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 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.

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

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.

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.

3.1
compromise
unauthorised disclosure, modification, substitution, or use of critical security parameters or the unauthorised modification or substitution of public security parameters

[SOURCE: ISO/IEC 19790:2012, 3.13]

3.2
conformal coating
material that may be applied in layers or in various thicknesses that adhere directly to the electronic components or printed circuit boards and provide a hard coating that deters machining, probing, energy or chemical attacks

3.3
critical security parameter
CSP
security related information whose disclosure or modification can compromise the security of a cryptographic module

[SOURCE: ISO/IEC 19790:2012, 3.18]

EXAMPLE Secret and private cryptographic keys, authentication data such as passwords, PINs, certificates or other trust anchors.

Note 1 to entry: A CSP can be plaintext or encrypted.

3.4
cryptographic boundary
explicitly defined perimeter that establishes the boundary of all components (i.e. set of hardware, software, or firmware) of the cryptographic module

[SOURCE: ISO/IEC 19790:2012, 3.21]

3.5
cryptographic module
module
set of hardware, software, and/or firmware that implements security functions and are contained within the cryptographic boundary

[SOURCE: ISO/IEC 19790:2012, 3.25]

3.6
differential power analysis
DPA
analysis of the variations of the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to a cryptographic operation

[SOURCE: ISO/IEC 19790:2012, 3.29]

3.7
environmental failure protection
EFP
use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions outside of the module's normal operating range

[SOURCE: ISO/IEC 19790:2012, 3.39]

3.8
environmental failure testing
EFT
use of specific methods to provide reasonable assurance that the security of a cryptographic module will not be compromised by environmental conditions outside of the module's normal operating range

[SOURCE: ISO/IEC 19790:2012, 3.40]

3.9
firmware
executable code of a cryptographic module that is stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution while operating in a non-modifiable or limited operational environment

[SOURCE: ISO/IEC 19790:2012, 3.45]

EXAMPLE Storage hardware can include but is not limited to PROM, EEPROM, FLASH, solid state memory, hard drives, etc.

3.10
hardware
physical equipment/components within the cryptographic boundary used to process programs and data

[SOURCE: ISO/IEC 19790:2012, 3.50]

3.11
passivation
effect of a reactive process in semiconductor junctions, surfaces or components and integrated circuits constructed to include means of detection and protection

[SOURCE: ISO/IEC 19790:2012, 3.87]

EXAMPLE Silicon dioxide or phosphorus glass.

Note 1 to entry: Passivation can modify the behaviour of the circuit. Passivation material is technology dependant

3.12
physical protection
safeguarding of a cryptographic module, CSPs and PSPs using physical means

[SOURCE: ISO/IEC 19790:2012, 3.90]

3.13
production-grade
product, component or software that has been tested to meet operational specifications

[SOURCE: ISO/IEC 19790:2012, 3.95]

3.14
physical security invasive attacks
attacks that involve a physical alteration to the implementation that may also cause an operating aberration different from normal operation

3.15
physical security non-invasive attacks
attacks that do not involve a physical alteration to the implementation cause an operating aberration different from normal operation

3.16
removable cover
physical means which permits an intentionally designed non-damaging access to the physical contents of a cryptographic module

[SOURCE: ISO/IEC 19790:2012, 3.101]

3.17
sensitive security parameters
SSP
critical security parameters (CSP) and public security parameters (PSP)

[SOURCE: ISO/IEC 19790:2012, 3.110]

3.18
simple power analysis
SPA
direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), in relation to the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to a cryptographic operation

[SOURCE: ISO/IEC 19790:2012, 3.114]

3.19
software
executable code of a cryptographic module that is stored on erasable media which can be dynamically written and modified during execution while operating in a modifiable operational environment

[SOURCE: ISO/IEC 19790:2012, 3.116]

EXAMPLE Erasable media can include but not limited to solid state memory, hard drives, etc.

3.20
tamper detection
automatic determination by a cryptographic module that an attempt has been made to compromise the security of the module

[SOURCE: ISO/IEC 19790:2012, 3.125]

3.21
tamper evidence
observable indication that an attempt has been made to compromise the security of a cryptographic module

[SOURCE: ISO/IEC 19790:2012, 3.126]

3.22
tamper response
automatic action taken by a cryptographic module when tamper detection has occurred

[SOURCE: ISO/IEC 19790:2012, 3.127]

3.23
TEMPEST
codename by the US National Security Agency to secure electronic communications equipment from compromising emanations, which, if intercepted and analysed, may disclose the information transmitted, received, handled, or otherwise processed

3.24
timing analysis
TA
analysis of the variations of the response or execution time of an operation in a security function, which may reveal knowledge of or about a security parameter such as a cryptographic key or PIN

3.25
zeroisation
method of destruction of stored data and unprotected SSPs to prevent retrieval and reuse

