measure both bona fide presentation test results and injection attack test results.

For both substantial and high levels of evaluation, the evaluator shall select at least 10 different attack types. The selection and the number of attacks should be based on the experience of the evaluator and on the creation and preparation time needed to process the attack types.

Once all the tests have been made, the evaluator shall write the corresponding metrics in the report, depending on the type of evaluation (see Clause 8).

If an injection attack has been able to fool the TOE (i.e. the attack has been identified and exploited), the evaluator shall rate it thanks to Attack Rating Methodology presented in Clause 10. If the attack is rated at a higher level than the evaluation, it should not be taken into account into the evaluation’s final results. Only attacks rated at the level (or lower) of the evaluation should be taken into account. The rules leading to the evaluation’s result are presented in Clause 8.5.

Eventually, the evaluator shall give the report to the developer of the TOE who can decide to make the report public or not. The structure of the report is presented in Clause 11.

8.3 Injection attack methods

The first step in injection attack testing should ensure the evaluator's ability to perform an injection, i.e., to ensure that they are able to exploit at least one injection attack method on the TOE.

As defined in Table 4 presented in Clause 8.6, the evaluator shall use a minimum number of injection attack methods depending on the evaluation level considered. This means that the evaluator should try to inject an injection attack instrument (starting with the simplest IAI) using at least the minimum number of injection methods as defined in Table 4.

In the event that the evaluator is unable to implement an injection attack method during the time associated with the evaluation level, defined in Table 4, then the realization of IAI is not necessary.

8.4 Injection attack instruments

8.4.1 Properties of injection attack instruments in biometric attacks

In biometric impostor attacks, the attacker intends to be recognized as a different but genuine individual.

For biometric data injection attacks, in which the subject intends to be recognized as a specific, targeted individual known to the system, it is necessary to create an IAI with three properties:

- Property 1. The sample appears as a natural biometric sample to any IAD mechanisms in place.
- Property 2. The sample appears as a natural biometric sample to any biometric data quality checks in place.
- Property 3. The sample injected contains extractable features that is a match against the targeted individual's reference

The most straightforward way to affect Property 3 is to create a digital copy of the targeted individual's biometric characteristic. In some cases, it is possible to produce a copy of a digital biometric characteristic in the form of a modified biometric sample which can be used for an injection attack. Yet, depending on how the TOE is implemented, having an accessible raw biometric sample is sometimes sufficient to bypass the TOE.

8.4.2 Creation and preparation

Evaluations of IAD mechanisms may be designed to answer the following questions:

- How consistently does a specific IAI subvert a biometric system?
- What factors influence the efficiency of an injection attack?
- What attack type with the lowest level of difficulty succeed in fooling the biometric system?

Injection attack instrument creation, provenance, usage, and handling – from creation to utilization – are central to evaluation of an IAD system.

In an evaluation of IAD systems, at least 10 attack types shall be selected (when attack types are needed). When creating and preparing IAI according to a selected threat, the following factors and parameters should be considered:

- IAI creation process: IAI creation may be based on multiple tools and equipment whose handling can impact IAI efficiency. IAI are not necessarily machine-generated finished products, and human factors can impact IAI performance.
- IAI preparation process: IAI may require treatment or preparation between creation and utilization.
- Effort required to create and prepare IAI: for example, skills required, technical know-how, creation time, and equipment to be used.
- IAI customization for a specific system: a given IAI may only be usable against a specific IAD system, based on an analysis of the injection attack detection properties.
- Biometric characteristic sourcing: IAI may be based on raw or modified biometric samples.
- IAI creation and preparation cost: creation of an IAI will involve cost for sourcing the equipment required and for manufacturing.

These properties will enter into account while rating the attacks which would bypass the IAD mechanism during evaluation (see Clause 10).

The Evaluation laboratory shall be in charge of selecting the attack types used during the evaluation.

Evaluations of IAD mechanisms and resulting reports shall describe how IAI were created and prepared, addressing the following:

- creation and preparation processes.
- effort required to create and prepare IAIs (e.g. technical know-how, creation time, difficulty of collecting biometric characteristics source, creation instruments, and preparation instruments).
- ability to consistently create and prepare IAIs with intended properties.
- customization of IAIs for specific systems.
- sourcing of biometric characteristics.
- changes in IAI creation or preparation processes over the course of the evaluation.

