BSI Standards Publication

Biometric data injection attack detection

bsi.

National foreword

This Published Document is the UK implementation of CEN/TS 18099:2024.

The UK participation in its preparation was entrusted to Technical Committee IST/44, Biometrics.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

This publication is not to be regarded as a British Standard.

Published by BSI Standards Limited 2024

ISBN 978 0 539 31507 3

ICS 35.030

Compliance with a Published Document cannot confer immunity from legal obligations.

This Published Document was published under the authority of the Standards Policy and Strategy Committee on 30 November 2024.

Amendments/corrigenda issued since publication

Date	Text affected

TECHNICAL SPECIFICATION **CEN/TS 18099**

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION November 2024

ICS 35.030

English Version

Biometric data injection attack detection

Détection d'attaques par injection de données biométriques

Detektion von Injektionsangriffen mit biometrischen Daten

This Technical Specification (CEN/TS) was approved by CEN on 13 October 2024 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. CEN/TS 18099:2024 E

Contents

Page

European foreword **4**

Introduction **5**

1 Scope **7**

2 Normative references **7**

3 Terms and definitions **8**

4 Symbols and abbreviations **10**

5 Conformance **11**

6 Characterization of biometric data injection attacks **11**
6.1 Injection Attack Methods **11**
6.2 Injection Attack Instruments **13**

7 Framework for injection attack detection mechanisms **14**
7.1 Overview of different types of injection attack detection **14**
7.2 Injection Attack Method Defence Mechanisms **15**
7.3 Injection Attack Instrument Defence Mechanisms **16**
7.4 Combination of different types of IAD **17**
7.5 Security vs general public use **17**

8 Evaluation of IAD systems **18**
8.1 Overview **18**
8.2 General principle of evaluation **18**
8.3 Injection attack methods **20**
8.4 Injection attack instruments **20**
8.5 Personal Data Protection of volunteers in IAD Assessments **21**
8.6 Levels of difficulty of the evaluations **21**

9 Metrics for IAD evaluations **23**
9.1 General **23**
9.2 Metrics for IAD subsystem evaluation **23**
9.3 Metrics for full system evaluation **23**

10 Attacks rating methodology **24**
10.1 General **24**
10.2 Identification and exploitation phases **25**
10.3 Time effort **25**
10.4 Expertise **26**
10.5 Knowledge of the product under evaluation **26**
10.6 Equipment **27**
10.7 Access to TOE **28**
10.8 Access to biometric characteristics **29**
10.9 Degree of scrutiny **29**

11 Report **30**

Annex A (normative) **Evaluation success decision based on vulnerability identification and exploitation and attack rating** **32**

Annex B (informative) **Different examples of injection attacks and injection attack instruments in the literature** **33**
B.1 Injection attacks **33**
B.2 Injection attack instruments **33**
Annex C (informative) **Obstacles to biometric data injection attack in a biometric system** **34**
C.1 Biometric data injection attack at enrolment **34**
C.2 Biometric data injection attack at verification **34**
Bibliography **36**

European foreword

This document (CEN/TS 18099:2024) has been prepared by Technical Committee CEN/TC 224 “Personal identification and related personal devices with secure element, systems, operations and privacy in a multi sectorial environment”, the secretariat of which is held by AFNOR.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. CEN shall not be held responsible for identifying any or all such patent rights.

Any feedback and questions on this document should be directed to the users’ national standards body. A complete listing of these bodies can be found on the CEN website.

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Republic of North Macedonia, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Türkiye and the United Kingdom.

Introduction

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 recognize people in order to check if they are known or not to 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 given rise to 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, the 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. The ISO/IEC 30107 series does 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.

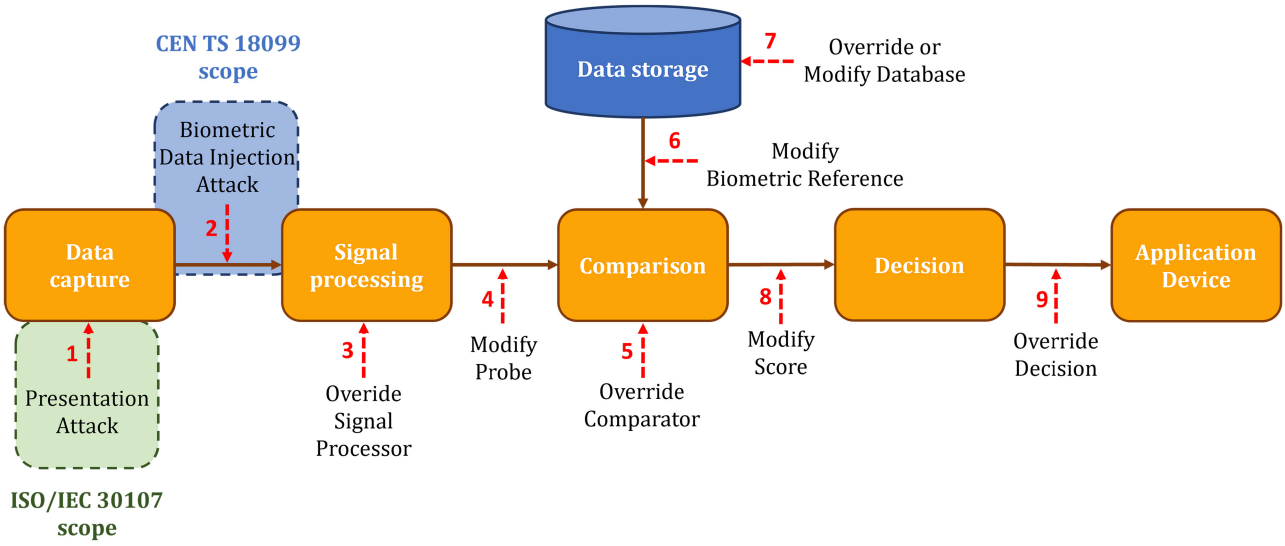

Figure 1 — Examples of points of attack in a biometric system [5]

The emergence of remote identity verification solutions based on biometric (such as facial) recognition and the use of mobile applications or web browser applications could 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 document 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 standardization 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 document 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 document.

1 Scope

This document provides an 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 document provides guidance on:

- System for the detection of Injection Attack Instruments (defined in 3.12),
- Appropriate mitigation risk of Injection Attack Instruments,
- Creation of test plan for the evaluation of Injection Attack Detection system (defined in 3.9).

If presentation attacks testing is out of scope of this document, 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 document (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 in 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.

EN ISO/IEC 2382-37, *Information technology — Vocabulary — Part 37: Biometrics (ISO/IEC 2382-37)*

ISO/IEC 19795-1, *Information technology — Biometric performance testing and reporting — Part 1: Principles and framework*

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

ISO/IEC 30107-3, *Information technology — Biometric presentation attack detection — Part 3: Testing and reporting*