INTERNATIONAL STANDARD

ISO/IEC 20085-1

First edition
2019-10

IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules —

Part 1: Test tools and techniques

Techniques de sécurité IT — Exigences de l'outil de test et méthodes d'étalonnage de l'outil de test utilisées pour tester les techniques d'atténuation des attaques non invasives dans les modules cryptographiques

Partie 1: Outils et techniques de test

Reference number
ISO/IEC 20085-1:2019(E)

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

Published in Switzerland

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.

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) or the IEC list of patent declarations received (see http://patents.iec.ch).

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

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

A list of all parts in the ISO/IEC 20085 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

Cryptographic modules provide cryptographic services and protect critical security parameters (CSPs). Protection of CSPs can either be logical, physical, or both. However, information such as knowledge of CSPs can leak out of the cryptographic module when manipulated, if the module is not designed to mitigate such leakage. Without mitigation, a malicious attacker can record available side-channel leakage. This leakage is a physical quantity related to the CSPs and can be analysed in a manner to extract knowledge of those parameters. Such analysis is passive, in that it simply collects the side-channel leakage utilizing measurement apparatus which is freely available. Notice that the measurement tool can be adaptively controlled. This kind of extraction and analysis is referred to as non-invasive. Techniques which allow the extraction of CSPs out of this non-invasive leakage is termed an “attack” on the module.

This document focuses on the measurement and analysis of side-channel information. Side-channel non-invasive test tools can be automated to collect such leakage. To characterize the quality of the test tools, metrics are needed, such as signal-to-noise ratio (S/N) (described in ISO/IEC 20085-2). ISO/IEC 20085 (all parts) addresses the measurement and analysis techniques. Those are automated in a test tool. The functionality and the operation of a test tool are described in ISO/IEC 20085 (all parts).

IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules —

Part 1:
Test tools and techniques

1 Scope

This document provides specifications for non-invasive attack test tools and provides information about how to operate such tools. The purpose of the test tools is the collection of signals (i.e. side-channel leakage) and their analysis as a non-invasive attack on a cryptographic module implementation under test (IUT).

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 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this document, the terms and definitions given ISO/IEC 19790 and the following apply.

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

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3.1
advanced side-channel analysis
ASCA
advanced exploitation of the fact that the instantaneous side-channels emitted by a cryptographic device depends on the data it processes and on the operation it performs to retrieve secret parameters

Note 1 to entry: Not to be confused with algebraic side-channel analysis (SCA).

Note 2 to entry: The adjective “advanced”, opposed to “simple”, qualifies side-channel analyses which require multiple side-channel measurements (see 6.2).

[SOURCE: ISO/IEC 17825:2016, 3.1, modified — Notes to entry have been added.]

3.2
analysis tool
test tool component with the ability to control the measurement process, read the recorded measurements, perform post-processing of the recorded measurements, and identify any valid attacks

3.3
application-specific tool
tool dedicated to the measurements and analyses required by ISO/IEC 20085 (all parts)

Note 1 to entry: Antonym of laboratory-assembled tool.

3.4
batch measurement
measurement that includes signals related to repeated execution of one cryptographic operation with a single or with different inputs

Note 1 to entry: See Figure A.1.

3.5
cartography
procedure involving placing a sensor at various positions and taking measurements at each of them to create a spatial (or visual) representation of some data

Note 1 to entry: See A.8.

3.6
horizontal attack
HA
modus operandi where sensitive information is extracted from a single measurement split into several parts

Note 1 to entry: The single measurement can be an averaged measurement obtained from a batch of measurements where repeated operations are conducted with the same cryptographic inputs.

[SOURCE: ISO/IEC 17825:2016, 3.8, modified — Note to entry has been added.]

3.7
implementation under test
IUT
implementation which is tested based on methods specified in ISO/IEC 17825:2016

[SOURCE: ISO/IEC 17825:2016, 3.9, modified — The words “in this International Standard” have been replaced with “in ISO/IEC 17825:2016”.]

3.8
laboratory assembled tool
tool made by assembly of commercial off-the-shelf (COTS) products

Note 1 to entry: Antonym of *application-specific tool* (3.3).

3.9
measurement tool
test tool component with the ability to measure signals in digital format (scalar or vector), time-synchronized with a trigger signal, and that records permanently or transiently the measurements for subsequent analysis

3.10
multivariate trace
trace made up of several samples

EXAMPLE The measurement of an electromagnetic field over time is a multivariate trace.

Note 1 to entry: Usually, a “trace” is considered multivariate.

3.11
non-invasive attack
attack that can be performed on a cryptographic module without direct physical contact with components within the cryptographic boundary of the module

Note 1 to entry: An attack that does not alter or change the state of the cryptographic module.

[SOURCE: ISO/IEC 19790:2012, 3.78]

3.12
signal-to-noise ratio
S/N
measure that compares the level of a desired signal to the level of background noise

Note 1 to entry: It is defined as the ratio of signal power to the noise power.

[SOURCE: ISO/IEC 27033-6:2016, 3.8, modified — The abbreviated term has been added.]

3.13
univariate trace
trace made up of one sample

EXAMPLE A measurement of duration is a univariate trace.

3.14
vertical attack
VA
modus operandi where sensitive information is extracted from different algorithm executions

Note 1 to entry: If the algorithms executions are the same, then the traces can be averaged in a view to increase their *signal-to-noise ratio* (3.12), and then a *horizontal attack* (3.6) can be carried out.

Note 2 to entry: The definition is equivalent to: "Modus operandi where sensitive information is extracted from measurements of repeated execution of one cryptographic operation with different inputs".

[SOURCE: ISO/IEC 17825:2016, 3.17, modified — Notes to entry have been added.]

