

ICS 35.240
CCS A 90

GA

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

GA/T 1137-2014

**Information security technology. Security technical
requirements for Anti-DoS attack products**

信息安全技术 抗拒绝服务攻击产品安全技术要求

(English Translation)

Issued on: March 10, 2014

Implemented on: March 10, 2014

Issued by: Ministry of Public Security

Table of Contents

- Introduction
- Introduction
- 1 Scope
- 2 Normative references
- 3 Terms and definitions
- 4 Anti-denial of service attacks Description
- 5 2 Security Environment
- 5.1 Hypothesis
- 5.2 Threat
- 5.3 3 Organization for Security Policy
- 6 Security objectives
- 6.1 Product Safety Objective
- 6.2 Objective 4 Environmental Safety
- 7 Security functional requirements
- 7.1 Denial of Service attacks Recognition

Foreword

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

This standard was proposed by the Ministry of Public Security Network Security Protection Agency.

This standard is under the jurisdiction of the Ministry of Public Security Information System Standardization Technical Committee.

This standard was drafted. Ministry of Public Security of Computer Information System Security Product Quality Supervision and Inspection Center, the new software Anhui Co., Beijing China Information Security Technology Co., Ltd. Green League, Third Institute of Ministry of Public Security.

Introduction

This standard describes in detail the anti-denial of service attacks and environment-related product safety assumptions, threats and organizational security policies defined resistance Service attack products and their supporting environment for security purposes, by the

basic principles of security features require proof cover product safety and traceability Purpose, safety purpose and can be traced back cover environment-related security assumptions, threats and organizational security policies.

The standard base-level reference to 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 standard only gives the anti-denial of service attacks products should meet the technical requirements of safety, but the denial of service attacks against specific product technology Art implementations, a method is not required.

Information Security Technology Anti-DoS product safety technical requirements

1 Scope

This standard specifies the security features against denial of service attacks product requirements, security assurance requirements and grading requirements.

This standard applies to reject anti-design, development and testing services attacks 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/T 5271.8-2001 Information technology - Vocabulary - Part 8. Security 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

3 Terms and Definitions

GB/T 5271.8-2001, GB 17859-1999 and GB/T 18336-2008 (all parts), and the definition of the following terms and Definitions apply to this document.

Denial of service attacks denialofserviceattack A network attack, by constructing a specific network service request, aimed at using excessive bandwidth or server resources, so that it He could not get the normal service request response.

Anti-DoS product Anti-DoSattackproduct Denial of service attacks to identify and intercept, thereby reducing its hazardous products.

ping of death attack by sending maliciously crafted ICMP packets lead to a large target

server crash.

Teardrop attack by sending maliciously crafted overlapping offset data packets lead to a target server crash.

UDP flood attack UDPfloodattack by sending a large number of UDP packets bandwidth or server resources of an attack.

syn flood attack TCP handshake by sending a large number of the first packet message, causing the target server runs out of resources and can not respond to normal please