SLOVENSKI STANDARD
kSIST-TS FprCEN/TS 18099:2024

01-september-2024

Odkrivanje napadov z vnašanjem biometričnih podatkov

Biometric data injection attack detection

Digitale Präsentationsangriffe in biometrischen Systemen

Détection d'attaques par injection de données biométriques

Ta slovenski standard je istoveten z: **FprCEN/TS 18099**

---

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ICS:

kSIST-TS FprCEN/TS 18099:2024
https://standards.iteh.ai/catalog/standards/sist/7f18c-de[illegible]-d95a9b752cc9/ksist-ts-fprcen-ts-18099-2024

35.030	Informacijska varnost	IT Security
35.240.15	Identifikacijske kartice. Čipne kartice. Biometrija	Identification cards. Chip cards. Biometrics

kSIST-TS FprCEN/TS 18099:2024 **en,fr,de**

2003-01.Slovenski inštitut za standardizacijo. Razmnoževanje celote ali delov tega standarda ni dovoljeno.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

kSIST-TS FprCEN/TS 18099:2024
https://standards.iteh.ai/catalog/standards/sist/09b7f18c-deb7-439e-bcf0-d95a9b752cc9/ksist-ts-fprcen-ts-18099-2024

kSIST-TS FprCEN/TS 18099:2024

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

FINAL DRAFT
FprCEN/TS 18099

June 2024

ICS 35.240.15

English Version

Biometric data injection attack detection

Détection d'attaques par injection de données biométriques

Digitale Präsentationsangriffe in biometrischen Systemen

This draft Technical Specification is submitted to CEN members for Vote. It has been drawn up by the Technical Committee CEN/TC 224.

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.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

Warning : This document is not a Technical Specification. It is distributed for review and comments. It is subject to change without notice and shall not be referred to as a Technical Specification.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

kSIST-TS FprCEN/TS 18099:2024
https://standards.iteh.ai/catalog/standards/sist/09b7f18c-deb7-439e-bcf0-d95a9b752cc9/ksist-ts-fprcen-ts-18099-2024

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

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

© 2024 CEN All rights of exploitation in any form and by any means reserved worldwide for CEN national Members.

Ref. No. FprCEN/TS 18099:2024 E

kSIST-TS FprCEN/TS 18099:2024

Contents

Page

iTeh Standards
(https://standards.iteh.ai)
Document Preview
kSIST-TS FprCEN/TS 18099:2024
https://standards.iteh.ai/catalog/standards/sist/...-ts-18099-2024

kSIST-TS FprCEN/TS 18099:2024

iTeh Standards
(https://standards.iteh.ai)
Document Preview

kSIST-TS FprCEN/TS 18099:2024
https://standards.iteh.ai/catalog/standards/sist/09b7f18c-deb7-439e-bcf0-d95a9b752cc9/ksist-ts-fprcen-ts-18099-2024

kSIST-TS FprCEN/TS 18099:2024

European foreword

This document (FprCEN/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.

This document is currently submitted to the Vote on TS.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

kSIST-TS FprCEN/TS 18099:2024
https://standards.iteh.ai/catalog/standards/sist/09b7f18c-deb7-439e-bcf0-d95a9b752cc9/ksist-ts-fprcen-ts-18099-2024

kSIST-TS FprCEN/TS 18099:2024

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.

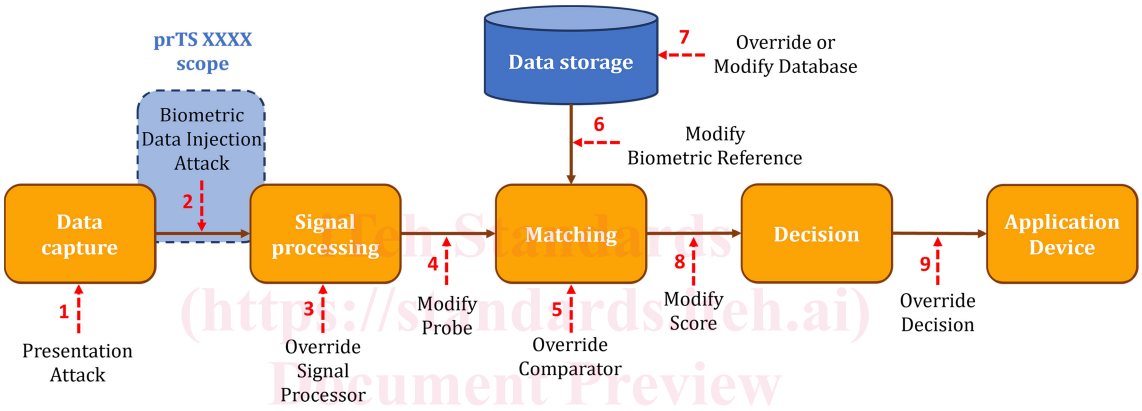

Figure 1 — Examples of points of attack in a biometric system [4]

