# GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80

# GB/T 20278-2013

Replacing GB/T 20278-2006

# Information Security Technology - Security Technical Requirements for Network Vulnerability Scanners

信息安全技术

网络脆弱性扫描产品安全技术要求



**Issued on: December 31, 2013** **Implemented on: July 15, 2014**

**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.**

# Table of Contents

# Foreword

This Standard was drafted according to the rules in GB/T 1.1-2009.

This Standard replaces GB/T 20278-2006 "Information Security Technology Technique Requirement for Network Vulnerability Scanners". The main differences in this Standard over GB/T 20278-2006 are as follows:

- The name of the standard was changed to "Information Security Technology - Security Technical Requirements for Network Vulnerability Scanners";
- The definition of "network vulnerability scan" was modified (see 3.3);
- "vulnerability of NIS service" (see 7.3.1.8 of 2006-edition) was deleted;
- "vulnerability of database" was deleted (see 7.3.1.18 of 2006-edition);
- "RPC port" was deleted (see 7.3.4.1 of 2006-edition);
- "NI service" was deleted (see 7.3.4.5 of 2006-edition);
- "alarm function" was deleted (see 7.4.4.1 of 2006-edition);
- "installation and operation control" was deleted (see 7.5 of 2006-edition);
- "interaction with IDS product", "interaction with fire wall product", "interaction with other application programs" were deleted ( see 7.7.4.2, 7.7.4.3,7.7.7.4 and 8 of 2006-edition);
- "performance requirements" was deleted;
- The requirement of upgrading security measures during product upgrading was added;
- The function of comparison and analysis between scanning results was added;
- Authentication data protection, authentication failure handling, timeout locking or logout, remote management and other functions were added in the self-security requirements of product;
- The integral structure of this Standard was adjusted; it is described according to the product security function requirements, self-security requirements and security assurance requirements; in addition, the requirement items of product self-security were detailed, and the contents of audit function requirements were defined.

This Standard was proposed by and shall be under the jurisdiction of National Technical Committee on Information Technology Security of Standardization

Administration of China (SAC/TC 260).

Certain content of this document may involve patent. The issuing organization of this Standard shall not undertake the responsibility of identifying these patents.

Drafting organizations of this Standard: Quality Supervision Testing Center of Ministry of Public Security for Computer information system security product, Venustech Information & Technology Co., Ltd. AND Netpower Information & Technology Co., Ltd.

Chief drafters of this Standard: Gu Jianxin, Lu Zhen, Yu You, Gu Jian, Zhao Ting, Wang Zhijia, Wang Honghong and Ming Xu.

# Information Security Technology - Security Technical Requirements for Network Vulnerability Scanners

## 1 Scope

This Standard specifies the security function requirements, self-security requirements and security assurance requirements of network vulnerability scanners, and classifies their levels according to different security technical requirements for network vulnerability scanners.

This Standard is applicable to the development, production and detection of network vulnerability scanners.

## 2 Normative References

The following documents are essential for the application of this document. For the dated references, only the dated editions apply to this document. For undated references, the latest editions (including amendments) apply to this document.

| | |
|---|---|
| GB 17859-1999 | Classified Criteria for Security Protection of Computer Information System |
| GB/T 18336.3-2008 | Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 3: Security Assurance Requirements |
| GB/T 25069-2010 | Information Security Technology - Glossary |

## 3 Terms and Definitions

For the purpose of this Standard, the terms and definitions specified in GB/T 17859-1999 and GB/T 25069-2010 as well as the following ones apply.

**3.1**

**Scan**

The process of using technical tools to detect the security risks that are existed in target system.

**3.2**

**Vulnerability**

The weakness in network system that may be made use of and cause hazard.

**3.3**

**Network vulnerability scan**

Remotely detect target system for security risk through network, inspect and analyze its security vulnerability thereby to find out the security loophole that may be utilized by intruder, and recommend some preventative and remedial measures.

**3.4**

**Banner**

A piece of information sent by application program, generally including words of welcome, application name and version, etc.

