ICS 35.040

L 80

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

中华人民共和国国家标准

GB/T 18336.2-2015/ISO/IEC 15408-2: 2008

Replace GB/T 18336.2-2008

Information technology—Security techniques—Evaluation criteria for IT security—Part 2: Security functional components

信息技术 安全技术 信息技术安全评估准则

第 2 部分：安全功能组件

(ISO/IEC 15408-2: 2008, IDT)

Issued on May 15, 2015 Implemented on January 01, 2016

Issued by General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China

Standardization Administration of the People's Republic of China

Contents

Foreword

GB/T 18336 “Information technology--Security techniques--Evaluation criteria for IT security” includes the following 3 parts:

— part 1: Introduction and general model;

— part 2: Security functional components;

— part 3: Security assurance components.

This part is part 2 of GB/T 18336.

This part is drafted in accordance with specifications in GB/T1.1-2009.

This part will replace GB/T 18336.2-2008 “Information technology--Security techniques--Evaluation criteria for IT security part 2: Security functional components”.

The main differences between this part and GB/T 18336.2-2008 are as follows:

— “assurance” is replaced by “guarantee”;
— “10.4 Export outside TSF control (FDP_ETC)” is amended as “10.4 Export from TOE (FDP_ETC)”;
— “10.7 Import from outside TSF control(FDP_ITC)” is amended as” 10.7 Import from outside TOE (FDP_ITC)”;
— “14.1 Bottom abstract machine test (FPT_AMT)”, “14.10 Referring to arbitration (FTP_RVM)” and”14.11 Domain separation” in “14 FPT class: TSF protection” are removed ;
— “14.12 Test of external entity(FPT_TEE)” is added in “14 FPT class: TSF protection”;
— "16.3 Session lock (FTA_SSL)" is amended as"16.3 Session lock and termination(FTA_SSL)";
— “threshold value” is replace by “ critical value”;
— “mediate” is replaced by “promote”.

This part is a translation copy and identical to the international standard ISO/IEC 15408-2:2008 “Information technology--Security techniques--Evaluation criteria for IT security part 2:Security functional components”.

The consistent domestic documents corresponding to normative international references in this part are as follows:

— GB/T 18336.1 “Information technology--Security techniques--Evaluation criteria for IT security part1: Introduction and general model”. (GB/T 18336.1-2015, ISO/IEC 15408-1: 2009, IDT)”

This part has the following editorial amendments:

— There is editorial error in the original text of sub-clause 4.1 and now it is amended as “For the relevant structure, regulations and guidelines, personnel responsible for standard drafting PP or ST shall refer to chapter 3 of ISO/IEC 15408-1 and relevant annexes”.

This part is proposed and under jurisdiction of China Information Security Standardization Technical Committee (SAC/TC 260).

The main drafting units of this standard include: China Information Technology Security Evaluation Center, Information Technology Security Test and Evaluation Center, The Third Research Institute of Ministry of Public Security, China Information Technology Security Evaluation Center Jilin Center.

The main drafters of this part include: Zhang Chongbin, Guo Ying, Shi Hongsong, Bi Haiying, Zhang Baofeng, Gao Jinping, Wang Feng, Yang Yongsheng, Li Guojun, Dong Jingjing, Xie Di, Wang Hongxian, Zhang Yi, Gu Jian, Qiu Zihua, Song Haohao, Chen Yan, Yang Yuanyuan, Li Fengjuan, Pangbo, Zhang Xiao, Liu Yuhan, Wang Shuyi, Zhou Boyang, Tang Xiqing, Jiang Xianlan, Zhang Shuangshuang.

The previous editions replaced by this part are as follows:

--GB/T 18336. 2-2001;

--GB/T 18336. 2-2008.

INTRODUCTION

Security functional components, as defined in this part, are the basis for the security functional requirements expressed in a Protection Profile (PP) or a Security Target (ST). These requirements describe the desired security behaviour expected of a Target of Evaluation (TOE) and are intended to meet the security objectives as stated in a PP or an ST. These requirements describe security properties that users can detect by direct interaction (i.e. inputs, outputs) with the IT or by the IT response to stimulus.

Security functional components express security requirements intended to counter threats in the assumed operating environment of the TOE and/or cover any identified organisational security policies and assumptions.

The audience for This part includes consumers, developers, and evaluators of secure IT products. ISO/IEC 15408-1 Clause 5 provides additional information on the target audience of ISO/IEC 15408, and on the use of ISO/IEC 15408 by the groups that comprise the target audience. These groups may use This part as follows:

a) Consumers, who use This part when selecting components to express functional requirements to satisfy the security objectives expressed in a PP or ST. ISO/IEC 15408-1 provides more detailed information on the relationship between security objectives and security requirements.

b) Developers, who respond to actual or perceived consumer security requirements in constructing a TOE, may find a standardised method to understand those requirements in This part. They can also use the contents of this part as a basis for further defining the TOE security functionality and mechanisms that comply with those requirements.

c) Evaluators, who use the functional requirements defined in This part in verifying that the TOE functional requirements expressed in the PP or ST satisfy the IT security objectives and that all dependencies are accounted for and shown to be satisfied. Evaluators also should use This part to assist in determining whether a given TOE satisfies stated requirements.

