GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.020
L 09

GB 17859-1999

Classified Criteria for Security Protection of Computer Information System

Issued on: September 13, 1999 **Implemented on: January 1, 2001**

Issued by: State Quality Technical Supervision Bureau

Table of Contents

Foreword

This Standard has three main goals: firstly, providing reference for the formulation of safety codes for computer information system and the supervision and inspection by law-enforcing departments; secondly, providing technical support for safety products development; and thirdly, providing technical guidance for construction and management of safety system.

This Standard is prepared by reference to American trusted computer system evaluation criterion (DoD 5200.28-STD) and explanation on computer network system (NCSC-TG-005).

In the text of this Standard, those in bold represent the performance requirements that are not appeared in lower level or being strengthened.

This Standard is the first part of serial standards for security protection of computer information system. The serial standards for security protection level of computer information system cover:

Classified Criteria for Security Protection of Computer Information System;

Guideline for Application of Classified Criteria for Security Protection of Computer Information System;

Evaluation Criteria for Security Protection of Computer Information System;

……

This Standard shall be implemented in accordance with specifications of the supporting national standards.

This Standard was proposed by and shall be under the jurisdiction of the Ministry of Public Security of the People's Republic of China.

Drafting organizations of this Standard: Tsinghua University, Peking University AND Chinese Academy of Sciences.

Chief drafting staffs of this Standard: Hu Daoyuan, Wang Lifu, Qing Sihan, Jing Qianyuan, Na Risong, Li Zhipeng, Cai Qingming, Zhu Weiguo and Chen Zhong.

This Standard shall be implemented from January 1, 2001.

The Ministry of Public Security of the People's Republic of China is responsible for the interpretation of this Standard.

Classified Criteria for Security Protection of Computer Information System

1 Scope

This Standard specifies five levels for security protection capacity of computer information system, i.e.:

Level 1: the user's discretionary protection level;

Level 2: system audit protection level;

Level 3: security label protection level;

Level 4: structured protection level;

Level 5: access verification protection level.

This Standard is applicable to the classification for technical capability levels for computer information system security protection. With the improving of security protection level, security protection capability of computer information system improves gradually.

2 Normative References

The following normative documents contain provisions which, through reference in this text, constitute the provisions of this Standard. At the time of publication, the editions indicated were valid. All the standards will be revised and modified, and all parties using this Standard shall discuss the possibility of using the latest version.

GB/T 5271 Data Processing - Vocabulary

3 Definitions

Except those defined in this chapter, other definitions not listed are detailed in GB/T 5271.

3.1 Computer information system

A man-machine system that is composed of computer and associated and supporting equipment and facility (including network) to collect, process, store, transmit and retrieve the information according to certain application goals and rules.

3.2 Trusted computing base of computer information system

The generic term for the protection devices in computer system, which includes hardware, firmware, software, and assembly responsible for the implementation of security policy, establishes a basic protection environment and provides additional user service required by a trusted computing system.

3.3 Object

Carrier of the information.

3.4 Subject

Person, process or equipment etc. which cause flow of information among objects.

3.5 Sensitivity label

A group of information that expresses the objects security level and describes the object data sensitivity; sensitivity label is adopted as the reference for mandatory access control decision in trusted computing base.

3.6 Security policy

Laws, specifications and enforcement regulations in management, protection and issuing of sensitive information.

3.7 Channel

Path for information transmission in system.

3.8 Covert channel

Communication channel which allows the process transmits information in the mode to damage system security strategy.

3.9 Reference monitor

Component for monitoring the authorization access relation between subject and object.

4 Level Classification Criteria

4.1 Level 1: the user's discretionary protection level

Trusted computing base of computer information system at this level enables the user to be possessed of security protection capability by isolating user from data, and is provided with the controlling capability in multiple forms to perform access control for the user, i.e., provide feasible means to the user to

protect information of the user and the user group as well as avoid illegal read/write and destroy concerning data by other users.

4.1.1 Discretionary access control

Trusted computing base of computer information system defines and controls the access to named object by named user in the system. Implementation mechanism (for example: access control list) allows the named user, under the identity of user and (or) user group, to specify and control sharing by object as well as prevents unauthorized user reading sensitive information.

4.1.2 Identity authentication

In the initial implementation by trusted computing base of computer information system, it is first required the user to label his own identity and authenticate the user's identity by protection mechanism (e.g.: password), then prevent unauthorized user to access user identity authentication data.

4.1.3 Data integrity

Trusted computing base of computer information system prevents unauthorized user modifying or destroying sensitive information by way of discretionary integrity policy.

4.2 Level 2: system audit protection level

Compared with the user's discretionary protection level, trusted computing base of computer information system at this level implements discretionary access control with finer granularity, and makes the user to be responsible for itself by logging in regulations, auditing security dependent event and isolating resources.

4.2.1 Discretionary access control

Trusted computing base of computer information system defines and controls the access to named object by named user in the system. Implementation mechanism (for example: access control list) allows the named user, under identity of user and (or) user group, to specify and control sharing by objects as well as prevents unauthorized user reading sensitive information **and controls access authority spreading. Discretionary access control mechanism prevents unauthorized user accessing object according to method designated by user or default mode. The granularity of access control is single user. For the user without access authority, only the authorized user is allowed to designate the access authority to object.**

4.2.2 Identity authentication

In the initial implementation by trusted computing base of computer information

system, it firstly requires the user to label his own identity and authenticates the user's identity by protection mechanism (e.g.: password), then prevents unauthorized user to access user identity authentication data. **Trusted computing base of computer information system is capable of making the user to be responsible for itself by providing unique label to the user. Trusted computing base of computer information system is also provided with the capability to correlate identity label with all auditable behaviors of the said user.**

4.2.3 Object reusing

In the idle space for object storing in trusted computing base of computer information system, before a subject is designated initially, assigned or re-assigned to object, all authorizations of the information contained in such object shall be revoked. In case a subject obtains the authority to access the released object, the current subject cannot obtain any information generated by activities by the original subject.

