International Standard

ISO/IEC 17825

Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

Technologie de l'information — Techniques de sécurité — Méthodes de test pour la protection contre les attaques non intrusives des modules cryptographiques

Second edition
2024-01

Reference number
ISO/IEC 17825:2024(en)

© ISO/IEC 2024



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2024

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **3**
5 Document organization ... **4**
6 Non-invasive attack methods ... **4**
7 Non-invasive attack test methods ... **7**
7.1 General ... 7
7.2 Test strategy ... 7
7.3 Side-channel analysis workflow ... 8
7.3.1 Core test flow ... 8
7.3.2 Side-channel resistance test framework ... 8
7.3.3 Required vendor information ... 9
7.3.4 TA leakage analysis ... 10
7.3.5 SPA/SEMA leakage analysis ... 11
7.3.6 DPA/DEMA leakage analysis ... 12
8 Side-channel analysis of symmetric-key cryptosystems ... **13**
8.1 General ... 13
8.2 Timing attacks ... 13
8.3 SPA/SEMA ... 13
8.3.1 Attacks on key derivation process ... 13
8.3.2 Side-channel collision attacks ... 14
8.4 DPA/DEMA ... 14
9 ASCA on asymmetric cryptography ... **16**
9.1 General ... 16
9.2 Detailed side-channel resistance test framework ... 17
9.3 Timing attacks ... 18
9.3.1 General ... 18
9.3.2 Standard timing analysis ... 18
9.3.3 Micro-architectural timing analysis ... 19
9.4 SPA/SEMA ... 19
9.5 DPA/DEMA ... 19
Annex A (normative) **Non-invasive attack mitigation pass/fail test metrics** ... **21**
Annex B (informative) **Requirements for measurement apparatus** ... **24**
Annex C (informative) **Associated security functions** ... **25**
Annex D (informative) **Emerging attacks** ... **27**
Annex E (informative) **Quality criteria for measurement setups** ... **30**
Annex F (informative) **Chosen-input method to accelerate leakage analysis** ... **32**
Annex G (informative) **Reasons that a side-channel is assessed as not measurable** ... **33**
Annex H (informative) **Information about leakage location in relation to algorithm time** ... **34**
Bibliography ... **35**

© ISO/IEC 2024 – 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.

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 or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

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. In the IEC, see www.iec.ch/understanding-standards.

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

This second edition cancels and replaces the first edition (ISO/IEC 17825:2016), which has been technically revised.

The main changes are as follows:

— test methods have been updated as per research trends;

— an introduction has been added which states the expectations in terms of security level of this document;

— requirements have been numbered to ensure their traceability.

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 and www.iec.ch/national-committees.

© ISO/IEC 2024 – All rights reserved

Introduction

Testing requires defined constants, which are derived from an axiomatic analysis of the security problem. The security assurance levels are bound to the testing and remaining risks. The testing approach can be characterized as follows:

a) Testing soundness

   1) A formal description of empirical closed-box testing provides the soundness, in the context of the attack, because the testing adheres to an accepted methodology.

   2) The application of the methodology does not ensure that all possible attacks are covered. Testing allows for weakness detection in a system; hence, it increases the confidence in a system's ability to withstand a set of simulated attacks. The implemented formalism allows to detect weaknesses, and the outcome is a reasonable level attested by tests.

   3) The level of assurance that can be reached with the methodology in this document is a "controlled" level of "reasonable" confidence level, which is the level low to medium. Level high is not reachable due to the closed-box approach. The meaning of "reasonable" is determined by the customer's risk threshold. The tester is defining the level of reasonability, in accordance with a security level target.

   4) Testing is guided by a strategy, which allows for transparency in the methodology and outcomes.

   5) The methodology is device-class specific. The pass/fail criteria should take into account the class of devices under test. For example, the criteria for devices with a deterministic behaviour (i.e. bare metal), and for devices with a complex software stack should be different.