[SOURCE: ISO/IEC 19790:2012, 3.134]

4 Symbols and abbreviated terms

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

EDC	Error Detection Code
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EME	Electro-Magnetic Emanation
HDL	Hardware Description Language
IC	Integrated Circuit
PROM	Programmable Read-Only Memory
RAM	Random Access Memory
ROM	Read-Only Memory

5 Physical security

Traditionally the term ‘physical security’ has been used to describe protection of material assets such as cash, jewellery, bonds, etc. from fire, water damage, theft, or similar perils. However on-going concerns in computer security have caused physical security to take on a new meaning: technologies and protocols used to safeguard information against physical attack. This information can be anything from a spreadsheet work file to cryptographic keys which are used to protect other files. This information can be stolen without being physically removed from where it is kept. If information can be accessed, it can simply be copied.

Physical security is a barrier placed around a computing system to deter unauthorized physical access. Physical access can be accomplished by either invasive or non-invasive techniques. This concept is complementary to both logical and environmental security. Logical security describes the mechanisms by which operating systems, security protocols and other software prevent unauthorized access to data. Environmental security describes the procedures that limit or prevent unauthorised physical access of a computing system by virtue of location such as guards, cameras, fences, structures, etc. Operational security depends on both the environmental security attributes that the computing system or device will operate and on the physical and logical security attributes of the computing system itself.

It may be reasonable for an individual to have access to a location (environmental security) and not to have access to the information stored on a computing system in that environment (physical and logical security). Physical security is increasingly important because advances in technology have reduced the footprint of what historically were large and complex computing systems to both smaller and mobile devices (e.g. tablet computing devices, smart phones and mobile memory tokens). These historically complex and compute intensive systems, and their system unique applications with large data storage mechanisms, are transitioning out of environmentally secure computer rooms and into less secure offices and homes. They are being migrated on to distributed, cloud-based data platforms and mobile devices where the physical location of the data may be uncertain. If the environment of the deployed computing system provided a measured level of protection, then the level of physical protection of the computing system itself may reduce to a simple tamper detection mechanism (e.g. to detect an insider attack) or where it is not necessary at all. Whereas sensitive information held on a portable device such as a smart card, smart phone or similar device, if lost or misplaced, would require much stronger physical protection. At the same time, the value of the cryptographic critical security parameters (e.g. cryptographic keys) and similar sensitive security parameters which provide access control to data on these computing systems is increasing as centralization decreases. The motivation to attack computing systems is increasing because the rewards for doing so are increasing.

For physical security to be effective the following criteria must be met: in the event of an attack, there should be a low probability of success and a high probability of detection either during the attack, or subsequent to penetration.

Physical security systems to protect sensitive data can make unauthorised access to the data difficult, as a bank vault makes stealing cash a daunting task (tamper resistant). They can trigger mechanisms to thwart the attack, much like an alarm system (tamper detection). They can make an attempted attack apparent so that subsequent inspection will show an attack had been attempted (tamper evident).

Physical security systems can be defined as providing protection against either *invasive* or *non-invasive* attacks. Physical security *invasive attacks* are attacks that involve a physical alteration to the implementation that may also cause an operating aberration different from normal operation. Physical security *non-invasive attacks* are attacks that do not involve a physical alteration to the implementation or cause an operating aberration different from normal operation.

Classification systems have been proposed, accepted and put into use that evaluate or test computing systems according to criteria that measure the difficulty of mounting a successful attack. However many of the methods for evaluation and testing may not lead to comparable results due to the lack of defined evaluation or test methods, scope of the applied methods or the consistency and competence of the evaluators or testers. This had led to the advancement of physical security and evaluation and testing standards; these standards have become accepted as they provide a baseline of repeatable, consistent and comparable results while at the same time the standards are being rigorously and publicly evaluated. These standards led organizations and national bodies to develop evaluation and testing programs to certify or validate implementations to this baseline level of assurance.

6 Physical security invasive mechanisms

6.1 Overview

A variety of physical security techniques are currently employed to protect hardware implementations. The physical security mechanisms must address a wide range of different technology implementations, use environments and attack scenarios. This field is increasingly recognized in the commercial market as users, both business and private individuals, request such features as they have become increasingly aware of the need to protect their sensitive information. Governments have been working on this problem for decades as applied to the protection of information for both unclassified and classified domains. The amount of sensitive, but unclassified, information that governments must protect can be vast, as includes (but is not limited to) health records, tax records, law enforcement records, business records (e.g. procurements or bids), communications, transaction records, and voter information. National and International standards have been developed to address various levels of physical security assurance which in many cases coincide with the use of cryptographic protocols which require the protection of the critical security parameters (e.g. cryptographic keys, access credentials, etc.). The ways and means described here are not an exhaustive list, nor are they represented as ultimate methods.