# GA

PUBLIC SECURITY STANDARD OF

THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.240

A 90

# GA/T 1393-2017

# Information security technology - Security technical requirements for computer security reinforcement systems

信息安全技术 主机安全加固系统 安全技术要求

**Issued on: April 19, 2017** **Implemented on: April 19, 2017**

**Issued by: The Ministry of Public Security of the People's Republic of China**

# Table of Contents

# Information security technology - Security technical requirements for computer security reinforcement systems

## 1 Scope

This Standard specifies the security function requirements, security assurance requirements and classification requirements for computer security reinforcement systems.

This Standard applies to the design, development and testing of computer security reinforcement systems.

## 2 Normative references

The following documents are indispensable for the application of this document. For dated references, only the dated version applies to this document. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 18336.3-2015, Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components

GB/T 25069-2010, Information security technology glossary

## 3 Terms and definitions

Terms and definitions determined by GB/T 18336.3-2015 and GB/T 25069-2010 are applicable to this document.

## 4 Description of computer security reinforcement systems

The computer security reinforcement system is based on the general operating system. It enhances the security functions of the operating system by marking the host and object of the operating system, adding mandatory access control, integrity protection and other technical means, to make up for the security of the general-purpose operating system, and to improve the security protection capabilities of the operating system.

development, guidance documents, life cycle support, test, vulnerability assessment.

### 5.2 Security grade

According to the strength of the security function requirements of the computer security reinforcement systems and GB/T 18336.3-2015, divide the security grade of the computer security reinforcement systems. The security grade is divided into basic grade and enhanced grade. The strength of security functions and the level of security assurance requirements are the specific basis for gradation; the security grade highlights the security feature.

## 6 Security function requirements

### 6.1 Authentication

The product's reinforcement requirements for the operating system's identity authentication function shall meet:

a) The operating system user identification shall use the user name and user identification (UID), and achieve the unique identification of the user throughout the life cycle of the operating system, and the consistency between the user name, UID, etc.;

b) For operating system users, use enhanced password management and/or token-based dynamic passwords and/or biometric authentication and/or digital certificates for identity authentication;

c) For operating system users, use the two-factor authentication technology in 6.1b) to authenticate users.

### 6.2 Security identification

The product's reinforcement requirements for the operating system security identification shall meet:

a) Set sensitivity labels on subjects and objects within the control range of operating system security functions;

b) When information is input from outside the control range of the operating system to the control range, its sensitivity label shall be marked by a label;

c) Set sensitivity labels on all subjects and objects of the operating system;

d) When information is input from within the control range of the operating system to outside the control range, the sensitivity label of the data shall be clearly marked.

e) Provide functions such as termination of illegal processes, simple attack detection, and measures to prevent audit data loss;

f) Audit records include the date, time, type, subject identification, object identification and results of the event.

### 6.5 Integrity protection

The product's reinforcement requirements for the operating system integrity protection shall meet:

a) Be able to set integrity labels for subjects and objects within the control range of operating system security functions; establish integrity protection strategy models; protect the integrity of important files during storage, transmission and processing;

b) Have measures to recover after detecting that the integrity has been damaged;

c) Ensure that low-integrity data cannot be inserted or overwritten to high-integrity data;

d) Ensure that the level of data integrity is not reduced during processing;

e) Establish a semi-formal integrity security policy model.

### 6.6 Remaining information protection

The product's reinforcement requirements for the operating system remaining information protection shall meet:

a) Ensure that the storage space where the authentication information of operating system users is located is completely cleared before being released or redistributed to other users, regardless of whether the information is stored on the hard disk or in the memory;

b) Ensure that the storage space where resources such as files and directories in the system are located is completely cleared before being released or reallocated to other users.

### 6.7 Administrator security management

#### 6.7.1 Initialization of administrator properties

The product shall provide the ability to initialize the attributes of the authorized administrator.

#### 6.7.2 The unique identifier of the administrator

It shall protect the data that is transmitted through the network between product components, so as to prevent unauthorized access.

### 6.9 Audit log management

The product shall provide the following functions to manage audit logs:

a) Perform a combined query of audit logs according to date, time, user identification, application resource identification and other conditions;

b) There are certain measures to prevent the loss of audit logs;

c) Back up the audit log and clear it after backup.

## 7 Security assurance requirements

### 7.1 Development

#### 7.1.1 Security architecture

The developer shall provide a description of the security architecture of the product security functions; the description of the security architecture shall meet the following requirements:

a) Be consistent with the grade of abstract description of the security function that is implemented in the product design document;

b) Describe the security domain of the product security function that is consistent with the security function requirements;

c) Describe why the product security function initialization process is secure;

d) Verify that the product security function can prevent damage;

e) Verify that the product security function can prevent the security feature from being bypassed.

#### 7.1.2 Functional specification

The developer shall provide a complete functional specification; the functional specification shall meet the following requirements:

a) Fully describe the security function of the product;

b) Describe the purpose and usage of all security function interfaces;

c) Identify and describe all parameters that are related to each security function interface;

f) Provide the mapping relationship between security function subsystems and modules;

g) Describe all security function realization modules, including their purpose and interaction with other modules;

h) Describe all the relevant interfaces that are required to implement the security function of the module, the return value of other interfaces, the interaction with other modules and the called interfaces;

i) Describe the support or related modules of all security functions, including their purpose and interaction with other modules.

### 7.2 Guiding documents

#### 7.2.1 Operating user guide

The developer shall provide a clear and reasonable operating user guide. The operating user guide is consistent with all other documents that are provided for assessment. The description of each user role shall meet the following requirements:

a) Describe the functions and privileges that are accessible to users who are controlled in the secure processing environment, including appropriate warning information;

b) Describe how to use the available interfaces that are provided by the product in a secure manner;

c) Describe the available functions and interfaces, especially all the security parameters that are controlled by the user; specify the security values when appropriate;

d) Clearly state every security-related event that is related to the user-accessible function that needs to be performed, including changing the security characteristics of the entity that is controlled by the security function;

e) Identify all possible states of product operation (including failures or operational errors that are caused by operations), and their causal relationships and connections with maintaining security operations;

f) Fully realize the security strategy that must be implemented for the security purpose.

#### 7.2.2 Preparation procedures

b) Implementation representation, security defect report and its resolution status.

#### 7.3.3 Delivery procedures

The developer shall use certain delivery procedures to deliver products and document the delivery process. When delivering each version of the product to the user, the delivery document shall describe all procedures necessary to maintain security.

#### 7.3.4 Development security

The developer shall provide development security document. The development security document shall describe all physical, procedural, personnel and other security measures necessary to protect the confidentiality and integrity of product design and implementation in the product development environment.

#### 7.3.5 Life cycle definition

The developer shall establish a life cycle model to perform necessary control of the development and maintenance of the product, and provide a life cycle definition document to describe the model that is used to develop and maintain the product.

#### 7.3.6 Tools and technology

The developer shall clearly define the tools that are used to develop the product, and provide the development tool document to unambiguously define the meaning of each statement in the implement and the meaning of all options that depend on the implementation.

### 7.4 Test

#### 7.4.1 Test coverage

The developer shall provide test coverage documents; the test coverage description shall meet the following requirements:

a) Indicate the correspondence between the test that is identified in the test document and the security function of the product that is described in the functional specification;

b) Show that the above correspondence is complete, and verify that all security function interfaces in the functional specification have been tested.

#### 7.4.2 Test depth

**This is an excerpt of the PDF (Some pages are marked off intentionally)**



**------ The End ------**