   6) Security testing is an "estimation" when based upon noisy measurements, or when the tester does not have full control of the implementation under test (IUT).

b) Repeatability (as per ISO/IEC 17025:2017, 7.2.2.4)

   Repeatability means similar results from the same (i.e. repeated) methodology, while reproducibility means similar results from similar methodology. Security evaluation is an estimation based on noisy measurements, on IUT whose behaviour is probably not in full control of the tester. In this document, there is a prerequisite that the IUT is closed-box, which can behave in a non-deterministic manner (at least, its internals – owing to some intentional randomization used as a protection). Furthermore, the test can only be carried out based on external observations and findings. As a result, the objective is to document a formal and transparent process of testing, where independent tests can be reproduced with similar expected results (as much as possible, within reasonable bounds). The methodologies are similar (e.g. executed by two testers) in that they yield similar outcome.

c) Cost of testing

   1) The objective is to devote the right amount of effort for the testing of a given assurance level. Cost effectiveness of the testing has a direct implication on assuring a certain level of security. Cost of testing includes, but is not limited to:

      i) Level of expertise and experience: Consequence/implication of using an already formalized process (agnostic in the IUT). The testers require skills and competencies.

      ii) Time: Elapsed time for data acquisition, even though the procedure is automated.

      iii) Equipment: The cost impact of equipment is covered in ISO/IEC 20085-1:2019 (requirements) and ISO/IEC 20085-2:2020 (calibration).

   2) This document aims to keep cost moderate. A threshold is reached in the assurance level up to a certain number of traces captured. The level of assurance does not increase significantly more beyond the threshold. The prescribed methodology cannot exceed a certain level of assurance by its design.

© ISO/IEC 2024 – All rights reserved

The following statements apply as an artefact of the methodology used:

d) Closed-box testing limits this methodology to exclusively test for leakage that does not account for specific features of a given algorithm's implementation (e.g. implementation specificities, such as parallel execution of unrelated cryptographic operations, or countermeasures, such as random masking, implementation of field arithmetic in elliptic curve cryptography).

e) Testing only considers leakage during tested cryptographic operations using keys. By design the process does not look for other potential sources of leakage (e.g. emissions during transit of keys over internal bus).

f) Results are dependent on the data sets and quality of equipment used during acquisition. Attackers with larger resources can still exploit attack paths tested by this methodology, even if they had passed the test based on increased resources and effort.

g) More sophisticated attacks can be applied and succeed. More sophisticated attacks refer to attacks other than conventional ones, for example the attacks that are particular to asymmetric ciphers (see 9.2).

h) Each specific application/cryptographic module API instance also requires a delta evaluation on top of the generic tests in this document. Such areas of assessment should include application-specific non-parametric module usage threats, such as traffic analysis, manipulation of logical order or scope of external operations.

In this document, requirements are numbered. By convention, the requirements are labelled as [CC.NN], where CC represents the clause number (e.g. 06 means Clause 6), and NN represents the requirement position within the Clause (e.g. the first requirement of Claude 6 is referred to as [06.01]). The purpose of labelled requirements is to ease the generation of documents showing compliance with this document, and their traceability for testers.

© ISO/IEC 2024 – All rights reserved

Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

1 Scope

This document specifies the non-invasive attack mitigation test metrics for determining conformance to the requirements specified in ISO/IEC 19790:2012 for security levels 3 and 4. The test metrics are associated with the security functions addressed in ISO/IEC 19790:2012. Testing is conducted at the defined boundary of the cryptographic module and the inputs/outputs available at its defined boundary.

This document is intended to be used in conjunction with ISO/IEC 24759:2017 to demonstrate conformance to ISO/IEC 19790:2012.

NOTE ISO/IEC 24759:2017 specifies the test methods used by testing laboratories to assess whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012 and the test metrics specified in this document for each of the associated security functions addressed in ISO/IEC 19790:2012.

The test approach employed in this document is an efficient "push-button" approach, i.e. the tests are technically sound, repeatable and have moderate costs.

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*

ISO/IEC 24759:2017, *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 the following apply.

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

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

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

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

3.2
correlation power analysis
CPA
analysis where the correlation coefficient is used as the statistical method

© ISO/IEC 2024 – All rights reserved