Information technology—Security techniques—Evaluation criteria for IT security—Part 2: Security functional components

1 Scope

This part of GB/T 18336 defines the required structure and content of security functional components for the purpose of security evaluation. It includes a catalogue of functional components that will meet the common security functionality requirements of many IT products.

2 Normative references

The articles contained in the following documents have become this document when they are quoted herein. For the dated documents so quoted, all the modifications (Including all corrections) or revisions made thereafter shall be applicable to this document.

ISO/IEC 15408-1, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model

3 Terms and definitions

For the purposes of this document, the following terms and definitions given in ISO/IEC 15408-1 apply.

4 Overview

ISO/IEC 15408 and the associated security functional requirements described herein are not meant to be a definitive answer to all the problems of IT security. Rather, this standard offers a set of well understood security functional requirements that can be used to create trusted products reflecting the needs of the market. These security functional requirements are presented as the current state of the art in requirements specification and evaluation.

This part does not presume to include all possible security functional requirements but

rather contains those that are known and agreed to be of value by this part authors at the time of release.

Since the understanding and needs of consumers may change, the functional requirements in This part will need to be maintained. It is envisioned that some PP/ST authors may have security needs not (yet) covered by the functional requirement components in This part. In those cases the PP/ST author may choose to consider using functional requirements not taken from ISO/IEC 15408 (referred to as extensibility), as explained in annexes A and B of ISO/IEC 15408-1.

4.1 Organisation of this part

Clause 5 describes the paradigm used in the security functional requirements of this part.

Clause 6 introduces the catalogue of this part functional components while clauses 7 through 17 describe the functional classes.

Annex A provides explanatory information for potential users of the functional components including a complete cross reference table of the functional component dependencies.

Annex B through Annex M provide the explanatory information for the functional classes. This material must be seen as normative instructions on how to apply relevant operations and select appropriate audit or documentation information; the use of the auxiliary verb should means that the instruction is strongly preferred, but others may be justifiable. Where different options are given, the choice is left to the PP/ST author.

Those who author PPs or STs should refer to clause 2 of ISO/IEC 15408-1 for relevant structures, rules, and guidance:

a) ISO/IEC 15408-1, clause 3 defines the terms used in ISO/IEC 15408.

b) ISO/IEC 15408-1, annex A defines the structure for STs.

c) ISO/IEC 15408-1, annex B defines the structure for PPs.

5 Functional requirements paradigm

This clause describes the paradigm used in the security functional requirements of this

part.

Key concepts discussed are highlighted in bold/italics. This subclause is not intended to replace or supersede any of the terms found in ISO/IEC 15408-1, clause 3.

This part is a catalogue of security functional components that can be specified for a Target of Evaluation (TOE). A TOE is a set of software, firmware and/or hardware possibly accompanied by user and administrator guidance documentation. A TOE may contain resources such as electronic storage media (e.g. main memory, disk space), peripheral devices (e.g. printers), and computing capacity (e.g. CPU time) that can be used for processing and storing information and is the subject of an evaluation.

TOE evaluation is concerned primarily with ensuring that a defined set of security functional requirements (SFRs) is enforced over the TOE resources. The SFRs define the rules by which the TOE governs access to and use of its resources, and thus information and services controlled by the TOE.

The SFRs may define multiple Security Function Policies (SFPs) to represent the rules that the TOE must enforce. Each such SFP must specify its scope of control, by defining the subjects, objects, resources or information, and operations to which it applies. All SFPs are implemented by the TSF (see below), whose mechanisms enforce the rules defined in the SFRs and provide necessary capabilities.

Those portions of a TOE that must be relied on for the correct enforcement of the SFRs are collectively referred to as the TOE Security Functionality (TSF). The TSF consists of all hardware, software, and firmware of a TOE that is either directly or indirectly relied upon for security enforcement.

The TOE may be a monolithic product containing hardware, firmware, and software.

Alternatively a TOE may be a distributed product that consists internally of multiple separated parts. Each of these parts of the TOE provides a particular service for the TOE, and is connected to the other parts of the TOE through an internal communication channel. This channel can be as small as a processor bus, or may encompass a network internal to

北京文心雕语翻译有限公司
Beijing Lancarver Translation Inc.

完整版本请在线下单/Order Checks Online for Full version

联系我们/or Contact:

TEL: 400-678-1309

QQ: 19315219 | Skype: Lancarver

Email：info@lancarver.com

http://www.lancarver.com

线下付款方式：

I. 对公账户：

单位名称：北京文心雕语翻译有限公司

开 户 行：中国工商银行北京学清路支行

账　　号：0200 1486 0900 0006 131

II. 支付宝账户：info@lancarver.com

III. Paypal: info@lancarver.com

注: 付款成功后，请预留电邮，完整版本将在一个工作日内通过电子 PDF 或 Word 形式发送至您的预留邮箱，如需索取发票，下单成功后的三个工作日内安排开具并寄出，预祝合作愉快！

NOTE All documents on the store are in electronic Adobe Acrobat PDF format, there is not sell or ship documents in hard copy. Mail the order and payment information to info@lancarver.com , you will shortly receive an e-mail confirming your order.