Chinese General Techniques Requirements for Important Information Systems

Haohao Song, Jian Gu

The MPS Quality Supervision and Testing Center of Security Products for Computer Information System, The Third Research Institute of Ministry of Public Security, Shanghai, China

songhh@mctc.gov.cn, gujian@mctc.gov.cn

Keywords:common criterion; protection profile; important information system; security level protection system

Abstract. As information security level protection system is constructed and developed, information system is graded based on the degree of importance. In this paper, the work objectives of construction and rectification in information security level protection are introduced firstly. Based on the analysis of compilation background of general techniques requirements for important information systems, the general techniques requirements for important information systems is presented in detail. Finally, Evaluation of general techniques requirements is evaluated objectively.

Introduction

In 1994, the Chinese information security level protection system is implemented. At the present stage, the grading and recording work have been finished in the work of information security level protection. Fig. 1 shows the Chinese legal and policy system of information security level protection.

Grading range of important information systems includes four aspects below. The construction and rectification of national important information systems is the focus of our work at this stage.

- The important information systems in information services unit of the business public Internet, Internet access service units, data centers and other units.
- The important information systems in railways, banking, customs, taxation, civil aviation, electricity, securities, insurance, foreign affairs, science and technology, development and reform, national defense, public security and other industries, sectors of production, scheduling, management and office.
- The important websites and office information systems in city (prefecture) level and above party and government organs.
- Information system involving state secrets.

Work Objectives of Construction and Rectification in Information Security Level Protection

Work objectives of construction and rectification in information security level protection consists of “three years”, “three priorities” and “five aspects of goals”.

- Three years. Because there are the more information systems in some important industries, subject to funding, personnel constraints, considering the actual situation, the work of construction and rectification for the national rated information system is in general completed in three years. The charge authority of every industry should have a reasonable deployment of the overall work progress in accordance with time requirements and according to the number of information systems in the industry and the actual situation.
- Three priorities. Through three priorities such as the organization of information security level protection security management system construction, technical measures construction and grade evaluation, the requirements of level protection system are implemented.
- Five aspects of goals. By security construction and rectification work, the following objectives in five areas will be achieved: First, the whole management level of information system significantly is improved; second, security prevention ability of information systems

© 2015. The authors - Published by Atlantis Press

is markedly enhanced, third, security risks and security incidents from information systems are decreased, the four are the validity in protecting the healthy development of information technology, five for the effective protection of national security, social order and public interests.

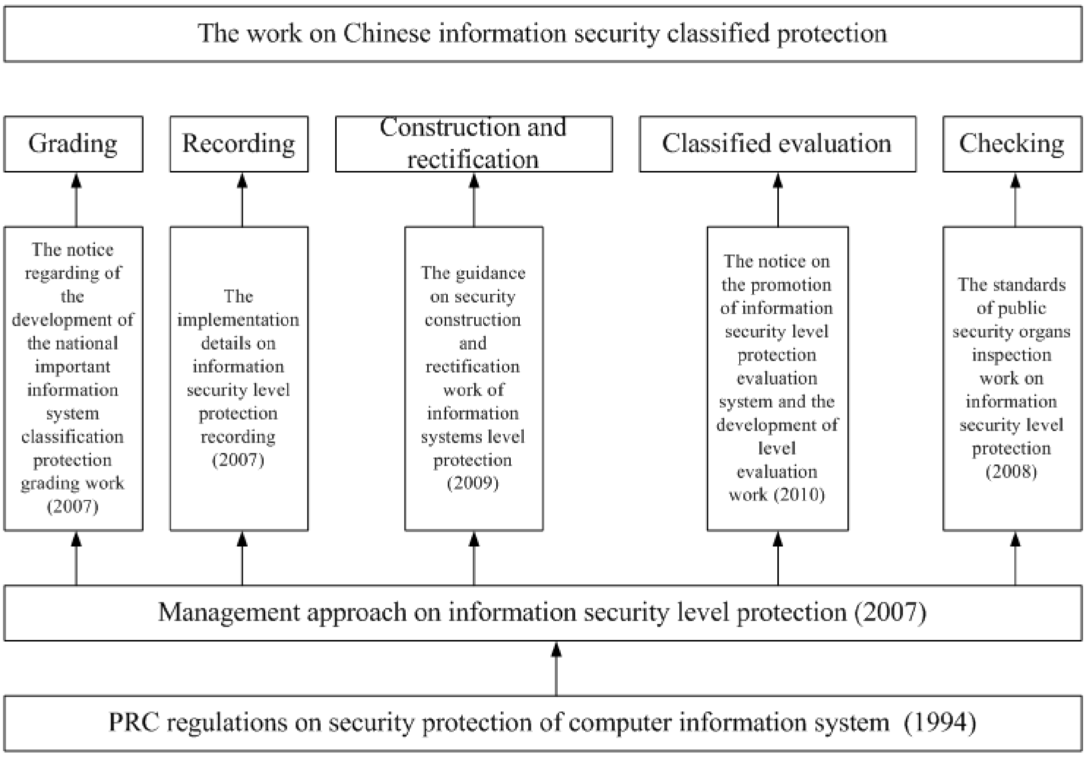
The work on Chinese information security classified protection
Grading
Recording
Construction and rectification
Classified evaluation
Checking
The notice regarding of the development of the national important information system classification protection grading work (2007)
The implementation details on information security level protection recording (2007)
The guidance on security construction and rectification work of information systems level protection (2009)
The notice on the promotion of information security level protection evaluation system and the development of level evaluation work (2010)
The standards of public security organs inspection work on information security level protection (2008)
Management approach on information security level protection (2007)
PRC regulations on security protection of computer information system (1994)

