Chinastandards.org

ICS 03.120.20
CCS A 00

RB

CERTIFICATION AND ACCREDITATION INDUSTRY STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

RB/T 205-2014

Security evaluation specifications for anti-denialrof-service system

抗拒绝服务系统安全评价规范

(English Translation)

Issued on: August 20, 2014 **Implemented on: March 1, 2015**

Issued by: National Certification and Accreditation Administration

Preview: page 1 of 4 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/rb-t-205-2014

Chinastandards.org

Table of Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms, definitions and abbreviations

3.1 Terms and definitions

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard is proposed and managed by the National Certification and Accreditation Administration.

This standard was drafted. China Information Security Certification Center, Shanghai Information Security Evaluation and Certification Center, Anhui Zhongxin Software Co., Ltd.

Introduction

This standard proposes anti-denial service according to GB/T 18336 "Information Technology Security Technology Information Technology Security Evaluation Criteria" the evaluation methods of the system's functional requirements, safety requirements, performance verification requirements and assurance requirements. At the same time, this standard gives the factory Quality assurance capabilities and product consistency requirements.

GB/T 18336 "Information Technology Security Technology Information Technology Security Evaluation Criteria" is the evaluation object (TOE) design and development and the basic criteria for assessing safety, giving general information on TOE's information technology, security technology and information security technology security assessment begging. This standard refers to GB/T 18336, combined with the specific characteristics of the anti-denial service system, select the safety function requirements of GB/T 18336.2 Some of the components in the assessment as safety requirements; select all components of the EAL2 level in the GB/T 18336.3 security assurance requirements to ensure the required assessment content.

The significance of the development of this standard is that it is beneficial for the certification body and testing organization to conduct detection, evaluation and certification

Preview: page 2 of 4 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/rb-t-205-2014

against the denial of service system.

It is beneficial for enterprises to refer to the use of anti-denial service system design and implementation.

Anti-denial service system security evaluation specification

1 Scope

This standard specifies the evaluation methods for anti-denial service systems, including functional, safety, performance verification and security assurance requirements.

This standard applies to the testing, evaluation and certification of anti-denial service systems. The design and implementation of anti-denial service systems can also be used.

2 Normative references

The following documents are indispensable for the application of this document. For dated references, only dated versions apply to this article.

Pieces. For undated references, the latest edition (including all amendments) applies to this document.

GB/T 18336 (all parts) Information technology security technology information technology security assessment criteria (ISO/IEC 15408) GB/T 25069 Information Security Technical Terminology

3.1 Terms and definitions

The following terms and definitions established in GB/T 18336 and GB/T 25069 apply to this document.

3.1.1

Denial of service attack A denial of service attack, a DoS attack. An attack that causes a denial of service is called a denial of service attack.

3.1.2

Anti-denial-of-service system Hardware devices or hardware and software combinations against denial of service attacks, by monitoring and controlling incoming and outgoing data streams, timely discovering background traffic Various types of denial of service attacks, filtering or bypassing attack traffic to ensure the passage of normal traffic and achieving denial of service attacks the protective effect of the blow.

3.1.3

Throughput the ability of the anti-denial service system to forward data without packet loss,

Preview: page 3 of 4 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/rb-t-205-2014

generally in percentage of the line speed (or rate) to represent.

3.1.4

Traffic traction trafficredirection the bypass deployment mode separates attack traffic from normal traffic, and the anti-denial service system specifically resists denial of service attacks.

A process that guarantees normal traffic as much as possible without being disturbed by an attack.

3.1.5

Bypass

Through a specific trigger state (power failure or crash), the two networks do not pass through the system of the network security device, and are directly physically turned on.

3.1.6

Document review document review refers to the information and documents submitted by the certification body to the applicant, and is reviewed according to the product technical specifications.

Preview: page 4 of 4 shown, 19 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/rb-t-205-2014