8.5 Personal Data Protection of volunteers in IAD Assessments

As a reminder, biometric data is qualified as "sensitive" by the General Data Protection Regulation (EU) 2016/679 (GDPR) [9]. To be compliant with GDPR, all volunteers used for assessment, whether it's for bona fide presentations or injection attacks, need to sign a volunteer agreement in which they give their explicit consent for the processing and usage of their biometric and personal data, in the scope of evaluations and for a predefined period of time.

Moreover, the evaluation laboratories need to be compliant with GDPR. Basically, it means that all biometric data used for evaluation need to arise from volunteers who signed the agreement and biometric data need to have the appropriate security environment for data storage.

8.6 Levels of difficulty of the evaluations

Table 4 describes the three different levels of compliance with this Technical Specification. All the characteristics from Table 4 shall be applied.

Table 4 Evaluation's levels

Levels	**Injection Attack Instruments (IAI)**	**Injection Attack Methods (IAM)**	**Knowledge of the TOE**	**Time elapsed to perform the evaluation (writing the target of security, creating IAIs, testing and making the report)**	**Level of Evaluator required**	**Must be resilient to minimum attack level**
Basic (Level 1)	No injection attack instruments but a statement of conformity shall be issued on a minimum of technical requirements	No injection attack methods but a statement of conformity shall be issued on a minimum of technical requirements	No target of security but issue a statement of conformity stating that the fulfilment of the requirements set out in the scheme has been demonstrated	Conformity self-assessment under the sole responsibility of the developers Or 2/3 days by an evaluation center	Substantial	Basic

Substantial (Level 2)	At least 10 different attack types including ones that are not directly listed in the security target with levels from basic to high shall be assessed	At least 2 different injection attack methods including ones that are not directly listed in the security target shall be used	Target of security	25 days	High	Substantial
High (Level 3)	At least 10 different attack types including ones that are not directly listed in the security target with levels from basic to high shall be assessed	At least 2 different injection attack methods including ones that are not directly listed in the security target shall be used	At least the target of security.	According to the analysis of the evaluation target. Minimum of 30 days.	Very high	High

The result of the evaluation, Pass or Fail, shall be based on the rules described in the annex A of this TS.

This TS does not cover the PAD testing. However, it is recommended to carry out, in addition to a conformity assessment with this TS, a conformity assessment with ISO/IEC 30107-3 if the TOE is a full-system product to identify all possible existing vulnerabilities of the TOE.

NOTE Clause 8.2.2 gives a description of what is a security target and how the evaluation laboratory should write the document thanks to developer's support.

9 Metrics for IAD evaluations

9.1 General

IAD mechanism performances for the classification of bona-fide testing can be expressed in terms of classification error rates. Such metrics will allow the evaluator to ensure that the system is performant and thus, that the system is not rejecting legitimate users otherwise it could discredit the results obtained for security testing (with attacks). The calculated bona-fide metrics (depending on the evaluation's type, see Clauses 9.2 and 9.3) shall be compared to the value's target described in the Security Target document and shall be in accordance with the rules defined in the annex of this TS.

ISO/IEC 19795-1 provides an overview of the reporting requirements for a biometric performance test for bona fide presentations.

Before applying any metrics in the evaluation, it is important to note that any IAD evaluation shall fulfil the requirements given in Clause 11, for reporting.

9.2 Metrics for IAD subsystem evaluation

9.2.1 General

IAD subsystem evaluations measure the ability of IAD subsystems to correctly classify injection attacks and bona-fide presentations.

9.2.2 Classification metrics

BPCER is reported in IAD subsystem evaluations.

At the IAD subsystem level, performance metrics for the set of bona fide presentations captured with the TOE shall be calculated and reported as BPCER. BPCER shall be calculated using the following formula:

$$BPCER = \frac{\sum_{i=0}^{N_{BF}} Res_i}{N_{BF}}$$

Where:

- N_{BF} is the total number of bona fide presentations performed on the TOE.
- Res_i takes value 1 if the ith presentation is classified as an injection attack and value 0 if classified as a bona fide presentation.

Evaluations of IAD mechanisms shall report the number of bona fide presentations correctly and incorrectly classified – total and by capture volunteer.

9.3 Metrics for full system evaluation

9.3.1 General

Full-system evaluations include comparison subsystem results in addition to IAD subsystem results.

9.3.2 Classification metrics

FNMR is reported in full system evaluations.

