

ICS 35.040
CCS L 80



**NATIONAL STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GB/T 21028-2007

**Information security technology -- Security techniques
requirement for server
(English Translation)**

Issued on: June 29, 2007

Implemented on: December 1, 2007

**Issued by: General Administration of Quality Supervision, Inspection and
Quarantine Standardization Administration of PRC**

Table of Contents

Foreword...	4
Introduction...	5
1 Scope...	6
2 Normative References...	6
3 Terms, Definitions and Abbreviations...	7
3.1 Terms and definitions...	7
3.2 Abbreviation...	8
4 Requirements for Server Security Function...	8
4.1 Device security...	8
4.1.1 Device label...	8
4.1.2 Support for reliable operation of device...	9
4.1.3 Monitoring the working status of the device...	9
4.1.4 Device electromagnetic protection...	9
4.2 Operation security...	9
4.2.1 Security monitoring...	9
4.2.2 Security audit...	10
4.2.3 Malicious code protection...	13
4.2.4 Backup and fault recovery...	13
4.2.5 Trusted technical support...	14
4.2.6 Trusted timestamp...	14
4.3 Data security...	15
4.3.1 ID authentication...	15
4.3.2 Discretionary access control...	16
4.3.3 Label...	17
4.3.4 Mandatory access control...	19
4.3.5 Data integrity...	21
4.3.6 Data confidentiality...	21
4.3.7 Dataflow control...	22
4.3.8 Trusted path...	22
5 Requirements of Server Security Classification...	23
5.1 Level-1: user discretionary protection level...	23
5.1.1 Security function requirements...	23

5.1.2 Security assurance requirements...	25
5.2 Level-2: system audit protection level...	26
5.2.1 Security function requirements...	26
5.2.2 Security assurance requirements...	30
5.3 Level-3: security label protection level...	31
5.3.1 Security function requirements...	31
5.3.2 Security assurance requirements...	36
5.4 Level-4: structured protection level...	38
5.4.1 Security function requirements...	38
5.4.2 Security assurance requirements...	44
5.5 Level-5: access verification protection level...	45
5.5.1 Security function requirements...	45
5.5.2 Security assurance requirements...	51
Appendix A (Informative) Relevant Concept Explanation...	53
A.1 Composition and interrelationship...	53
A.2 Special requirements for server security...	53
A.3 Further explanation of subject and object...	54
A.4 SSOS, SSF, SSP, SFP, and their relationships...	55
A.5 Explanation on cryptographic technique...	55
A.6 Explanation on electromagnetic protection...	55
Bibliography...	56

1 Scope

This Standard specifies, based on the five security protection levels specified in GB

17859-1999, the security technical requirements required by the server and the different security technical requirements for each security protection level.

This Standard is applicable to the design, implementation, purchase and use of the hierarchical server in accordance with the requirements of the five security protection levels specified in GB 17859-1999. The testing and management of server security according to the requirements of the five security protection levels specified in GB

17859-1999 can be referred to.

2 Normative References

The provisions in following documents become the provisions of this Standard through reference in this Standard. For dated references, the subsequent amendments (excluding corrigendum) or revisions do not apply to this Standard, however, parties who reach an agreement based on this Standard are encouraged to study if the latest versions of these documents are applicable. For undated references, the latest edition of the referenced document applies.

GB 17859-1999 Classified Criteria for Security Protection of Computer Information System

GB/T 20271-2006 Information Security Technology - Common Security Techniques Requirement for Information System

GB/T 20272-2006 Information Security Technology - Security Techniques Requirement for Operating System

GB/T 20273-2006 Information Security Technology - Security Techniques Requirement for Database Management System

GB/T 20520-2006 Information Security Technology - Public Key Infrastructure - Time Stamp Specification use, etc.; and provide monitoring data analysis functions, if necessary.

4.2.1.2 Network security monitoring

The server shall monitor the incoming and outgoing network data flow in real time at its network interface unit. According to the different requirements of different security level against the network security monitoring, the network security monitoring shall:

- a) Do not depend on the server operating system, and is not unavailable due to the non-power-off failure of the server;
- b) The incoming and outgoing network data flow is tested according to the established security policies and rules;
- c) Support security policies and rules for user-defined network security monitoring;
- d) Have the function of monitoring the classification of network application behavior, and have the ability to provide alarm and interruption according to the security policies;
- e) Provide centralized management functions in order to receive the security policies and rules issued by the network security monitoring centralized management platform; and provide audit data source to the network security monitoring centralized management

platform.

4.2.2.1 Response of security audit

The security audit SSF shall respond to the audit events as follows:

- a) Audit log records: when a security invasion event is detected, the audit data shall be recorded in the audit log;
- b) Real-time alarm generation: when a security invasion event is detected, the real-time alarm information shall be generated, and alarm selectively according to the setting of the alarm switch;
- c) Termination of the offending process: when a security invasion event is detected, the offending process shall be terminated;
- d) Service cancellation: when a security invasion event is detected, the current service shall be cancelled;
- e) User account disconnection and invalidation: when a security invasion event is detected, the current user account shall be disconnected, and invalidated.

current activities and the established usage model. When the user's challenge level exceeds the threshold condition, it can indicate that a threat to security is about to occur.

c) Simple attack detection: it can detect the occurrence of the signature events that pose a significant threat to the implementation of SSF. Thus, the SSF shall maintain and indicate the internal representation of the signature events that invaded the SSF; compare the detected system behavior records and the signature events, when a match is found between the two ones, then an attack on the SSF is imminent.

d) Complex attack detection: on the basis of the above simple attack detection, multiple steps of invasion can be detected; a complete invasion situation can be simulated based on a known sequence of events; point out a signature event or time for event sequence that indicate a potential invasion of the SSF.

4.2.2.4 Security audit review

According to the different requirements of different security levels against the security audit review, the security audit review can be divided into:

- a) Basic audit review: provide the ability to read information from audit records, namely, provide the ability for the authorized user to obtain and interpret the audit information. When the user is a person, the information must be expressed in a human-readable manner; when the user is an external IT entity, the audit information must be expressed electronically without ambiguity.
- b) Limited audit review: on the basis of basic audit review, the users without read and