4.2.4 Auditing

Trusted computing base of computer information system can create and maintain the access audit trial records of the object protected, also prevent unauthorized user accessing or destroying the object protected.

Trusted computing base of computer information system can record the following events: adopting identity authentication mechanism; introducing the object in the user's address space (for example: file opening and program initialization); deleting object; actions implemented by operator, system administrator or (and) system security administrator, and other events relative to system security. For each event, the audit record includes: date and time of event, user, event type and whether the event is successful. The audit record includes request source (for example: terminal identifier) for identity authentication event and name of object for the event that object is introduced in the user's address space and the event that object is deleted.

For auditing event which cannot be distinguished independently by trusted computing base of computer information system, the auditing mechanism provides audit record interface which may be invoked by authorization subject. These audit records are different from audit records distinguished independently by trusted computing base of computer information system.

4.2.5 Data integrity

Trusted computing base of computer information system prevents unauthorized user from modifying or destroying sensitive information by way of discretionary integrity policy.

4.3 Level 3: security label protection level

resource) which can be accessed directly or indirectly by external subject. , and designates sensitivity labels for these subjects and objects; these labels are the combination of level classification and non-level category as well as the reference for implementing mandatory access control. **Trusted computing base of computer information system supports the security level composed of two or more ingredients.** The direct or indirect access to objects by all external subjects of trusted computing base of computer information system shall meet the following cases: subject may be capable of reading object only in case the level classification in subject security level is higher than or equal to that in object security level and the non-level category in subject security level contains all non-level categories in object security level; subject may be capable of writing an object only in case the level classification in subject security level is lower than or equal to that in object security level and the non-level category in subject security level is contained in the non-level category in object security level. Trusted computing base of computer information system adopts identity and authentication data to authenticate the user's identity, ensure the security level of external subject for trusted computing base of computer information system created by user, and authorizes to be under control of the said user's security level and of authorization.

4.4.3 Labeling

Trusted computing base of computer information system maintains sensitivity labels relative to computer information system resources (e.g.: subject, storage object and read only memory) which may be accessed directly or indirectly by external subject. These sensitivity labels are the basis for implementing mandatory access. In order to input data not with security label, trusted computing base of computer information system requires the security level of the said data from the authorized user and then accepts such security level which may also be audited by trusted computing base of computer information system.

4.4.4 Identity authentication

In the initial implementation by trusted computing base of computer information system, it is first required the user to label his own identity, besides, trusted computing base of computer information system maintains user identity authentication data and determines user access authority and authorization data. Trusted computing base of computer information system adopts these data and protection mechanism (e.g.: password) to authenticate the user's identity, then prevent unauthorized user to access user identity authentication data. Trusted computing base of computer information system is capable of making the user to be responsible for itself by providing unique label to the user. Trusted computing base of computer information system is also provided with the capability to correlate identity label with all auditable behaviors of the said user.

4.4.5 Object reusing

Trusted computing base of computer information system can create and maintain the access audit trial records of the object protected, and prevent unauthorized user accessing or destroying the object protected.

Trusted computing base of computer information system can record the following events: adopting identity authentication mechanism; introducing the object in the user's address space (for example: file opening and program initialization); deleting object; actions implemented by operator, system administrator or (and) system security administrator, and other events relative to system security. For each event, the audit record includes: date and time of event, user, event type and whether the event is successful. The audit record includes request source (for example: terminal identifier) for identity authentication event as well as name of object and object security level for the event that object is introduced in the user's address space and the event that object is deleted. Moreover, trusted computing base of computer information system is possessed of the capability to audit and modify the readable output mark.

For auditing event which cannot be distinguished independently by trusted computing base of computer information system, the auditing mechanism provides audit record interface which may be invoked by authorized subject. These audit records are different from audit records distinguished independently by trusted computing base of computer information system. Trusted computing base of computer information system is capable of auditing the event which may possibly be used in the case that covert storage channel is utilized.

Trusted computing base of computer information system contains the mechanism which is capable of monitoring auditable security event occurrence and accumulation; once threshold is exceeded, immediate alarm to security administrator must be possible. Besides, if these security-related events continue to occur or accumulate, the system shall suspend at the minimal cost.

4.5.7 Data integrity

Trusted computing base of computer information system prevents unauthorized user modifying or destroying sensitive information by way of discretionary and mandatory integrity policy. In network environment, integrity sensitivity labels are adopted to assure the information is not damaged in transmission.

4.5.8 Covert channel analysis

System developer shall search the covert storage channel thoroughly and determine the maximum bandwidth labeled with channel one by one according to actual measurement or engineering estimate.

4.5.9 Trusted path

In case user is connected (for example: subject security level is registered and

modified), trusted computing base of computer information system provides trusted communication path between it and user. Communication on trusted path may only be activated by trusted computing base of computer information system and is isolated logically and distinguished correctly from communication on other paths.

4.5.10 Trusted recovery

Trusted computing base of computer information system provides process and mechanism to ensure the recovery of computer information system after failure or interruption without damage on any security protection.

_____ END _____

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

------ The End ------