BS ISO/IEC 30107-1:2016

BSI Standards Publication

Information technology — Biometric presentation attack detection

Part 1: Framework

bsi.

...making excellence a habit.™

Document Sharing Hub

Full document details: BS ISO/IEC 30107-1:2016

National foreword

This British Standard is the UK implementation of ISO/IEC 30107-1:2016.

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 secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2016.
Published by BSI Standards Limited 2016

ISBN 978 0 580 77139 2

ICS 35.040

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 January 2016.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30107-1:2016

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)

Documents
Document Sharing Hub
© ISO/IEC 2016

Full document details: BS ISO/IEC 30107-1:2016

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2016, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 30107-1:2016

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **2**
5 Characterisation of presentation attacks ... **3**
5.1 General ... 3
5.2 Presentation attack instruments ... 4
6 Framework for presentation attack detection methods ... **5**
6.1 Types of presentation attack detection ... 5
6.2 The role of challenge-response ... 5
6.2.1 Challenge-response related to liveness ... 6
6.2.2 Liveness not related to challenge-response ... 6
6.2.3 Challenge-response not related to biometrics ... 6
6.3 Presentation attack detection process ... 6
6.4 Presentation attack detection within biometric system architecture ... 7
6.4.1 Overview in terms of the generalized biometric framework ... 7
6.4.2 PAD processing considerations relative to the other biometric subsystems ... 8
6.4.3 PAD location implications regarding data interchange ... 9
7 Obstacles to biometric imposter presentation attacks in a biometric system ... **9**
Bibliography ... **11**

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30107-1:2016

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*

© ISO/IEC 2016 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30107-1:2016

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.

© ISO/IEC 2016 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 30107-1:2016