At the full-system level, performance metrics for the set of bona fide presentations captured with the TOE shall be calculated and reported as FNMR. FNMR shall be calculated using the following formula:

$$FNMR = \frac{\sum_{i=0}^{N_{BF}} Res_i}{N_{BF}}$$

Where:

- N_{BF} is the total number of bona fide presentations performed on the TOE.
- Res_i takes value 1 if the ith presentation is classified as an injection attack and value 0 if classified as a bona fide presentation.

Evaluations of full-system shall report the number of bona fide presentations correctly and incorrectly classified – total and by capture volunteer.

10 Attacks rating methodology

10.1 General

Giving a level of difficulty to an attack is really useful as it allows to give an indication of the risks incurred by a product (and its data) equipped with a biometric security. With this biometric attack rating methodology, each evaluation laboratory will be able to give a mark to possible attacks on the TOE.

In this methodology, criteria are associated with marks in order to give a weight to each attack, to attribute then the intended level of attack (basic, substantial or high) in function of this weight. The EU Cybersecurity Act recommends these three assurance levels (basic, substantial or high) to express the cybersecurity risk. These assurance levels are commensurate with the level of the risk associated with the intended use of the product, service or process, in terms of the probability and impact of an incident. This document uses the same vocabulary to correspond to what is currently used in cybersecurity.

Depending on the attack, each criterion gives a rating to the attack, and the sum of all these marks gives a total weight to the attack. Thanks to this weight, the evaluator will give a level to the attack.

Table 5 lists the levels of attack with their weight's intervals.

Table 5 Attack's levels

Weight's interval	**Attack's level (resistance)**
0 to 10	No rating
11 to 20~~15~~	Basic
21~~16~~ to 30~~20~~	Enhanced Basic
~~2~~31 to 40~~25~~	Moderate/Substantial
~~26~~ 41 and above	High
At least one "Not Practical" mark	Not Practical

Not practical corresponds to the limit of an evaluation laboratory. The lab can estimate that an attack is not achievable by a random attacker, but only by powerful organizations: intelligence agencies, terrorist groups… Thus, if a criterion is associated with a "not practical" mark, the attack will be considered not achievable and will get the level "not practical".

The methodology considers two phases of the attack: identification and preparation.

NOTE This methodology is inspired by the Joint Interpretation Library (JIL) attack rating methodology used for smartcard security evaluations. It has been adapted to biometric systems but is based on the same structure. [10]

NOTE 2 The level of an attack can vary through time.

10.2 Identification and exploitation phases

The identification phase measures the effort required to create the attack. The advantages given to the laboratory to allow the first implementation of the attack within a reasonable time must be taken into account. These benefits can be of different natures, such as:

- access to non-public information (source code, design documents) or even confidential information (crypto keys, error logs).
- access to a product whose configuration is advantageous for the attacker compared to the operational configuration.

The exploitation phase measures the effort required to reproduce the attack in operational condition. The attacker is supposed to have useful information and automatic tools from the identification phase. On the other hand, the attacker is no longer supposed to have any particular advantages other than the information resulting from the identification phase.

Each criterion will give a weight to the attack for each phase.

The different criteria considered by this methodology are described in the next subclauses.

10.3 Time effort

The time effort is the time spent by an attacker in order to achieve an attack against a biometric system. The number of days corresponds to “working days”, as this methodology will be applied by laboratories.

Table 6 lists the time effort weight’s intervals for identification and exploitation phases.

Table 6 Time effort weights

Interval	**Identification weight**	**Exploitation weight**
< one hour	0	0
< one day	1	3
< three days	2	4
< 7 days	3	6
< 25 days	6	8
> 25 days	10	10
Not practical	*	*

10.4 Expertise

Expertise levels are defined based on the attacker ability to achieve the attack, on his/her knowledge (software, hardware…) and on his/her ability to operate the necessary tools.

These are the three levels of expertise:

- Laymen
- Skilled
- Experts

Laymen are attackers who have no particular expertise in any field linked to the attack.

Skilled attackers are familiar with the security behavior of the product type and are familiar with laboratory measurements and equipment.

Experts are attackers who has expertise in a field or equipment linked to the attack and necessary to achieve the attack.

In very specific cases, several types of expertise are required to make an attack. The “Multiple experts” level can be used but it should be noticed that the different skills must concern fields that have nothing to do with each other, for instance expert in motion design and mobile penetration testing.