Figure 1. Chinese legal and policy system of information security level protection.

Compilation Background Of General Techniques Requirements For Important Information Systems

After TCSEC entered China, it combined the characteristics of China, then was revised and improved, and a mandatory national standard GB17859-1999 [1] was formatted. After a long-term development in China, the standard has formed its own unique system. GB18336-2008 is completely translated from ISO/IEC15408 [2], ISO/IEC15408 is CC (Common Criterion). In a sense, GB17859-1999 represents the actual demand for information security in China, GB18336-2008 [3] represents the requirements with international standards. Therefore, GB17859-1999 and GB18336-2008 together form two basis of information security standard system.

As the general techniques requirements for important information systems, it must also take into account GB17859-1999 and GB18336-2008 at the same time, thus it can be distinctive and compatible with the existing features of important information systems, and can meet the actual needs for the construction and rectification of national important information systems.

For the security assessment needs of general information system, PP (Protection Profile) is used as an extension of the mechanism of customization security requirements in ISO / IEC 15408. Usually for typical application requirements, the corresponding PP is designed based on some of the basic components package provided ISO / IEC 15408 standard itself.

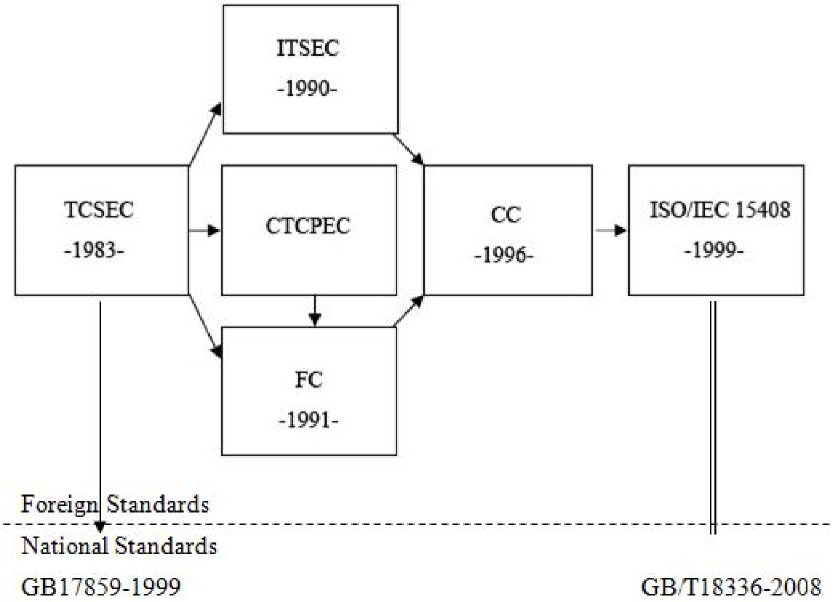

Figure 2. Relationship between GB 17859-1999 and GB/T 18336-2008.

In order to make the general techniques requirements for important information systems absorb the features of ISO / IEC 15408, we study the method of generated PP to generate the security elements of the general techniques requirements. Of course, different from completely generating a PP, We must also consider China a number of other unique requirements, that is, GB17859-1999 system requirements.

In summary, in the compilation process of general techniques requirements for important information systems, we must consider the following factors.

- The features of Chinese important information systems
- Security function level
- Assurance requirements level

Introduction Of General Techniques Requirements For Important Information Systems

Security Assurance Requirements. Based on the in-depth understanding of security assurance requirements of ISO/IEC 15408, the related content is described localized. And on this basis, the security assurance requirements of seven levels in ISO/IEC 15408 is classed into five security levels corresponding to the five security levels of GB17859. Based on the positioning of general techniques requirements of important information systems, the last three levels are used as the content.

From the specific content of view, 8 categories of assurance requirements of ISO/IEC 15408 were re-arranged in the standard, and on the basis of the above, the security assurance requirements set of the general techniques requirements was achieved.