iTeh Standards (https://standards.iteh.ai) Document Preview
kSIST-TS FprCEN/TS 18099:2024
https://standards.iteh.ai/catalog/standards/sist/09b7f18c-deb7-439e-bcf0-d95a9b752cc9/ksist-ts-fprcen-ts-18099-2024

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],

kSIST-TS FprCEN/TS 18099:2024

— 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.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

kSIST-TS FprCEN/TS 18099:2024
https://standards.iteh.ai/catalog/standards/sist/09b7f18c-deb7-439e-bcf0-d95a9b752cc9/ksist-ts-fprcen-ts-18099-2024

kSIST-TS FprCEN/TS 18099:2024

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.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

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),

kSIST-TS FprCEN/TS 18099:2024
https://standards.iteh.ai/catalog/standards/sist/09b7f18c-deb7-4e9e-be10-d95a9b752ce5/ksist-ts-fprcen-ts-18099-2024

- 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.

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

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*

kSIST-TS FprCEN/TS 18099:2024

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37, ISO/IEC 19795-1, ISO/IEC 30107-1 and ISO/IEC 30107-3, and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

- ISO Online browsing platform: available at https://www.iso.org/obp
- IEC Electropedia: available at https://www.electropedia.org/

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 (3.12), before the execution of the feature extraction process

Note 1 to entry: 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].

iTeh Standards
(https://standards.iteh.ai)
Document Preview
kSIST-TS FprCEN/TS 18099:2024
https://standards.iteh.ai/catalog/standards/sist/09b7f18c-deb7-439e-bcf0-d95a9b752cc9/ksist-ts-fprcen-ts-18099-2024

3.4
enrolment evaluation
measuring of the ability of a biometric system to correctly detect injection attacks and classify bona fide presentations at enrolment phase

3.5
full system
system which includes both biometric comparison and Injection Attack Detection (IAD) subsystems

3.6
full system evaluation
measuring of 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 behaviour

3.8
injection
modification of a data flow by modifying the data source or overwriting the data

kSIST-TS FprCEN/TS 18099:2024

3.9
injection attack detection
IAD
automated determination of a biometric data injection attack

Note 1 to entry 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
measuring of 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 (3.17), used in a biometric data injection attack

iTeh Standards
(https://standards.iteh.ai)
Document Preview

3.13
injection attack instrument defence mechanism
IAIDM
biometric defence mechanisms aiming at making a biometric system resistant to injection attack instruments

kSIST-TS FprCEN/TS 18099:2024
https://standards.iteh.ai/catalog/standards/sist/09b7f18c-deb7-439e-bcf0-d95a9b752cc9/ksist-ts-fprcen-ts-18099-2024

3.14
IAI species
class of injection attack instruments created using a common production method and based on different biometric characteristics

EXAMPLE 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

kSIST-TS FprCEN/TS 18099:2024

3.18
read-only memory
ROM
type of computer storage containing non-volatile, permanent data that, normally, can only be read, not written to

Note 1 to entry: ROM contains the programming that allows a computer to start up or regenerate each time it is turned on.

3.19
operating system read-only memory
OS ROM
ROM which contains the Operating System of the device, which are all the programs which manage resources of the device

3.20
security target
document which defines the assets protected by the Target Of Evaluation (TOE), the threats which will be taken into account during the evaluation and the security functions implemented by the TOE to prevent the threats

3.21
target of evaluation
TOE
product that is the subject of the evaluation

iTeh Standards
(https://standards.iteh.ai)
Document Preview

3.22
threat
injection attack scenario used by the attacker to bypass the IAD mechanism

Note 1 to entry: For the other terms not defined here, see their definition in the normative references.

https://standards.iteh.ai/catalog/standards/sist/09b7f18c-deb7-439e-bcf0-d95a9b752cc9/ksist-ts-fprcen-ts-18099-2024

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 and 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