Table 7 lists the expertise weight’s intervals for identification and exploitation phases.

Table 7 Expertise's weights

Interval	**Identification weight**	**Exploitation weight**
Layman	0	0
Skilled	2	2

Expert	5	4
Multiple experts	7	6

10.5 Knowledge of the product under evaluation

Knowledge of the product under evaluation refers only to classification levels related to the identification and exploitation of vulnerabilities in the product under evaluation.

In general, it is expected that all knowledge required in the exploitation phase of the attack will be passed on from the identification phase by way of suitable scripts describing the attack. To require sensitive or critical information for exploitation would be unusual.

The classification of the information for this criterion will be determined by the protection of the information. The higher the classification, the more difficult it will be for an attacker to retrieve the information required for an attack.

The following classification for information about the product under evaluation is to be used:

- **Public information:** information is considered public if it can be easily obtained by anyone (from internet for instance) or if it is provided by the developer to any customer without further means.
- **Restricted information:** information is considered restricted if it is controlled within the developer organization and distributed to subcontractors or special customers under a non-disclosure agreement.
- **Sensitive information:** this is knowledge that is only available to discrete teams within the developer organization. Sensitive information is protected by appropriate technical, environmental and organizational means. If such information needs to be distributed to or accessed by other organizations outside the developer, this must be limited to a strict need-to-know basis protected by a specific contract.
- **Critical information:** this is knowledge that is only available to teams on strict need-to-know basis within the developer organization. Critical information is physically and environmentally protected by high secure infrastructure as well as secure physical environment including attack detection and attack prevention layers. If such information needs to be accessed by other organizations than the developer, this must be limited to a strict need-to-know basis protected by a specific contract.

Table 8 lists the knowledge of the TOE weight's intervals for identification and exploitation phases.

Table 8 Knowledge of the TOE weights

Interval	**Identification weight**	**Exploitation weight**
Public information	0	0
Restricted information	2	2
Sensitive information	4	3
Critical information	6	5

EDITOR'S NOTE: We have removed "Not Practical" criterion during Task Force meeting (24/01/2024)

10.6 Equipment

Equipment refers to the hardware/software or tools that are required to perform the attack on the product under evaluation.

We separate equipment in five different categories:

- Standard equipment: equipment that is affordable and easily available to the attacker.
- Specialized equipment: this refers to fairly expensive equipment and/or not available in standard markets
- Bespoke: this refers to very expensive equipment and/or with difficult and controlled access. In addition, if more than one specialized equipment are required to perform different parts of the attack, this value can be used.
- Multiple Bespoke: this refers to a situation, where different types of bespoke equipment are required for distinct steps of an attack
- Not Practical: the equipment required to perform the attack is too expensive or too difficult to obtain when compared with the possible gains or advantages which could be seeked by an attacker.

Table 9 lists the equipment weight's intervals for identification and exploitation phases.

Table 9 Equipment's weights

Interval	Identification weight	Exploitation weight
Standard	0	0
Specialized	2	4
Bespoke	4	6
Multiple Bespoke	6	10
Not Practical	*	*

10.7 Access to TOE

~~Sample type is a criterion which allows the evaluator to qualify the type of TOE which was made available to him/her during the evaluation by the developer. Indeed, in order to save time during the evaluation, it is possible that certain countermeasures (e.g., transaction counters) have been deactivated to facilitate the work of the evaluator. Here are the different sample's types:~~

- ~~Normal sample: in this case, the evaluator is using the same TOE than classical user.~~
- ~~Open sample: the evaluator has access to a version of a TOE with standard countermeasures (e.g., limited number of tries) deactivated.~~
- ~~Critical sample: the evaluator has access to a version of a TOE with critical countermeasures (e.g., virtual camera detection system) deactivated.~~

~~Table 10 lists the sample type weight's intervals for identification and exploitation phases.~~

~~*Table 10 Sample type weights*~~

~~**Interval**~~	~~**Identification weight**~~	~~**Exploitation weight**~~
~~Normal sample~~	~~0~~	~~Not Applicable~~

~~Open sample~~	~~3~~	~~Not Applicable~~
~~Critical sample~~	~~6~~	~~Not Applicable~~

Access to TOE refers to measuring the difficulty to access the TOE either to prepare the attack or to perform it on the target system.

For the identification phase, elements that should be taken into account include the easiness to buy the same biometric equipment (with and without countermeasures).

