INTERNATIONAL STANDARD

ISO/IEC 30107-1

First edition
2016-01-15

Information technology — Biometric presentation attack detection —

Part 1: Framework

Technologies de l'information — Détection d'attaque de présentation en biométrie —

Partie 1: Structure

Reference number
ISO/IEC 30107-1:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

ISO/IEC 30107-1 was prepared by Technical Committee ISO/TC JTC1, *Information technology*, Subcommittee SC 37, *Biometrics*.

ISO/IEC 30107 consists of the following parts, under the general title *Information technology — Biometric presentation attack detection*:

— *Part 1: Framework*

— *Part 2: Data formats*

— *Part 3: Testing and reporting*

Introduction

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

Since the beginning of these technologies, the possibility of subversion of recognition by determined adversaries has been widely acknowledged, as has the need for countermeasures to detect and defeat subversive recognition attempts, or presentation attacks. Subversion of the intended function of a biometric technology can take place at any point within a security system and by any actor, whether a system insider or an external adversary. This International Standard (ISO/IEC 30107) will be limited in scope, however, focusing on techniques for the automated detection of presentation attacks undertaken by biometric capture subjects at the point of presentation and collection of the relevant biometric characteristics. We will call these automated techniques "Presentation Attack Detection" (PAD) methods.

The potential for subversion of biometric systems at the point of data collection by determined individuals acting as biometric capture subjects has limited the use of biometrics in applications which are unsupervised by an agent of the system owner, such as remote collections over untrusted networks. Guidelines on e-authentication, for example, do not recommend the use of biometrics as an authentication factor for this reason. In unattended applications, such as remote authentication over open networks, automated presentation attack detection methods could be applied to mitigate the risks of attack. Standards, best practices and independently evaluated techniques could improve the security of all systems employing biometrics, whether using supervised or unsupervised data capture, including those using biometric recognition to secure online transactions.

As is the case for biometric recognition, PAD techniques are subject to errors, both false positive and false negative: false positive indications wrongly categorize routine presentations as attacks, thus impairing the efficiency of the system, and false negative indications wrongly categorize presentation attacks as routine, not preventing a security breach. Therefore, the decision to use a specific implementation of PAD will depend upon the requirements of the application and consideration of the trade-offs with respect to security and efficiency.

The purpose of this part of ISO/IEC 30107 is to provide a foundation for PAD through defining terms and establishing a framework through which presentation 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. This foundation will also benefit other standards projects in ISO/IEC committees and sub-committees. This International Standard does not advocate a specific technique as a standard PAD tool.

There are two other parts of ISO/IEC 30107. Part 2 defines data formats for conveying the type of approach used in biometric presentation attack detection and for conveying the results of presentation attack detection methods. Part 3 establishes principles and methods for performance assessment of presentation attack detection algorithms or mechanisms.

Information technology — Biometric presentation attack detection —

Part 1: Framework

1 Scope

This part of ISO/IEC 30107 establishes terms and definitions that are useful in the specification, characterization and evaluation of presentation attack detection methods.

Outside the scope are

— standardization of specific PAD detection methods;

— detailed information about countermeasures (i.e. anti-spoofing techniques), algorithms, or sensors; and

— overall system-level security or vulnerability assessment.

The attacks to be considered in ISO/IEC 30107 are those that take place at the sensor during the presentation and collection of the biometric characteristics.

Any other attacks are considered outside the scope of ISO/IEC 30107.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 2382-37:2012, *Information technology — Vocabulary — Part 37: Biometrics*

NOTE The electronic version of ISO/IEC 2382-37:2012 can be downloaded for free from the ISO/IEC Information Technology Task Force (ITTF) web site: http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 2382-37:2012 and the following apply.

3.1
artefact
artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

3.2
liveness
quality or state of being alive, made evident by anatomical characteristics, involuntary reactions or physiological functions, or voluntary reactions or subject behaviours

EXAMPLE 1 Absorption of illumination by the skin and blood are anatomical characteristics.