4 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 19790 and the following apply.

API Application Programming Interface

COTS Commercial Off-The-Shelf

CSP Critical Security Parameter

SPA Simple Power Analysis

5 Test tools

5.1 General

ISO/IEC 20085 (all parts) relates to ISO/IEC 17825:2016, which specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790 for Security Levels 3 and 4. The test metrics are associated with the security functions specified in ISO/IEC 19790.

This document also relates to ISO/IEC 20085-2, which details how the test tool shall be calibrated, to adjust to the requirements (threshold values, for Security Levels 3 and 4) of ISO/IEC 17825.

5.2 Types of side-channels

5.2.1 General

ISO/IEC 17825:2016, Clause 6, specifies three types of side-channels concerned with non-invasive attacks, namely:

a) the power consumption of the IUT,

b) the electromagnetic emissions of the IUT, and

c) the computation time of the IUT.

These side-channels are represented in Figure 1, and are addressed in the Introduction, 5.2.2, 5.2.3 and 5.2.4. These side-channels are measured passively insofar as the IUT behaviour is not disturbed by the measurement tool.

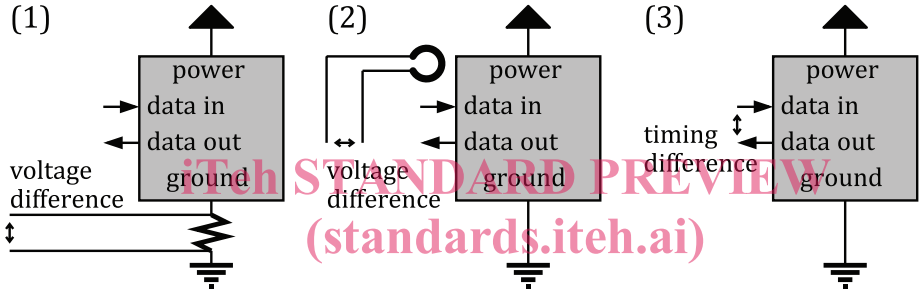

Figure 1 — Three types of side-channels

Other types of side-channels are emerging (see ISO/IEC 17825:2016, B.6).

5.2.2 Power consumption

The power side-channel can be measured by various means. Power measurements are typically measured as a voltage difference.

5.2.3 Electromagnetic emissions

The measurement is indicated by a voltage difference measured by an antenna. Therefore, the measurement can be carried out remotely, and without contact with the cryptographic module.

5.2.4 Computation time

The measurement is indicated by a difference of timing for the selected cryptographic operation, obtained as the subtraction of times corresponding to the cryptographic resources to triggers (*start* and *end*).

5.3 Categorization of test tool

Test tools can be broadly categorized in two types: "Laboratory Assembled", and "Application Specific".

— For Laboratory Assembled tools the non-invasive attack test tool is assembled from two or more commercial off-the-shelf (COTS) products, each of which can have another purpose in the laboratory.

— Application Specific tools, which can also be available as COTS products are dedicated to the measurements and requirements of ISO/IEC 20085 (all parts). They cannot be used for other laboratory testing tasks.

NOTE A test tool is not necessarily a crafted tool. It can be built from parts of equipment used in other contexts.

5.4 Test tool components

5.4.1 General

A test tool is made up of two components: a measurement tool and an analysis tool. Their requirements are detailed in this subclause.

5.4.2 Measurement tool

Measurement tools are required to collect the side-channel emanations from the IUT. There shall be at least two measures: time (horizontal side-channel) and voltage/electromagnetic field (vertical side-channel).

The measurement tools can be two distinct tools i.e. a timer and a digitizer. Both functions can be presented by a single tool (e.g. an oscilloscope), which is able to measure vertical quantities as well as timing as a "function" feature. Such a setup can perform all the tests found in ISO/IEC 20085 (all parts) serially without the need for hardware setup reconfiguration. The single-tool solution is recommended as more convenient for the tester and supports accuracy since the experimental conditions are maintained unchanged during the whole test procedure.

Such measurement tool shall reflect the internal operations carried out within the IUT. For instance, the horizontal side-channel shall relate to the number of required computations, while the vertical side-channel shall show up when a critical security parameter (CSP) is used. In this second case, the CSP can directly influence the vertical side-channel or indirectly, e.g. because it is mixed with parts of the plaintext/ciphertext (assuming the operation is a symmetrical encryption).

Horizontal side-channel can be measured as the duration between a request and a response. However, unpredictable latency can decrease the S/N of such measurement. A more accurate option consists in the derivation of the operation duration from a vertical side-channel trace. In this case, the actual duration can be measured[5]. The sensor involved is a timer. The test requirements listed in ISO/IEC 17825 demand a resolution less than or equal to the clock frequency of the cryptographic module making up or embedded in the IUT.

Vertical side-channel can be measured either globally or locally. Global vertical side-channel measurement consists in the acquisition of an aggregate quantity, e.g. the total power consumption of the whole IUT. This method is well suited for single-chip modules. Local vertical side-channel measurement consists in using a sensor smaller than the IUT, which is placed at various locations around or inside the IUT, where the S/N is stronger. This procedure is referred to as a cartography (see details in A.8). It is a preferred method for the localization of the leakiest position in the case the IUT is a multi-chip module. The sensor shall be able to probe leaked information without tampering with the IUT.

Examples of such sensors are:

— an antenna (microscopic, mesoscopic or macroscopic) which measures the electromagnetic field emitted by the IUT;

— a current probe placed on the communication or power cables of the IUT can measure leakage outside the boundary of the IUT[6].

An illustration of horizontal versus vertical attacks, and univariate traces versus multivariate traces, is given in Figure 2.