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 18336.1-2015/ISO/IEC 15408-1: 2009

Replace GB/T 18336.1-2008

Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model

信息技术 安全技术 信息技术安全评估准则

第 1 部分：简介和一般模型

(ISO/IEC 15408-1: 2009, 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 1 of GB/T 18336.

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

This part will replace GB/T 18336.1-2008 “Information technology--Security techniques--Evaluation criteria for IT security part 1: Introduction and general model”.

The main differences between this part and GB/T 18336.1-2008 are as follows:

--“2 Normative references” are added;

--In “3 Terms and definitions”, “3.2 Terms and definitions concerning development (ADV) class”, “3.3 Terms and definitions concerning guidance documentation (AGD) class”, “3.4 Terms and definitions concerning life cycle support(ALC) class”, “Terms and definitions concerning vulnerability assessment (AVA) class” and “3.6 Terms and definitions concerning combination (ACO) class” are added;

--In “ 5 Introduction”, “5.2 TOE” is added;

--The "IT product and system" to which GB/T 18336 is applicable is amended as "IT product";

--"5.1 Elements concerning security" and " 5.2 Assurance method" are amended as" 6.2 Asset and countermeasures" and "6.3 Evaluation" in this part;

--“5.3 Security concepts” in GB/T 18336.1-2008 is removed;

--“5.4.1 Expression of security requirements” is reedited as “7 Clipping security requirements” in this part;

--“5.4.2 Evaluation types” in GB/T 18336.1-2008 is removed;

--“8 Protection profile and package” is added;

--“6 GB/T 18336 Requirements and evaluation results” is reedited as “9 Evaluation results” in this part;

--“Annex A Protection profile specification” is reedited as “Annex B Protection profile specification" in this part while “B.11 Protection profile of low level assurance” and “B.12 Referring to other standards in PP”;

--“Annex B Specification of security target” is reedited as “Annex A Specification of security target” in this part and “ A.3 Using ST”, “ A.11 Problems solved by ST”, “A.12 Security target of low level assurance” and “A.13 Referring to other standards in ST” are added.

This part is a translation copy and identical to the international standard ISO/IEC 15408-1: 2008 “Information technology--Security techniques--Evaluation criteria for IT security part1: Introduction and general mode”.

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

--GB/T 18336.2 –2015 “Information technology--Security techniques--Evaluation criteria for IT security Part 2: Security functional components (ISO/IEC 15408-2:2008,IDT)”

--GB/T 18336.3-2015 "Information technology--Security techniques--Evaluation criteria for IT security Part 3: Security assurance components (ISO/IEC 15408-3:2008,IDT)”

GB/T 30270 “Information technology-Security technology-Methodology for IT security evaluation(GB/T 30270-2013, ISO/IEC 18045:2005,IDT)

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.

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, Jia Wei, Wang Yuhang, Wang Yanan.

The previous editions replaced by this part are as follows:

--GB/T 18336.1-2001;

--GB/T 18336.1-2008.

INTRODUCTION

This part of ISO/IEC 15408 permits comparability between the results of independent security evaluations. ISO/IEC 15408 does so by providing a common set of requirements for the security functionality of IT products and for assurance measures applied to these IT products during a security evaluation. These IT products may be implemented in hardware, firmware or software.

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

ISO/IEC 15408 is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

ISO/IEC 15408 is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore users of this International Standard are cautioned to exercise care that this flexibility is not misused. For example, using ISO/IEC 15408 in conjunction with unsuitable evaluation methods, irrelevant security properties, or inappropriate IT products, may result in meaningless evaluation results.

Consequently, the fact that an IT product has been evaluated has meaning only in the context of the security properties that were evaluated and the evaluation methods that were used. Evaluation authorities are advised to carefully check the products, properties and methods to determine that an evaluation will provide meaningful results. Additionally, purchasers of evaluated products are advised to carefully consider this context to determine whether the evaluated product is useful and applicable to their specific situation and needs.

ISO/IEC 15408 addresses protection of assets from unauthorised disclosure, modification, or loss of use. The categories of protection relating to these three types of failure of security are commonly called confidentiality, integrity, and availability, respectively.

ISO/IEC 15408 may also be applicable to aspects of IT security outside of these three. ISO/IEC 15408 is applicable to risks arising from human activities (malicious or otherwise) and to risks arising from non-human activities. Apart from IT security, ISO/IEC 15408 may be applied in other areas of IT, but makes no claim of applicability in these areas.

Certain topics, because they involve specialized techniques or because they are somewhat peripheral to IT security, are considered to be outside the scope of ISO/IEC 15408. Some of these are identified below.

a) ISO/IEC 15408 does not contain security evaluation criteria pertaining to administrative security measures not related directly to the IT security functionality. However, it is recognised that significant security can often be achieved through or supported by administrative measures such as organizational, personnel, physical, and procedural controls.

b) The evaluation of some technical physical aspects of IT security such as electromagnetic emanation control is not specifically covered, although many of the concepts addressed will be applicable to that area.

c) ISO/IEC 15408 does not address the evaluation methodology under which the criteria should be applied. This methodology is given in ISO/IEC 18045.

d) ISO/IEC 15408 does not address the administrative and legal framework under which the criteria may be applied by evaluation authorities. However, it is expected that ISO/IEC 15408 will be used for evaluation purposes in the context of such a framework.

e) The procedures for use of evaluation results in accreditation are outside the scope of ISO/IEC 15408. Accreditation is the administrative process whereby authority is granted for the operation of an IT product (or collection thereof) in its full operational environment including all of its non-IT parts. The results of the evaluation process are an input to the accreditation process. However, as other techniques are more appropriate for the assessments of non-IT related properties and their relationship to the IT security parts, accreditors should make separate provisions for those aspects.

f) The subject of criteria for the assessment of the inherent qualities of cryptographic algorithms is not covered in ISO/IEC 15408. Should independent assessment of mathematical properties of cryptography be required, the evaluation scheme under which ISO/IEC 15408 is applied must make provision for such assessments.

Information technology—Security techniques—Evaluation criteria for IT security—Part 1: Introduction and general model

1 Scope

This part of GB/T 18336 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of the ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products.

It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of the ISO/IEC 15408; defines the terms and abbreviations to be used in all parts of the ISO/IEC 15408; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given.

It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations.

The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. This part of ISO/IEC 15408 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation methodology is given in ISO/IEC 18045 and the scope of evaluation schemes is provided.

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 15408-2, 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, the following terms and definitions apply.

NOTE This clause contains only those terms which are used in a specialized way throughout ISO/IEC 15408. Some combinations of common terms used in ISO/IEC 15408, while not meriting inclusion in this clause, are explained for clarity in the context where they are used.

3.1 Terms and definitions common use

3.1.1

adverse actions

actions performed by a threat agent on an asset

3.1.2

assets

entities that the owner of the TOE presumably places value upon

3.1.3

assignment

specification of an identified parameter in a component or requirement

3.1.4

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.