Since the assurance requirements of the general techniques requirements re-organized the assurance requirements of ISO/IEC 15408 in the seven-level EAL, and there is not a simple relation between both, the level of the general techniques requirements with the corresponding level of EAL of ISO/IEC 15408 is shown in Table 1.

TABLE I. Relations of the level of general techniques requirements with the EAL level

Level of general techniques requirements	First Level	Second Level
EAL Level	Between EAL4 and EAL5	Between EAL6 and EAL7

Security Functional Requirements.

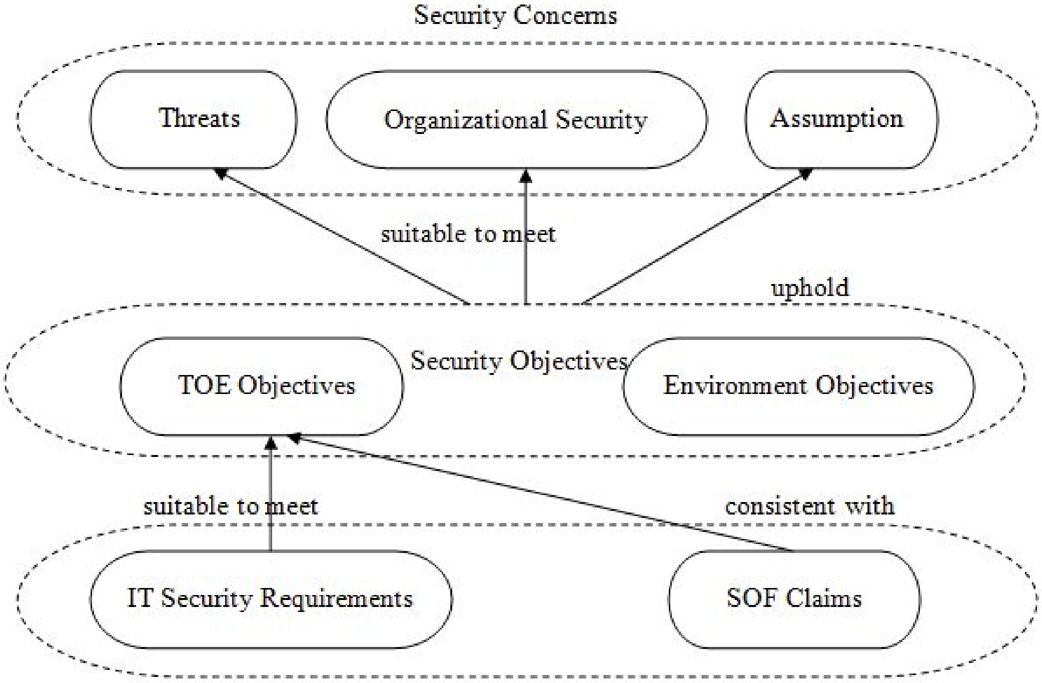

Figure 3. PP rationale requirements.

In order to more formal, more detailed presentation on the related security functional requirements of general techniques requirements, we have considered ISO/IEC TR 15446:2004, Information technology-Security techniques-Guide for the production of Protection Profiles and Security Targets, NEQ, and applied its approaches into the compilation process of general techniques requirements, and successfully achieved our objective.

Based on the guidelines for the compilation provided by ISO/IEC TR 15446:2004, referring to PP rationale requirements as shown in Fig.3, the compilation group of general techniques requirements referred the compilation processes of a number of PP, and localized the security function components of adopted ISO/IEC 15408, combined with some of the contents of China's information security level protection, and ultimately compiled the general techniques requirements for important information systems.

Conclusion

The presented general techniques requirements for important information systems not only includes the security elements of the ISO/IEC 15408, but also meets the actual demand of important information systems in China very well because it is constructed based on the guidance of ISO/IEC TR 15446:2004 like PPs.

The general techniques requirements will be regarded as the unique and authoritative guidance document for important information systems in the Chinese civil market, and will be used as the proof to designing, testing and evaluation of important information systems.

Acknowledgment

Research presented in this paper is sponsored by National Science and Technology Significant Project "Security Evaluation Technology Research on Smart Mobile Terminals " (No. 2012ZX03002011) and 2013 Annual Technical Standards Special Project of Science and Technology Commission of Shanghai Municipality " Research on key technical standards of testing on Information security product" (No. 13DZ0500501).

References

[1] GB 17859-1999 Classified Criteria for Security Protection of Computer Information System (1999).

[2] ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation, Version 3.1 (2006).

[3] GB/T 18336.1-2008 Information Technology-Security techniques—Evaluation Criteria for IT security - Part 1: Introduction and general model (2008).

[4] GB/T 18336.2-2008 Information Technology-Security techniques—Evaluation Criteria for IT security (2008).

[5] GB/T 18336.3-2008 Information Technology-Security techniques—Evaluation Criteria for IT security (2008).