For exploitation phase, both technical (such known/unknown tuning) and organizational measures (limited number of tries, etc.) should be taken into account.

The number and the level of equipment requested to build the attack is also taken into account in this factor.

This factor is not expressed in terms of time. The levels are as follows.

1. Easy: For identification phase, there is no strong constraint for the attacker to buy the TOE (reasonable price) to prepare its attack. For exploitation phase, there is no limit in the number of tries.
2. Moderate: For identification phase, specialized distribution schemes exist (not available to individuals) or the limit in the number of tries is deactivated. For exploitation phase, either a tuning of the attack for the final system is required (unknown parameterization of countermeasures for example) or the limit in the number of tries is deactivated.
3. Difficult: For identification phase, the system is not available except for identified users and access requires compromising of one of the actors or critical countermeasures are deactivated (e.g., virtual camera detection system). For exploitation phase, for example IAIs shuold be adapted to the (unknown) specific tuning or critical countermeasures are deactivated (e.g., virtual camera detection system).

Interval	Identification weight	Exploitation weight
Easy	0	0
Moderate	2	2
Difficult	4	4

EDITOR'S NOTE: We have ~~removed "Not Practical" criterion during Task Force meeting (24/01/2024)~~changed the criterion "Sample type" by "Access to the TOE" to better align with ISO 19989-1 Annex F.

[10.8] ~~Biometric sourcing~~Access to biometric characteristics

The access to the biometric characteristic or biometric sample is a key element for the attacker in order to achieve a biometric attack, as this is the biometric characteristic of the ~~victim~~ target that will permit the attacker to perform the attack. The quality of biometric sourcing will influence the attack's quality. Here are the different levels of ~~types of biometric sourcing~~access to biometric characteristics:

- ~~Easy: The attacker has access to a good quality biometric characteristic while being away from the victim and making no effort (e.g., sample on social media).~~

- ~~Hard: The biometric characteristic is not readily available for the attacker and the attacker needs to make important effort to get a workable sample (e.g., making a social attack to get the biometric sample). The risk of being spotted by the victim is high for the attacker.~~
- ~~Not practical: the evaluation laboratory concludes that obtaining a workable biometric characteristic from "exterior" is not possible for the attacker~~.
- Not needed. Access to biometric characteristic is not needed during this attack's phase.
- Easy. Samples of these modalities can be collected without difficulty, even without direct contact with an enrolled data subject (an exploration of the web and the social networks and so forth). Examples are 2D face, signature image, and voice signal.
- Moderate require multiple acquisitions, probably in a controlled way, without the collaboration of an enrolled data subject but probably with a direct contact with them. An example would be to make a social attack to get the biometric sample).
- Difficult. The biometric characteristic is captured with specific equipment which requires full cooperation from the target. An example could be the acquisition of iris images with a binocular sensor.

NOTE: The similarity between the attacker and the victim, if needed, shall be taken into account as a difficulty to obtain the biometric source.

Table 11 lists the biometric sourcing weight's intervals for identification and exploitation phases.

Table 11 Biometric sourcing weights

Interval	Identification weight	Exploitation weight
~~Easy~~Not needed	0	~~Not Applicable~~0
Easy	0	0
Moderate	4	4
Difficult~~Hard~~	8~~4~~	~~Not Applicable~~8
~~Not Practical~~	~~*~~	~~Not Applicable~~

EDITOR'S NOTE: We have changed the criterion "Biometric sourcing" by "Access to the biometric characteristic" to better align with ISO 19989-1 Annex F. We have added a criteria called "not needed" to adapt to all scenarios.

10.8[10.9] Degree of scrutiny

Degree of scrutiny refers to the one applied during usage the TOE. Here are the different existing levels of scrutiny:

- None: the attacker is not supervised while he achieves an attack.
- Overseen: there is at least a security agent, or an operator trained for fraud detection, who oversees the usage of the TOE. However, the control is done quickly in order to be efficient in time and is done remotely.
- Not practical: The security agent is physically present and close from the attacker and the control is really thorough (e.g., the security agent checks the fingers of the individual before fingerprint recognition). The evaluation laboratory can notice that an attack is "not practical" when the level of security control is high enough to consider that an attacker is not enough confident to perform an attack.

Table 12 lists the degree of scrutiny weight's intervals for identification and exploitation phases.