# 4 Abbreviations

For the purpose of this Standard, the following abbreviations apply.

| | |
|---|---|
| CGI: | Common Gateway Interface |
| CVE: | Common Vulnerabilities and Exposures |
| DNS: | Domain Name System |
| DoS: | Denial of Service |
| FTP: | File Transfer Protocol |
| IP: | Internet Protoco1 |
| NETBIOS: | NETwork Basic Input Output System |
| NFS: | Network File System |
| POP3: | Post Office Protocol 3 |
| RPC: | Remote Procedure Call |
| SMB: | Server Message Block |
| SMTP: | Simple Mail Transfer Protocol |
| SNMP: | Simple Network Management Protocol |

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

# 5 Level Classification of Network Vulnerability Scanners

## 5.1 Description of Level Classification

### 5.1.1 Basic-level

This level specifies basic functional requirements for network vulnerability scanners, It limits the use of the product function and the control of data access through certain user identification and identity authentication, making product be possessed with the ability of autonomous security protection, guaranteeing that the network vulnerability scanners can operate normally and with audit function so that the operation behaviors of administrators and scanning events are traceable. It provides basic analysis processing capability according to the scanning result through obtaining scanning information and generates report. Its self-security requirements shall be in accordance with the relevant requirements of system audit protection level in GB 17859-1999, and security assurance requirements shall be in accordance with the requirement of EAL Level 2 specified in GB/T 18336.3-2008.

### 5.1.2 Enhanced-level

Network vulnerability scanners of this level not only meet all the aforesaid basic-level requirements, but also further divide different security management roles, so as to detail the control of product management rights, in addition, the input and output as well as comparison of scanning result, the scanning under known account number / password, upgrading security measures, IP address scanning restriction, interactivity requirements, audit storage safety and other contents are added, making the functional requirements of products more complete and the use more convenient. The self-security requirements of product shall be in accordance with the requirements of security label protection level specified in GB 17859-1999, the security assurance requirements of product cover all stages of the product from development to application, in accordance with the requirements of EAL Level 4 specified in GB/T 18336.3-2008, and on this basis, lifting vulnerability analysis requirement to be able to resist the attack initiated by attacker with medium attack capability.

## 5.2 Level Classification

The level classification of network vulnerability scanners are shown in Tables 1, 2 and 3. The level assessment of network vulnerability scanners is obtained comprehensively in accordance with these three tables, the network vulnerability scanners in accordance with basic-level shall meet all the items that basic-level product shall meet as specified in Tables 1, 2 and 3; the network vulnerability scanners

in accordance with enhanced-level shall meet all the items that enhanced-level products shall meet as specified in Tables 1, 2 and 3.

**Table 1 Level Classification of Security Function Requirements**

| Security function requirements | | | Basic-level | Enhanced-level |
|---|---|---|---|---|
| Information acquisition | Port scanning | TCP port | * | * |
| | | UDP port | * | * |
| | | Port protocol analysis | * | * |
| | Operating system detection | | * | * |
| | Service banner | | * | * |
| | Other information | | * | * |
| Content of vulnerability scanning | Vulnerability of browser | | * | * |
| | Vulnerability of mail service | | * | * |
| | Vulnerability of FTP service | | * | * |
| | Vulnerability of Web service | | * | * |
| | Vulnerability of DNS service | | * | * |
| | Vulnerability of other known TCP/IP services | | * | * |
| | Vulnerability of RPC service | | * | * |
| | Vulnerability of SNMP service | | * | * |
| | Weak password | | * | * |
| | Vulnerability of Windows operating system user, group, password, sharing and registry, etc. | | * | * |
| | Trojan horse | | * | * |
| | Vulnerability of NFS service | | * | * |
| | Vulnerability of router/switch | | * | * |
| | Vulnerability of DoS attack | | * | * |
| | File sharing | | * | * |
| Scanning result analysis and treatment | Result storing | | * | * |
| | Import and export of result | | - | * |
| | Report generation | | * | * |
| | Report customization | | - | * |
| | Report output | | * | * |
| | Result browsing | | * | * |
| | Suggestion on vulnerability mending | | * | * |
| | Result comparison | | - | * |
| Scan configuration | Scanning strategy | | * | * |
| | Schedule task | | * | * |
| | Known account number / password scanning | | - | * |
| Security of scanning object | Effect on performance of the network where target system locates | | * | * |
| | Effect on target system | | * | * |
| Upgrading capability | | | * | ** |
| Scanning speed | | | * | * |

# 7 Security Technical Requirements for Basic-level

## 7.1 Security Function Requirements

### 7.1.1 Information acquisition

#### 7.1.1.1 Port scanning

##### 7.1.1.1.1 TCP port

Network vulnerability scanner shall be able to scan all TCP ports and inspect whether they are open.

