TECHNICAL SPECIFICATION

ISO/IEC TS 19249

First edition
2017-10

Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications

Technologies de l'information — Techniques de sécurité — Catalogue des principes architecturaux et conceptuels pour la sécurisation des produits, systèmes et applications

Reference number
ISO/IEC TS 19249:2017(E)

© ISO/IEC 2017



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2017, Published in Switzerland

All rights reserved. Unless otherwise specified, 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
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 ..... **v**
Introduction ..... **vi**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Architectural principles for secure products, systems and applications **2**
4.1 General 2
4.2 Domain separation 3
4.2.1 General 3
4.2.2 Principles for defining domain structures 3
4.2.3 Principles for defining inter-domain communication 3
4.2.4 Security policies that may be enforced using domain separation 4
4.2.5 Examples 4
4.2.6 Considerations for evaluation 4
4.3 Layering 5
4.3.1 General 5
4.3.2 Principles for defining layers 5
4.3.3 Principles for Interfaces exposed by a layer 5
4.3.4 Security policies that may be enforced using layering 5
4.3.5 Examples 6
4.3.6 Considerations for evaluation 6
4.4 Encapsulation 6
4.4.1 General 6
4.4.2 Principles for defining encapsulation 7
4.4.3 Security policies that may be enforced using encapsulation 7
4.4.4 Examples 7
4.4.5 Considerations for evaluation 7
4.5 Redundancy 7
4.5.1 General 7
4.5.2 Principles for defining redundant elements 8
4.5.3 Principles for keeping consistency between redundant elements 8
4.5.4 Security policies that may be enforced using redundancy 8
4.5.5 Examples 8
4.5.6 Considerations for evaluation 9
4.6 Virtualization 10
4.6.1 General 10
4.6.2 Principles for defining virtualization 10
4.6.3 Security policies that may be enforced using virtualization 10
4.6.4 Examples 11
4.6.5 Considerations for evaluation 11
5 Design principles **11**
5.1 General 11
5.2 List of design principles for security 12
5.2.1 Least privilege 12
5.2.2 Attack surface minimization 13
5.2.3 Centralized parameter validation 15
5.2.4 Centralized general security services 17
5.2.5 Preparing for error and exception handling 18
5.3 Using the design principles when designing a secure system or application 20
5.3.1 General 20
5.3.2 Least privilege 20
5.3.3 Attack surface minimization 20

© ISO/IEC 2017 – All rights reserved

5.3.4 Centralized parameter validation 20
5.3.5 Centralized security services 20
5.3.6 Preparing for error and exception handling 21

6 Evaluation activities for the architectural principles 21
6.1 General 21
6.2 Domain separation 22
6.3 Layering 23
6.4 Encapsulation 23
6.5 Redundancy 24
6.6 Virtualization 25

Bibliography 26

 © ISO/IEC 2017 – 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. 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 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

© ISO/IEC 2017 – All rights reserved

Introduction

This document describes architectural and design principles that may be used in the development of secure products, systems and applications.

Each principle is described in a structured way, characterizing the principle itself, describing how it can be used, how it can support security, how it may help in the security assessment of the product, system or application, as well as its dependency on other principles described in this document.

Examples are provided for each principle on how it may be implemented, how it may contribute to security properties and functions and what other aspects have to be taken into account in the example provided to also address non-security related requirements like usability and performance.

A guideline is provided linking this to security evaluations performed using ISO/IEC 15408 (all parts) and ISO/IEC 18045 and addresses both developers and evaluators of secure products, systems and applications.

© ISO/IEC 2017 – All rights reserved

Information technology — Security techniques — Catalogue of architectural and design principles for secure products, systems and applications

1 Scope

This document provides a catalogue of architectural and design principles that can be used in the development of secure products, systems and applications together with guidance on how to use those principles effectively.

This document gives guidelines for the development of secure products, systems and applications including a more effective assessment with respect to the security properties they are supposed to implement.

This document does not establish any requirements for the evaluation or the assessment process or 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 15408-1, *Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*

ISO/IEC 15408-2, *Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional components*

ISO/IEC 15408-3, *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components*

ISO/IEC 18045, *Information technology — Security techniques — Methodology for IT security evaluation*

3 Terms and definitions

For the purposes of this document, terms and definitions given in ISO/IEC 15408-1, ISO/IEC 15408-2, ISO/IEC 15408-3 and ISO/IEC 18045 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
security property
property of a system or application that is crucial to achieve the security objectives defined for the system or application

3.2
security relevant attribute
attribute assigned to an object, subject or user of a system or application that is used to enforce a security policy

© ISO/IEC 2017 – All rights reserved

3.3
privilege
specific security relevant attribute for a subject or user that allows that user or subject to perform dedicated activities bound to that security relevant attribute

3.4
transparent encryption service
service provided by the system that is either always on or that can be switched on by an administrator which automatically encrypts and decrypts data on persistent storage or on communication links and where the user that stores or transmits data is not aware that this encryption service is performed

EXAMPLE Automatic disk encryption services (like self-encrypting disks); tunnelling a communication link through an IPSec or TLS protected communication link.

4 Architectural principles for secure products, systems and applications

4.1 General

Building a secure product, system or application requires not only the implementation of functional requirements but also an architecture that allows for the effective enforcement of specific security properties the product, system or application is supposed to enforce. The ability to withstand attacks the product, system or application may face in its intended operational environment is highly dependent on an architecture that prohibits those attacks or – if they cannot be prohibited – allows for detection of such attacks and/or limitation of the damage such an attack can cause. Structuring the product, system or application into dedicated domains that are isolated from each other and can only communicate using well defined communication paths where specific security policies can be enforced is a generic architectural principle that can be applied. The architectural structure imposed by such domains has to be carefully selected to support the enforcement of security properties and requirements but also assist in the implementation of non-security related requirements. Such a structure should also not cause unacceptable degradation of the performance of the product, system or application. Finding the right balance in the architectural structure that supports all requirements for a product, system or application is the main topic the architectural principles defined in this clause can be used in co-operation with the related design principles.

There are a few fundamental principles for security that need to be observed regardless of any architecture or design principle. Those have been known for a long time and were first documented in a study performed on behalf of the US Government in 1972.[1] Those fundamental principles are:

— the implementation of security functions needs to be such that those functions cannot be bypassed or tampered with by untrusted code;

— the security functions need to be always invoked when required to enforce the security policy;

— the part that implements the security functionality need to be small enough to be analysed for correctness and potential security critical side effects.

In a later report [2], the parts of a product that need to be trusted for enforcing the security policy and that satisfy the security principles above was called the "Trusted Computing Base" or TCB.

A number of design principles discussed in this document were previously introduced in [3] in 1974. Since then, IT products and systems have significantly grown in complexity and are now often distributed, rely on external service providers, and cover a wider spectrum of security functionality. This requires more complex architectures and designs and this document provides a description of architectural and design principles with their security-related aspects.

 © ISO/IEC 2017 – All rights reserved