Table 12 Degree of scrutiny weights

Interval	Identification weight	Exploitation weight
None	0	0
Overseen	2~~3~~	~~5~~3
Not Practical	*	*

11 Report

The report is a document which presents the TOE and summarizes the work done by the evaluation laboratory. This document has the purpose to be public, but the TOE developer can decide to keep it private. The report shall provide at least the following items:

1. Introduction
   - Document scope
   - Report identification
   - Glossary
   - Formatting
2. Identification of the TOE and the security target
3. Security problem and environment
   - Usage and environment
   - Expert opinion on the security problem
4. Product implementation
   - Setup
   - Ease of use
   - Expert opinion and potential vulnerabilities identified
5. Conception and development
   - Documents and supplies
   - Impact analysis
   - Architecture
   - Attack surface analysis
   - Expert opinion and identified vulnerabilities
6. Component version analysis
   - Components used by the TOE
   - Expert opinion
7. Compliance and resistance of security functions
   - Summary of analyzed/unanalyzed security functions
   - Details of the analysis work (test results)
8. Evaluation summary
   - Summary of non-compliances
   - Summary of technical facts
   - Summary of vulnerabilities
   - Summary on the security of the TOE
   - Expert opinion
9. References

Evaluations of IAD mechanisms shall report the following:

- number of injection attack instruments, threats and attack types considered in the evaluation.
- number of test volunteers involved in the testing.
- number of sources from which IAIs were created.
- description of output information available from IAD mechanism.

The work done by the evaluator shall be formatted like this:

Vulnerability

A vulnerability is a weakness of the TOE allowing the establishment of an attack path and an attack rating. In the report, the vulnerabilities will be presented in this form:

VUL.X : « Vulnerability title »

Vulnerability description.

Technical fact

A technical fact is a slight weakness or bad practice that does not allow the establishment of an attack path and its rating. In the report, the technical facts will be presented in this form:

TF.X : « Technical fact title »

Technical fact description.

Non-compliance

A non-compliance of the TOE corresponds to a non-compliance of the TOE with respect to the security target written for this technical audit. Please note that a non-compliance does not call into question the security of the TOE. In the report, non-compliances will be presented in this form:

NC.X : « Non-compliance title »

Non-compliance description.

Positive statement

A positive statement corresponds to the absence of vulnerability or technical fact on an analyzed element of the TOE. In this report, the positive statements will be presented in this form:

PS.X : « Positive statement title»

Positive statement description.

Annex A(normative)1136

Evaluation success decision based on vulnerability identification and exploitation and attack rating

The result of the evaluation, Pass or Fail, will depend on the rating obtained by the attack which would bypass the system. To get a Pass, the TOE needs:

- **To have a bona fide presentation rate (BPCER for IAD sub-system evaluation and FNMR for full system evaluation) corresponding to the one indicated in the security target, and it is recommended with a maximum of 15%. At least, 300 legitimate transactions shall be performed by the laboratory along the evaluation process.**
- **To be resilient to all attacks reaching the level corresponding to the evaluation's level. If there is an existing vulnerability (i.e. the attack has been identified and exploited), rated with a level under or equal to the evaluation's level (see Clause 8.6), it means that the TOE is not resilient for such attack, and thus that the evaluation's result is FAIL.**

EXAMPLE A TOE, which is undertaking a conformance evaluation with this TS at Substantial Level will get a Pass result even if an attack rated as High level has fooled the TOE during the assessment. This High level vulnerability will be considered as residual risk.

Annex B
(informative)2147

Different examples of injection attacks and injection attack instruments in the litterature

B.1 Injection attacks

In [14], the authors show how to perform injection attacks on state-of-the-art Presentation Attack Detection for face recognition systems. In [23], the authors perform injection attacks on a Remote Identity Proofing Solution using a passport and face recognition.

The Table 13 summarizes the injection attack methods and instruments used by the authors:

Table 13 Example of injection attacks presented in [14] and in [23]

Injection Attack Methods	Injection Attack Instruments
Virtual Camera Software	A portrait image
External Capture Card	A morphed image
Android Camera API hooking	A portrait image animated (also called face reenactment)
	A portrait video
	An edited portrait video
	A low quality deepfake video
	A high quality deepfake video

B.2 Injection attack instruments

A lot of different digital biometric trait falsification techniques are presented in the literature. Table 14 presents a non-exhaustive list of injection attack instruments proposed by researchers:

Table 14 Examples of injection attacks instruments from literature

Biometric characteristic	Injection Attack Instruments	Examples in literature
Face	Deepfake video	[7], [14], [15], [16]
	Face reenactment	[7], [14], [17]
	Morphed image	[7], [18]
Voice	Synthetised voice with text to speech	[19], [20]
	Synthetised voice with voice	[19], [20]

	conversion	
	Mimicked voice	[21]
Iris	Synthetic irises	[24], [25]
Fingerprint	Synthetic fingerprints	[25], [26]

Annex C
(informative)3158

Obstacles to biometric data injection attack in a biometric system

C.1 Biometric data injection attack at enrolment

This paragraph gives a focus onto attacks on the enrolment process for identity proofing solutions for know-your-costumer services which emerge into sensitive markets such as financial activities or governmental services for instance.

For a biometric data injection attack to succeed:

1. the genuine biometric sample is replaced by the IAI into the targeted biometric system,
2. the IAI is successfully processed to produce a biometric reference,
3. it is possible to make the attack under the system-level security procedures in place, and
4. if present, a IAD subsystem does not classify the biometric sample as an attack.

Dependent on the type of biometric system and the quality of the injection attack, the success of the attack might be prevented at any of these stages. For instance (corresponding to the order of the stages above):

1. The replacement can be detected and thus the biometric sample received is classified as malicious by the system,
2. The quality of the replaced biometric sample is not sufficient for feature extraction,

C.2 Biometric data injection attack at verification

This paragraph gives a focus onto biometric impostors which will represent a huge threat for identity proofing solutions based on biometric verification with identity document which emerge into sensitive markets such as border crossing management, banking activities or governmental services for instance.

For an injection attack to succeed:

1. the genuine biometric sample is replaced by the IAI into the targeted biometric system,
2. the IAI is successfully processed to produce a biometric sample,
3. the comparison between the target biometric reference and the biometric probe leads to a match,
4. it is possible to make the attack under the system-level security procedures in place, and
5. if present, a IAD subsystem does not classify the IAI as an attack.

Dependent on the type of biometric system and the quality of the injection attack, the success of the attack might be prevented at any of these stages. For instance (corresponding to the order of the stages above):

1. The replacement can be detected and thus the biometric sample received is classified as malicious by the system

   EXAMPLE: The system could detect the replacement because the recorded voice is not following the expected response to the challenge, or because a machine learning component detects relevant artifacts in the sample.

2. The quality of the replaced biometric sample is not sufficient for feature extraction,

3. Due to the quality of the data, the attack led to a non-match with the targeted biometric reference,

<u>END OF DOCUMENT</u>

Bibliography

[1] ANSSI. “Référentiel d’exigences ANSSI – Prestataires de vérification d’identité `à distance - version 1.1”. In: (2021). URL: https://www.ssi.gouv.fr/uploads/2021/03/anssi-referentiel-exigences-pvid-v1.1.pdf (visited on 01/25/2022).

[2] ETSI. “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects” In: (2021). URL: https://www.etsi.org/component/rsfiles/download-file/files?path=ESITraining%255CETSI%2Bstandards%2Bfor%2Btrust%2Bservices%2Band%2Bdigital%2Bsignatures%2B-%2B6%2Bidentity%2Bproofing%2BSL%2Bv3.pdf (visited on 01/25/2022)

[3] ENISA. “Remote Identity Proofing : Attacks and Countermeasures”. In: (2022). URL: https://www.enisa.europa.eu/publications/remote-identity-proofing-attacks-countermeasures (visited on 05/05/2022)

[4] BSI. “Technical Guideline TR-03147 Assurance Level Assessment of Procedures for Identity Verification of Natural Persons”. In: (2018). URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03147/TR03147.pdf?__blob=publicationFile&v=1 (visited on 05/05/2022)

[5] Ratha N.K., Connell J.H., Bolle R.M. “Enhancing security and privacy in biometrics-based authentication systems”. IBM Syst. J. 2001, 40 (3)

[6] ISO/IEC. “30107-1 Information technology – Biometric presentation attack detection - Part 1: Framework”. In: (2016). URL: https://www.iso.org/standard/53227.html.

[7] Carta, K., Mouille, S, Barral, C., El Mrabet, N., “On the Pitfalls of Videoconferences for Challenge-Based Face Liveness Detection”. In Proceedings of the 25th World Multi-Conference on Systemics, Cybernetics and Informatics: WMSCI 2021, Vol. I, pp. 1-6. International Institute of Informatics and Cybernetics, July 2021.

