TECHNICAL SPECIFICATION

ISO/IEC TS 30104

First edition
2015-05-15

Information Technology — Security Techniques — Physical Security Attacks, Mitigation Techniques and Security Requirements

Technologies de l'information — Techniques de sécurité — Attaques de sécurité physique, techniques d'atténuation et exigences de sécurité

Reference number
ISO/IEC TS 30104:2015(E)

© ISO/IEC 2015



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2015, 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

Contents

Page

Foreword ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Symbols and abbreviated terms **5**
5 Physical security **5**
6 Physical security invasive mechanisms **6**
6.1 Overview 6
6.2 Tamper proof 7
6.3 Tamper resistant 7
6.4 Tamper detection 7
6.5 Tamper evident 7
6.6 Additional physical security considerations 8
6.6.1 Summary 8
6.6.2 Size and weight 8
6.6.3 Mixed and Layered Systems 8
7 Physical security invasive attacks and defences **8**
7.1 Overview 8
7.2 Attacks 9
7.2.1 Attack mechanisms 9
7.2.2 Machining methods 9
7.2.3 Shaped charge technology 11
7.2.4 Energy attacks 11
7.2.5 Environmental conditions 12
7.3 Defences 12
7.3.1 Overview 12
7.3.2 Tamper resistant 13
7.3.3 Tamper evident 14
7.3.4 Tamper detection sensor technology 15
7.3.5 Tamper responding 18
8 Physical security non-invasive mechanisms **20**
8.1 Overview 20
8.2 Mixed and Layered Systems 20
9 Physical security non-invasive attacks and defences **20**
9.1 Overview 20
9.2 Attacks 20
9.2.1 Overview 20
9.2.2 External Probe attacks 20
9.2.3 External EME attacks 21
9.2.4 Timing analysis 21
9.3 Defences 21
10 Operating Envelope Concept **22**
11 Development, delivery and operation considerations **22**
11.1 Introduction 22
11.2 Development 22
11.2.1 Functional test and debug 22
11.2.2 Security testing 22
11.2.3 Environmental testing 23
11.2.4 Factory installed keys or security parameters 23

© ISO/IEC 2015 – All rights reserved

11.3 Delivery ... 23
11.3.1 Documentation ... 23
11.3.2 Packaging ... 24
11.3.3 Delivery verification ... 24
11.4 Operation ... 24
11.4.1 Overview ... 24
11.4.2 Implementation feedback ... 24
11.4.3 Feedback during attack ... 24

12 Physical security evaluation and testing ... 24
12.1 Overview ... 24
12.2 Standards ... 25
12.2.1 FIPS PUB 140-2, ***Security Requirements for Cryptographic Modules*** ... ***25***
12.2.2 Derived Test Requirements for FIPS PUB 140-2, ***Security Requirements for Cryptographic Modules*** ... ***25***
12.2.3 ISO/IEC 19790:2012, ***Information technology — Security techniques — Security requirements for cryptographic modules*** ... ***25***
12.2.4 ISO/IEC 24759:2014 ***Information technology — Security techniques — Test requirements for cryptographic modules*** ... ***26***
12.2.5 ISO/IEC 15408-1:2009, ***Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*** ... ***26***
12.2.6 ISO/IEC 15408-2:2008, ***Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*** ... ***26***
12.2.7 ISO/IEC 15408-3:2008, ***Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*** ... ***27***
12.2.8 ISO/IEC 18045:2008, ***Information technology — Security techniques — Methodology for IT security evaluation*** ... ***27***
12.3 Programs and schemes ... 27
12.3.1 NIST and CSE Cryptographic Module Validation Program ... 27
12.3.2 Japan Cryptographic Module Validation Program ... 27
12.3.3 Korea Cryptographic Module Validation Program ... 27
12.3.4 Common Criteria ... 28

Annex A (informative) **Example of a physical security design ... 29**

Bibliography ... 30

 © ISO/IEC 2015 – All rights reserved

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.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *Security techniques*.

© ISO/IEC 2015 – All rights reserved

Introduction

The protection of sensitive information does not rely solely on the implementation of software mechanisms employing cryptographic techniques, but also relies significantly on appropriate hardware implemented security devices that employ tamper detection and protection of critical security parameters (e.g. cryptographic keys, authentication data, etc.).

This is especially relevant for devices that may be installed, deployed or operated in hostile, untrusted, or non-secure environments, or for devices that contain high-value data assets.

An attacker may not be motivated by the economic value or the successful access to sensitive information, but simply the challenge of compromising a design or system that has been advertised as “secure”. The challenge to break the design gives such an attacker instant fame and recognition amongst peer groups.

Currently, much of the information in this area originates from disparate sources, may not be presented consistently, and may not address appropriate evaluation and testing techniques.

© ISO/IEC 2015 – All rights reserved

Information Technology — Security Techniques — Physical Security Attacks, Mitigation Techniques and Security Requirements

1 Scope

Physical security mechanisms are employed by cryptographic modules where the protection of the modules sensitive security parameters is desired. This Technical Specification addresses how security assurance can be stated for products where the risk of the security environment requires the support of such mechanisms. This Technical Specification addresses the following topics:

— a survey of physical security attacks directed against different types of hardware embodiments including a description of known physical attacks, ranging from simple attacks that require minimal skill or resources, to complex attacks that require trained, technical people and considerable resources;

— guidance on the principles, best practices and techniques for the design of tamper protection mechanisms and methods for the mitigation of those attacks; and

— guidance on the evaluation or testing of hardware tamper protection mechanisms and references to current standards and test programs that address hardware tamper evaluation and testing.

The information in this Technical Specification is useful for product developers designing hardware security implementations, and testing or evaluation of the final product. The intent is to identify protection methods and attack methods in terms of complexity, cost and risk to the assets being protected. In this way cost effective protection can be produced across a wide range of systems and needs.

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 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

ISO/IEC 24759, *Information technology — Security techniques — Test requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19790 and ISO/IEC 24759 apply and are duplicated here for reference.

NOTE Definitions followed by a reference in square brackets are taken verbatim from ISO/IEC 19790:2012 or ISO/IEC 24759:2014 All other terms and definitions are adapted from those in ISO/IEC 19790:2012 or ISO/IEC 24759:2014.

© ISO/IEC 2015 – All rights reserved