INTERNATIONAL ISO/IEC

First edition
2020-03

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

Part 2: Test calibration methods and apparatus

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 2: Méthodes et appareillage d'étalonnage et d'essai

Reference number
ISO/IEC 20085-2:2020(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

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.

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.

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.

Introduction

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

Non-invasive attack testing is a method to determine whether the leakage of a cryptographic module can be exploited to extract critical security parameters. A non-invasive attack test tool returns a pass status if the cryptographic module leakage is determined to be of a minimal amount which may prevent disclosure of critical security parameters. Otherwise, it returns a fail status.

This document focuses on the calibration of the side-channel measurement tool. This calibration process enables two measurement tools to record measurements equally usable in terms of side channel analysis. Calibration is presented as the combination of two techniques:

a) definition of a method for calibration;

b) requirement of a reference cryptographic module (called an artefact) to define a clear threshold between test results, in terms of fail or pass.

Both aspects are covered in this document.