TECHNICAL REPORT

ISO/IEC TR 24485

First edition
2022-10

Information security, cybersecurity and privacy protection — Security techniques — Security properties and best practices for test and evaluation of white box cryptography

Sécurité de l'information, cybersécurité et protection de la vie privée — Techniques de sécurité — Propriétés de sécurité et bonnes pratiques pour les essais et l'évaluation de la cryptographie en boîte blanche

Reference number
ISO/IEC TR 24485:2022(E)

© ISO/IEC 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

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

© ISO/IEC 2022 – All rights reserved

Contents

Page

Foreword ..... **v**

Introduction ..... **vi**

1 Scope **1**

2 Normative references **1**

3 Terms and definitions **1**

4 Security properties of white box cryptography **2**
4.1 Implementation of a white box cryptography 2
4.1.1 General 2
4.1.2 Description of a WBC 2
4.1.3 Adherence between WBC code and the device hosting it 3
4.2 WBC attack path(s) 3
4.2.1 General 3
4.2.2 De-embedding of code (code lifting) 3
4.2.3 Device analysis 4
4.2.4 Code analysis 4
4.3 WBC usages 4
4.3.1 General 4
4.3.2 Symmetric encryption 5
4.3.3 Asymmetric encryption / signature 5
4.3.4 Keyed hash function 5
4.3.5 Customized cryptographic algorithm 5
4.4 Security properties 5
4.4.1 General 5
4.4.2 Secrecy of the key 5
4.4.3 Difficulty to attack diversified instance 6
4.4.4 Difficulty to lift the code 6
4.4.5 Difficulty to reverse-engineer the binary / obfuscation code 6

5 Best practices for WBC **7**
5.1 Tests condition 7
5.1.1 General 7
5.1.2 WBC under source code version 7
5.1.3 WBC under compiled code version 7
5.1.4 Best practices for testing 7
5.2 Security tests 7
5.2.1 General 7
5.2.2 Testing the key secrecy 7
5.2.3 Testing the difficulty to attack diversified instances 7
5.2.4 Testing the difficulty to lift the code 8
5.2.5 Testing the difficulty to reverse-engineer the binary / obfuscation code 8

6 Best practices for WBC **8**
6.1 General 8
6.2 Core analyses 8
6.2.1 General 8
6.2.2 Cryptanalytic analysis of tables 8
6.2.3 Side-channel analysis on WBC 8
6.2.4 Fault injection analysis on WBC 9
6.2.5 Evaluation involving combined techniques 9
6.3 Analysis aiming at circumventing access to the plain WBC protection 9
6.3.1 General 9
6.3.2 Reverse-engineering of the binary code 9
6.3.3 Space hardness evaluation 9

Annex A (informative) **Design of white-boxing-friendly cryptographic algorithms** **10**

© ISO/IEC 2022 – All rights reserved

Bibliography **11**

© ISO/IEC 2022 – 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).

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

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

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 2022 – All rights reserved

Introduction

The white box cryptography (WBC) is a specific implementation method for cryptographic algorithms where the secret key and the algorithm are entangled, so that the user can freely stimulate the latter. However, the secret key is deeply engraved in the implementation, such that it is hard to extract and is unambiguous. Furthermore, it is also difficult to update the WBC implementation in order to change the key.

WBC is typically used for implementation when secure cryptographic module functionality (such as a tamper-resistance device or a physically unclonable function) is unavailable for the protection of secrets.

Business cases include DRM (digital right management) and HCE (host card emulation), in the contexts of media protection and payment applications. WBC implementations are widely deployed on mobile devices, where the cryptographic implementation is provided over the top.

The purpose of this document is to provide best practices on security assurance and to facilitate users to assess the security level of several WBC implementations. It is important to share common information and best practices about test and evaluation of WBC security.

© ISO/IEC 2022 – All rights reserved

Information security, cybersecurity and privacy protection — Security techniques — Security properties and best practices for test and evaluation of white box cryptography

1 Scope

This document introduces security properties and provides best practices on the test and evaluation of white box cryptography (WBC). WBC is a cryptographic algorithm specialized for a key or secret, but where the said key cannot be extracted.

The WBC implementation can consist of plain source code for the cryptographic algorithm and/or of a device implementing the algorithm. In both cases, security functions are implemented to deter an attacker from uncovering the key or secret.

Security properties consist in the secrecy of security parameters concealed within the implementation of the white box cryptography. Best practices for the test and evaluation includes mathematical and practical analyses, static and dynamic analyses, non-invasive and invasive analyses.

This document is related to ISO/IEC 19790 which specifies security requirements for cryptographic modules. In those modules, critical security parameters (CSPs) and public security parameters (PSPs) are the assets to protect. WBC is one solution to conceal CSPs inside of the implementation.

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, *Information technology — Security techniques — Security 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
white box cryptography
WBC
physically unprotected cryptographic software implementation aimed at mitigating the risk of extracting secrets obfuscated within the implementation

3.2
white-boxing generator
program which dynamically generates a new *white box cryptography* (3.1) instance

© ISO/IEC 2022 – All rights reserved

3.3
disembedding
extracting software binary code from its intended platform in a malicious way to transfer it to a separate platform amenable to analysis

4 Security properties of white box cryptography

4.1 Implementation of a white box cryptography

4.1.1 General

A white box cryptography (WBC) implementation is a software code implementing a cryptographic function. The implementation can be varied, to match constraints in terms of performance (code size, execution duration, power or energy consumption, etc.), usability (portability, description language, etc.) and of security.

4.1.2 Description of a WBC

A WBC implementation can be available in different forms including:

a) Source code or compiled code (e.g. binary code).

b) Plain or intentionally obfuscated code.

c) Standalone code with an API (application programming interface) to a software cryptographic library (hence with a clearly defined boundary) or code embedded into an application (hence a difficult task to separate the WBC code from the applicative code).

d) For greatest risk mitigation, typically, a unique WBC instance is deployed for each obfuscated cryptographic operation or key usage for each platform instance. It is indeed common to distribute a unique WBC implementation (corresponding to a unique key) per device. Therefore, there is a need for a program to generate WBC implementations. There are various levels of availability of the WBC code generator (as known as white-boxing generator), including:

    1) It is public. This is either because it has been stolen or leaked by an insider, or because it is used in a trustworthy context where it is paramount that the system be open so as to avoid risks of backdoors; or

    2) Only some aspects are known. This means the design rationale can be public, but be itself configured with some secrets; or

    3) It is completely secret.

The generation of the WBC implementation (displayed as “WBC exe”) from the WBC generator is depicted in Figure 1 showing the two contexts of white-boxing generator; when the attacker knows it and when it does not know it. The “grey” situation, where some aspects are known, can also be envisioned. Depending on the case, the analysis strategy can differ. The input/output correspond to the user interface of the crypto-algorithm except the secret key, for example:

a) If the application is a block-cipher input is Plaintext and output is Ciphertext

b) If the application is a digital-signature input is the message to be signed and output is the signature

c) If the application is a Message Authentication Code, input is the message to be authenticated and output is the authentication tag

© ISO/IEC 2022 – All rights reserved