##### 7.1.1.1.2 UDP port

Network vulnerability scanner shall be able to scan all UDP ports and inspect whether they are open.

##### 7.1.1.1.3 Port protocol analysis

For the opened TCP/UDP port obtained by scanning, the network vulnerability scanner shall be able to judge the universal service or used protocol of corresponding ports.

#### 7.1.1.2 Operating system detection

Network vulnerability scanner shall be able to detect the type and version number of operating system.

#### 7.1.1.3 Service banner

Network vulnerability scanner shall be able to acquire the banners of all open common services.

#### 7.1.1.4 Other information

Network vulnerability scanner shall be able to detect other information, such as network configuration information and, operating status information.

### 7.1.2 Content of vulnerability scanning

#### 7.1.2.1 Vulnerability of browser

Network vulnerability scanner shall be able to inspect the information and configuration related to browser security, and make appropriate security suggestions if dangerous or unreasonable configuration is found. The inspection items shall include:

a) Browser version number;

b) Browser security settings;

c) Vulnerability of browser;

d) Other security risks.

#### 7.1.2.2 Vulnerability of mail service

Network vulnerability scanner shall be able to inspect the security problems of such service programs using POP3, SMTP and other protocols related to e-mail:

a) Service program banner and version number.

b) The vulnerability of service program, including:

- Lack of legality inspection on input;
- Unable to handle abnormal conditions correctly.

c) Risk or wrong configuration of server, including:

- Allowing EXPN and VRFY commands;
- Allowing e-mail forwarding;
- Other insecure configuration.

d) Other security risks.

#### 7.1.2.3 Vulnerability of FTP service

Network vulnerability scanner shall be able to inspect the security problems of such service programs using FTP protocol, and the inspection items shall include:

a) Service program banner and version number.

b) The vulnerability of service program, including:

- Lack of legality inspection on input;
- Unable to handle abnormal conditions correctly.

c) Risk or wrong configuration of server, including:

- Allowing anonymous login;
- Using default password;
- Allowing dangerous commands;

- Other insecure configurations.

d) Other security risks.

#### 7.1.2.4 Vulnerability of Web service

Network vulnerability scanner shall be able to inspect the security problems of such programs providing Web service, and the inspection items shall include:

a) Service program banner and version number.

b) The vulnerability of service program, including:

- Lack of legality inspection on input;
- Unable to handle abnormal conditions correctly.

c) The vulnerability of scripts running on server and CGI program.

d) Risk or wrong configuration of server, including:

- File attribute error;
- Directory attribute error;
- Other insecure configurations.

e) Other security risks.

#### 7.1.2.5 Vulnerability of DNS service

Network vulnerability scanner shall be able to inspect the security problems of DNS service, and the inspection items shall include:

a) Service program banner and version number.

b) The vulnerability of service program, including:

- Lack of legality inspection on input;
- Unable to handle abnormal conditions correctly.

c) Other security risks.

#### 7.1.2.6 Vulnerability of other known TCP/IP services

Network vulnerability scanner shall be able to inspect the security problems of other service programs using TCP/IP protocol, and the inspection items shall include:

a) Service program banner and version number.

d) Version number of SAMBA server software.

#### 7.1.3 Scanning result analysis and treatment

##### 7.1.3.1 Result storing

Scanning result shall be able to be written in result database.

##### 7.1.3.2 Report generation

Network vulnerability scanner shall be able to generate corresponding report according to scanning result, and the requirements for the report shall include the following contents:

a) The CVE No., detailed information, remedial suggestion, etc. of each vulnerable point;

b) Risk level assessment of target, which shall grade the scanned vulnerable points in terms of risk severity and mark out the level explicitly;

c) General result report after scanning multiple targets;

d) Critical vulnerability scanning information may be generated with a summary report.

