

ICS 35.240
CCS A 90

GA

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

GA/T 403.2-2002

Replacing GA/T 403.2-2002

**Information security technology. Security technical
requirements for intrusion detection products. Part 2: Host.
based products
(English Translation)**

Issued on: March 24, 2014

Implemented on: March 24, 2014

Issued by: Ministry of Public Security

Table of Contents

Introduction	
Introduction	
1 Scope	
2 Normative references	
3 Terms and definitions	
4 Host Intrusion Detection Product Description	
5 1 Security Environment	
5.1 Hypothesis	
5.2 Threat	
5.3 2 Organization for Security Policy	
2 6 security purposes	
6.1 Product Safety Objective	
6.2 Environmental security objectives	
7 Security functional requirements	
7.1 Data acquisition function claim	
7.2 Intrusion analysis Claim	
7.3 Intrusion Response Feature Requirements	
7.4 Management Control functional requirements	
7.5 Test results processing requirements	
5 7.6 product flexibility requirements	
7.7 Authentication	
7.8 Administrators to manage	
7.9 Security Audit	
7.10 Data Security Event	
7.11 Communications Security	
7.12 8 self-protection	
7.13 8 Self-monitoring	
8 8 Security assurance requirements	
8.1 Configuration Management	
8.2 Delivery and Operation	
8.3 Development	
8.4 Guidance document	

11	8.5 Life Cycle Support
	8.6 Test
	8.7 Vulnerability assessment
9	Basic principles of technical requirements
9.1	Security functional requirements Fundamentals
9.2	Security assurance requirements 15 Fundamentals
10	Classification of claim
10.1	Overview
10.2	Classification of security functional requirements
10.3	Classification of security assurance requirements

Foreword

GA/T 403 "information security technology intrusion detection product safety technical requirements" is divided into two parts.

--- Part 1. network products;

--- Part 2. Host products.

This section GA/T 403 Part 2.

This section drafted in accordance with GB/T 1.1-2009 given rules.

This Part replaces GA/T 403.2-2002 "IT intrusion detection products safety - Part 2. Host-based production Goods ", compared with the GA/T 403.2-2002 main technical changes are as follows.

--- Standard name was changed to "information security technology intrusion detection products safety - Part 2. Host products";

--- Increased Host-based intrusion detection product description (see Chapter 4);

--- Increase the security environment, including the assumptions, threats and organizational security policies (see Chapter 5);

--- Increased security purposes, including the purpose of product safety and environmental safety purposes (see Chapter 6);

--- Remove the host intrusion detection product performance requirements (see the 2002 edition, Chapter 7);

--- Deleted the database support (see the 2002 version of 6.1.5.5);

--- Modify the content of security functional requirements (see Chapter 7, Chapter 8, 2002

edition);

--- Increase the technical requirements of the basic principles, including the basic principles of security functional requirements and security assurance requirements for the basic principles (see Chapter 9).

Please note that some of the content of this document may involve patents. Release mechanism of the present document does not assume responsibility for the identification of these patents.

This part is proposed by the Ministry of Public Security Network Security Protection Agency.

This part of the jurisdiction of the Ministry of Public Security Information System Standardization Technical Committee.

This section drafted by. Ministry of Public Security of Computer Information System Security Product Quality Supervision and Inspection Center, Blue Shield Information Security Technology Co. Shares Companies, Third Institute of Ministry of Public Security.

Introduction

GA/T in this part 403 is described in detail with the host intrusion detection products safe environment-related assumptions, threats and organizational security policies Strategy, defines the destination host intrusion detection security products and supporting environment, demonstrated by the basic principles of security functional requirements and can be traced back Products covered security purposes, for security purposes can be traced back cover and secure environment-related assumptions, threats and organizational security policies.

This section basically level with reference to the GB/T 18336.3-2008 prescribed level EAL2 security assurance requirements, and enhance the level at EAL4 level Security assurance requirements based on the vulnerability analysis requires upgrade to an attacker can withstand moderate attack potential attack.

This section only gives a Host-based intrusion detection products should meet the technical requirements of safety, but for Host-based intrusion detection products of specific skills Art implementations, a method is not required.

Information Security Technology Intrusion detection products safety technical requirements
Part 2. Host-based products

1 Scope

GA/T 403 provisions of this part of the Host-based intrusion detection products, security functional requirements, security assurance requirements and grading requirements.

This section applies to the design, development and testing Host-based intrusion detection products.

2 Normative references

The following documents for the application of this document is essential. For dated references, only the dated version suitable for use herein Member. For undated references, the latest edition (including any amendments) applies to this document.

GB 17859-1999 computer information system security protection classification criterion
GB/T 18336-2008 (all parts), Information technology - Security techniques - Information Technology Security Evaluation Guidelines GB/T 25069-2010 Information security technology terms

3 Terms and Definitions

GB 17859-1999, terms and definitions GB/T 18336-2008 (all parts) and GB/T 25069-2010 defined apply this document.

4 Host Intrusion Detection Product Description

Host-based intrusion detection products to system logs, application logs as a data source, or by other means (such as monitoring systems tune Use) to collect information from the target host on the analysis, which found abnormal behavior Intrusion Detection System. Host-based intrusion detection products through Often as a standalone version, installed on the monitored host.

5.1 Suppose

Host-based intrusion detection products related assumptions security environment as shown in Table 1.

Table 1 is assumed

If the name is assumed Description Physical access Product processing resources should be limited within controlled access to devices to prevent unauthorized physical access. All implementation of product safety Full policy-related hardware and software shall be protected from unauthorized physical changes Human capacity authorized administrator is harmless, well-trained, and follow the Administrator's Guide