[8] ISO/IEC. “19795-1 Information technology — Biometric performance testing and reporting — Part 1: Principles and framework”. In: (2021). URL: https://www.iso.org/standard/73515.html

[9] ISO/IEC “ISO/IEC. “30107-1 Information technology — Biometric presentation attack detection — Part 1: Framework”. In (2022) URL: https://www.iso.org/standard/53227.html

[10] European Parliament. “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation)”. In: (2016). URL: https//eur-lex.europa.eu/eli/reg/2016/679/oj

[11] JIL. “Application of Attack Potential to Smartcards”. In: (2013). URL: https://sogis.org/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v2-9.pdf

[12] CCN (Centro Criptologico Nacional). CCN-STIC 140-F.11 – Guia de Seguridad de las TIC – Taxonomía de productos STIC – Anexo F.11: Herramientas de Videoidentificación. Public access: https://www.ccncert.cni.es/en/series-ccn-stic/guias-deacceso-publico-ccn-stic/5461-guia-140-anexo-f-11-herramientas-devideoidentificacion.html

[13] U. Waldmann, D. Scheuermann, C. Eckert: Protected transmission of biometric user authentication data for oncard-matching. In: 2004 ACM Symposium on Applied Computing; https://doi.org/10.1145/967900.967990

[14] Carta, K., Huynh, A., Mouille, S., Brangoulo, S., Mrabet, N., Barral, C. (2023). “How video injection attacks can even challenge state-of-the-art Face Presentation Attack Detection Systems” In: 14th International Multi-Conference on Complexity, Informatics and Cybernetics.

[15] D. Güera and E. J. Delp, "Deepfake Video Detection Using Recurrent Neural Networks," 2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Auckland, New Zealand, 2018, pp. 1-6

[16] P. Korshunov and S. Marcel, "Vulnerability assessment and detection of Deepfake videos," 2019 International Conference on Biometrics (ICB), Crete, Greece, 2019, pp. 1-6

[17] Thies, J., Zollhofer, M., Stamminger, M., Theobalt, C., & Nießner, M. (2016). Face2face: Real-time face capture and reenactment of rgb videos. In Proceedings of the IEEE conference on computer vision and pattern recognition (pp. 2387-2395).

[18] M. Ferrara, A. Franco and D. Maltoni, "The magic passport," IEEE International Joint Conference on Biometrics, Clearwater, FL, USA, 2014, pp. 1-7

[19] Ergünay, S. K., Khoury, E., Lazaridis, A., & Marcel, S. (2015, September). On the vulnerability of speaker verification to realistic voice spoofing. In 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS) (pp. 1-6). IEEE

[20] Zhang, Y., Jiang, F., & Duan, Z. (2021). One-class learning towards synthetic voice spoofing detection. IEEE Signal Processing Letters, 28, 937-941.

[21] Lau, Y. W., Wagner, M., & Tran, D. (2004, October). Vulnerability of speaker verification to voice mimicking. In Proceedings of 2004 International Symposium on Intelligent Multimedia, Video and Speech Processing, 2004. (pp. 145-148). IEEE.

[22] ISO/IEC. “19792 Information security, cybersecurity and privacy protection - General principles of security evaluation of biometric systems”. In: (2009). URL: https://www.iso.org/standard/84753.html

[23] Carta, K., Mouille, S., Mrabet, N., Barral, C. (2022). “Video injection attacks on remote digital identity verification solution using face recognition” In: 13th International Multi-Conference on Complexity, Informatics and Cybernetics.

[24] S. Shah and A. Ross, "Generating Synthetic Irises by Feature Agglomeration," *2006 International Conference on Image Processing*, Atlanta, GA, USA, 2006, pp. 317-320, doi: 10.1109/ICIP.2006.313157.

[25] A. Makrushin, A. Uhl and J. Dittmann, "A Survey on Synthetic Biometrics: Fingerprint, Face, Iris and Vascular Patterns," in *IEEE Access*, vol. 11, pp. 33887-33899, 2023, doi: 10.1109/ACCESS.2023.3250852.

[26] J. J. Engelsma, S. Grosz and A. K. Jain, "PrintsGAN: Synthetic Fingerprint Generator," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 5, pp. 6111-6124, 1 May 2023, doi: 10.1109/TPAMI.2022.3204591.