##### 7.1.3.3 Report output

The report shall be able to be output in such general file formats as PDF, DOC, HTML, etc.

##### 7.1.3.4 Result browsing

Network vulnerability scanner shall provide the function of browsing the scanning result.

##### 7.1.3.5 Suggestion on vulnerability mending

Network vulnerability scanner shall be able to propose mending suggestion for the vulnerability discovered, and the suggestion on vulnerability mending shall meet the following requirements:

a) Propose specific vulnerability mending methods targeted at different types of operating systems;

b) The vulnerability shall be described in detail, and the provided vulnerability mending methods shall ensure its rationality and availability.

#### 7.1.4 Scan configuration

##### 7.1.4.1 Scanning strategy

Network vulnerability scanner shall provide a convenient method to customize strategies, and shall be able to designate the scope of scan address, scope of port, type of vulnerability, etc.

#### 7.1.4.2 Schedule task

Network vulnerability scanner shall be able to customize scanning schedule and be able to conduct scan task by set time or periodically.

### 7.1.5 Security of scanning object

#### 7.1.5.1 Effect on performance of the network where target system locates

The scanning shall not affect the proper functioning of network.

#### 7.1.5.2 Effect on target system

The scanning shall not affect the proper functioning of target system, and shall avoid using the method of attack to test; when using some scanning measures (such test measures as DoS attack) that are potential to generate negative effects on target system, network vulnerability scanner shall give explicit prompt to target system or target system administrator prior to test.

### 7.1.6 Upgrading capability

Network vulnerability scanner shall be able to update the feature library of vulnerability:

a) The design of product architecture shall be beneficial to product upgrade and be convenient for upgrade operation;

b) Support manual or auto upgrade operation.

### 7.1.7 Scanning speed

Network vulnerability scanner shall provide a reasonable scanning speed and shall be able to regulate the scanning speed by such methods as adjusting the number of scanning threads or processes.

## 7.2 Self-security Requirements

### 7.2.1 Identification and authentication

#### 7.2.1.1 User identification

##### 7.2.1.1.1 Attribute definition

Network vulnerability scanner shall specify the security attributes corresponding to each management role, e.g., management role identification, authentication

b) Be intrinsically consistent;

c) Describe the structure of security function according to subsystems;

d) Describe the security function provided by each security function subsystem;

e) Identify any fundamental hardware, firmware or software required by security function, and one representation of the function provided by the supportive protection mechanism which is realized by these hardware, firmware or software;

f) Identify all the interfaces of security function subsystems;

g) Identify which interfaces are externally visible in security function subsystems.

#### 7.3.3.3 Informal correspondence verification

The developer shall provide correspondence analysis among all the adjacency pairs represented by product security function.

For each adjacency pair represented by product security function, the analysis shall clarify that all relevant security functions represented by relatively abstract security function shall be refined correctly and completely in relatively specific security function representation.

### 7.3.4 Instructive documents

#### 7.3.4.1 Administrator manual

The developer shall provide administrator manual which shall be kept consistent with other documents submitted for evaluation.

The administrator manual shall cover the following contents:

a) Management functions and interfaces which are accessible to administrators;

b) How to safely manage products;

c) The functions and authorities that shall be controlled in the security handling environment;

d) All assumptions of users' behaviors concerned with safe operation of product;

e) All the security parameters controlled by administrators, if possible, security values shall be indicated;

f) Every security-related event concerned with management function, including the modification of security characteristics of the entity controlled by security

b) The vulnerability of service program, including:

- Lack of legality inspection on input;
- Unable to handle abnormal conditions correctly.

c) Risk or wrong configuration of server, including:

- Allowing EXPN and VRFY commands;
- Allowing e-mail forwarding;
- Other insecure configuration.

d) Other security risks.

#### 8.1.2.3 Vulnerability of FTP service

Network vulnerability scanner shall be able to inspect the security problems of such service programs using FTP protocol, and the inspection items shall include:

a) Service program banner and version number.

b) The vulnerability of service program, including:

- Lack of legality inspection on input;
- Unable to handle abnormal conditions correctly.

c) Risk or wrong configuration of server, including:

- Allowing anonymous login;
- Using default password;
- Allowing dangerous commands;
- Other insecure configurations.

d) Other security risks.

#### 8.1.2.4 Vulnerability of Web service

Network vulnerability scanner shall be able to inspect the security problems of such programs providing Web service, and the inspection items shall include:

a) Service program banner and version number.

b) The vulnerability of service program, including:

- Lack of legality inspection on input;
- Unable to handle abnormal conditions correctly.

c) The vulnerability of scripts running on server and CGI program.

d) Risk or wrong configuration of server, including:

- File attribute error;
- Directory attribute error;
- Other insecure configurations.

e) Other security risks.

#### 8.1.2.5 Vulnerability of DNS service

Network vulnerability scanner shall be able to inspect the security problems of DNS service, and the inspection items shall include:

a) Service program banner and version number.

b) The vulnerability of service program, including:

- Lack of legality inspection on input;
- Unable to handle abnormal conditions correctly.

c) Other security risks.

#### 8.1.2.6 Vulnerability of other known TCP/IP services

Network vulnerability scanner shall be able to inspect the security problems of other service programs using TCP/IP protocol, and the inspection items shall include:

a) Service program banner and version number.

b) The vulnerability of service program, including:

- Lack of legality inspection on input;
- Unable to handle abnormal conditions correctly.

c) Error configuration of service program.

#### 8.1.2.7 Vulnerability of RPC service

Network vulnerability scanner shall be able to inspect the security problems of such service programs using RPC protocol as well as whether dangerous RPC service is

opened or not.

#### 8.1.2.8 Vulnerability of SNMP service

Network vulnerability scanner shall be able to inspect the security problems of such service programs using SNMP protocol, and the inspection items shall include:

a) Vulnerability inspection of SNMP password.

b) Inspect whether SNMP service will reveal the following sensitive information of system, including:

- TCP port table;
- UDP port table;
- Service list;
- Process list;
- Routing list;
- Network interface equipment list.

#### 8.1.2.9 Weak password

Network vulnerability scanner shall be able to inspect the robustness of system user password by method of dictionary or exhaustion, etc., inspection items shall include:

a) Whether the password of simply converted user name is used by the system;

b) Whether the easy-to-guess password is used by the system.

#### 8.1.2.10 Vulnerability of Windows operating system user, group, password, sharing and registry, etc.

Network vulnerability scanner shall be able to inspect some peculiar vulnerabilities of Windows operating system, the inspection items shall include:

a) System security settings, including:

- Access authorization setting of registry items;
- Audit policy setting;
- System password policy setting.

b) Inspections for operating system version and patch installation.

c) Other relevant inspections.

#### 8.1.2.11 Trojan horse

Network vulnerability scanner shall be able to inspect whether the default port used by common Trojan horses is open, and shall be able to conduct test and analysis for the open port obtained by scanning and to warn about unknown services and known Trojan horses.

#### 8.1.2.12 Vulnerability of NFS service

Network vulnerability scanner shall be able to inspect the vulnerability relevant to NFS service.

#### 8.1.2.13 Vulnerability of router/switch

Network vulnerability scanner shall be able to inspect the vulnerability relevant to router, switch and their startup services.

#### 8.1.2.14 Vulnerability of DoS attack

Network vulnerability scanner shall be able to conduct real attack against target host with actual attack technique so as to inspect the capability of target host to defend against known DoS attack.

#### 8.1.2.15 File sharing

Network vulnerability scanner shall be able to inspect the used NETBIOS or SMB sharing to discover dangerous settings. Inspection items shall include:

a) Important directories are shared;

b) Shared directory may be written in by anonymous user;

c) Whether the default or too-simple shared password is used;

d) Version number of SAMBA server software.

### 8.1.3 Scanning result analysis and treatment

#### 8.1.3.1 Result storing

Scanning result shall be able to be written in result database.

#### 8.1.3.2 Import and export of result

**Import and export operation of scanning result can be conducted.**

#### 8.1.3.3 Report generation

#### 8.1.4 Scanning configuration

##### 8.1.4.1 Scanning strategy

Network vulnerability scanner shall provide a convenient method to customize strategies, and shall be able to designate the scope of scan address, scope of port, type of vulnerability, etc.

##### 8.1.4.2 Schedule task

Network vulnerability scanner shall be able to customize scanning schedule and be able to conduct scan task by set time or periodically.

##### 8.1.4.3 Known account number/password scanning

**Network vulnerability scanner shall be able to carry out a much more efficient scanning for target system via its known account number/password.**

#### 8.1.5 Security of scanning object

##### 8.1.5.1 Effect on performance of the network where target system locates

The scanning shall not affect the proper functioning of network.

##### 8.1.5.2 Effect on target system

The scanning shall not affect the proper functioning of target system, and shall avoid using the method of attack to test; when using some scanning measures (such test measure as DoS attack) that are potential to generate negative effects on target system, network vulnerability scanner shall give explicit prompt to target system or target system administrator prior to test.

#### 8.1.6 Upgrading capability

Network vulnerability scanner shall be able to update the feature library of vulnerability:

a) The design of product architecture shall be beneficial to product upgrade and be convenient for upgrade operation;

b) Support manual or auto upgrade operation;

c) **Possess upgrade security measures to prevent receiving wrong or bogus product upgrade package, e.g., such measures as adopting identity authentication, digital signature and data transmission encryption, etc.**

#### 8.1.7 Scanning speed

the authentication data.

#### 8.2.1.2.3 Authentication failure handling

**Network vulnerability scanner shall provide some authentication failure handling measures (such as setting maximum login failure times, etc.) to prevent brute breaking attack against cryptogram.**

#### 8.2.1.2.4 Timeout locking or logout

**The network vulnerability scanner shall have locking or logout function for login timeout. Without any operation within the set time period, the session may be locked or terminated, and identity authentication shall be conducted again for reoperation. The maximum timeout shall only be set by authorized administrator.**

### 8.2.2 Security management

#### 8.2.2.1 Security management function

Network vulnerability scanner shall ensure the authorized administrator possessing the following management authorities:

a) Check security attributes;

b) Modify security attributes;

c) Turn on and turn off all or a part of security functions;

d) Develop and modify all kinds of security policies.

#### 8.2.2.2 Usability

Network vulnerability scanner shall be able to run stably and offer a convenient and easy-to-use management interface:

a) Provide accurate and intuitive scanning progress display to facilitate the users to know about the scanning process;

b) Scan task shall be able to be paused or terminated at any time.

#### 8.2.2.3 Role management

**Network vulnerability scanner shall be able to distinguish administrator roles:**

**a) Possess at least two types of administrator roles with different authorities, such as operator, security officer, auditor, etc.;**

**b) Shall customize all kinds of different authorization roles according to different function modules and shall be able to assign roles to**

**technical measures to detect the modification or the difference between the main copy of the developer and the version received by the user. It shall also describe how to use multiple programs to discover product delivery to the user in the disguise of the developer or when the developer does not send anything to the user.**

#### 8.3.2.3 Installation, generation and startup programs

The developer shall provide document to describe the installation, generation and startup process of the product.

### 8.3.3 Development

#### 8.3.3.1 Functional specification

##### 8.3.3.1.1 Informal functional specification

The developer shall provide one functional specification which shall meet the following requirements:

a) Describe the security function and external interface of product in informal form;

b) Be intrinsically consistent;

c) Describe the purpose and usage methods of all the external interfaces, and provide the details of effect, exceptions and error messages in due course;

d) Represent the product security functions completely.

##### 8.3.3.1.2 Well-defined external interface

**Functional specification shall cover rationality of security function represented completely.**

#### 8.3.3.2 High level design

##### 8.3.3.2.1 Descriptive high level design

The developer shall provide high level design of product security functions, which shall meet the following requirements:

a) The representation shall be informal;

b) Be intrinsically consistent;

c) Describe the structure of security function according to subsystems;

d) Describe the security function provided by each security function subsystem;

e) Identify any fundamental hardware, firmware or software required by security function, and one representation of the function provided by the supportive protection mechanism realized by these hardware, firmware or software;

f) Identify all the interfaces of security function subsystems;

g) Identify which interfaces are externally visible in security function subsystems.

**8.3.3.2.2 Security strengthened high level design**

**The security strengthened high level design provided by developer shall meet the following requirements:**

**a) Describe the purpose and usage methods of all the interfaces of products and provide the details of effect, exceptions and error messages in due course;**

**b) Describe products from two aspects: i.e. security policy implementation and other subsystems.**

**8.3.3.3 Subset of security function realization**

**The developer shall provide realization representation for the selected security function subset. Realization representation shall be unambiguous and define security function in detail so as to generate security function with no need of further design. Realization representation shall be intrinsically consistent;**

**8.3.3.4 Descriptive low level design**

**The developer shall provide low level design of security function which shall meet the following requirements:**

**a) The representation shall be informal;**

**b) Be intrinsically consistent;**

**c) Describe security function according to models;**

**d) Describe the purpose of each model;**

**e) Define the interrelationship between models according to the provided security function and the dependence to other models;**

**f) Describe how each security policy implementation function is provided;**

**g) Identify all interfaces of security function model;**

**h) Identify which interfaces are externally visible in security function model;**

**The developer shall establish one life cycle model to make necessary control over the development and maintenance of products and provide models described in the life cycle documents to develop and maintain products.**

#### 8.3.5.3 Well-defined development tools

**The developer shall clearly define the product development tools and provide unambiguous definition of each statement and the meaning of options in the development tool documents.**

### 8.3.6 Test

#### 8.3.6.1 Test coverage

##### 8.3.6.1.1 Evidence for coverage

The developer shall provide the evidence for test coverage.

It shall be shown in evidence for test coverage that the test identified in test document is corresponding to the product security function described in functional specification.

##### 8.3.6.1.2 Coverage analysis

**The developer shall provide the analysis result of test coverage.**

**The analysis result of test coverage shall show that the correspondence between the test identified in test document and the product security function described in functional specification is complete.**

#### 8.3.6.2 Test: high level design

**The developer shall provide test depth analysis.**

**The depth analysis shall demonstrate that the tests identified in the test documents are enough to prove that the function is consistent with its high level design.**

#### 8.3.6.3 Functional test

The develop shall test the security function, document the results and provide test document.

The test document shall include the following items:

a) The test plan, which shall identify the security function to be tested and describe the objective of test;

b) The test process, which shall identify the test to be executed, and describe

the test overview of each security function, including the order dependence on other test results;

c) Expected test result, which shall indicate the expected output after the success of test;

d) Actual test result, which shall indicate that each tested security function can operate as required.

#### 8.3.6.4 Independent test

##### 8.3.6.4.1 Consistency

The developer shall provide products suitable for the test and provide the same test set as those used in the product self-test.

##### 8.3.6.4.2 Sampling

The developer shall provide a group of equivalent resources for sampling test of security function.

### 8.3.7 Vulnerability assessment

#### 8.3.7.1 Misuse

##### 8.3.7.1.1 Guide review

**The developer shall provide instructive documents which shall meet the following requirements:**

**a) Identify all possible operating modes (including operation after failure and mis-operation), their consequences and the significance to secure operation maintenance;**

**b) Be complete, clear, consistent and reasonable;**

**c) List all assumptions regarding the intended use environment;**

**d) List all requirements for external security measures (including external program, physical or personnel control).**

##### 8.3.7.1.2 Analysis confirmation

**The developer shall provide analysis document to demonstrate that the instructive documents are complete.**

#### 8.3.7.2 Product security function strength assessment

The developer shall make an security function strength analysis to each security

mechanism with notice of security function strength identified in the instructive documents and explain the measurement for the security mechanism reaching or exceeding the defined minimum strength grade or specific function strength.

#### 8.3.7.3 Vulnerability analysis

##### 8.3.7.3.1 Vulnerability analysis for developer

The developer shall execute vulnerability analysis and provide vulnerability analysis documents.

The developer shall make analysis and document to all kinds of product functions from the obvious approach in which the users may damage security policy. For determined vulnerability, the developer shall explicitly record the taken measures. For each vulnerability, it shall be shown that it shall not be used in the use environment of products.

##### 8.3.7.3.2 Independent vulnerability analysis

**The developer shall provide documents to prove that the products identified with vulnerability can resist obvious penetrability attack.**

##### 8.3.7.3.3 Intermediate resistibility

**The developer shall provide documents to prove that the products can resist the penetrability attack of intermediate strength and that vulnerability searching is systematic.**

**_____ END _____**

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



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