Chinastandards.org

ICS 35.240
CCS A 90

GA

INDUSTRY STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GA/T 698-2014

Replacing GA/T 698-2007

Information security technology. Technical requirements for information filtering products

信息安全技术 信息过滤产品技术要求

(English Translation)

Issued on: March 24, 2014 **Implemented on: March 24, 2014**

Issued by: Ministry of Public Security

Preview: page 1 of 5 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-698-2014

Chinastandards.org

Table of Contents

Introduction
Introduction
1 Scope
2 Normative references
3 Terms and definitions
4 Abbreviations
Information filtering Product Description 1
2 6 Security Environment
6.1 Hypothesis
6.2 Threat
6.3 3 Organization for Security Policy
7 Security objectives
7.1 Product Safety Objective
7.2 Objective 4 Environmental Safety
8 Security functional requirements
8.1 Protocol identification
8.2 Application filtering
8.3 Policy Applications
8.4 Identification and authentication
8.5 Identification of failure handling
8.6 Lock timeout or cancellation
8.7 Safety Support System
8.8 Administrator permissions
8.9 Remote Management Security
8.10 Audit Logs
8 9 Security assurance requirements
9.1 Configuration Management
9.2 Delivery and Operation
9.3 Development
9.4 Guidance document
11 9.5 Life Cycle Support
9.6 Test

Preview: page 2 of 5 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-698-2014

9.7 Vulnerability assessment
10 Basic principles of technical requirements
10.1 13 basic principles of security functional requirements
10.2 13 basic principles of security assurance requirements
11 Classification requirements
11.1 Overview
11.2 Classification of security functional requirements
11.3 Classification of security assurance requirements

Foreword

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

Instead of the standard GA/T 698-2007 "information security technology filtration products information security functional requirements." And GA/T 698-Compared to 2007, the main technical changes are as follows.

--- Standard name changed to "information security technology information filtering products technical requirements" (see cover, the cover of the 2007 edition);

--- Increased abbreviations (see Chapter 4);

--- Increasing the information filtering product description (see Chapter 5);

--- Increase the security environment, including the assumptions, threats and organizational security policies (see Chapter 6);

--- Increased security purposes, including the purpose of product safety and environmental safety purposes (see Chapter 7);

--- Added "Policy Applications" requirements (see 8.3);

--- Increase the "identification and authentication" requirements (see 8.4);

--- Added "Remote Management security" requirements (see 8.9);

--- Increased security assurance requirements (see Chapter 9);

--- 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 paragraph 10 chapter);

--- Deleted "links Information filtering" requirements (see the 2007 version 4.1.5);

--- Delete the words "search engine filtering" requirements (see the 2007 version 4.1.6);

--- Remove the "black list, white list" of requirements (see the 2007 version 4.1.8);

Preview: page 3 of 5 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-698-2014

--- Deleted "TELNET information filtering", "instant message filtering" and "chat filtering" requirements (see the 2007 edition the 4.4.2,4.4.4,4.4.5).

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 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, Ministry of Public Security Network Security Protection Agency, square N Information Industry Holdings Co., Ltd. Blue Shield Information Security Technology, Third Institute of Ministry of Public Security.

Introduction

This standard is described in detail and product safety information filtering environment-related assumptions, threats and organizational security policies defined filtering capacity Security purposes product and its supporting environment, demonstrated by the basic principles of security functional requirements and be able to trace the products covered by security purposes, security purposes it can be traced back cover and secure environment-related 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 information filtering products should meet the technical requirements of security, but filtration products for information specific technical implementation, party Method is not required.

Information security technology information filtering technical requirements

1 Scope

This standard specifies the information filtering product security functional requirements, security assurance requirements and grading requirements.

This standard applies to information filtering product design, development, and testing.

Preview: page 4 of 5 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-698-2014

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 Abbreviations

The following abbreviations apply to this document.

FTP. File Transfer Protocol (FileTransferProtocol) HTTP. Hypertext Transfer Protocol (HypertextTransferProtocol) IM. Instant Messaging (InstantMessenger) IP. Internet Protocol (InternetProtocol) MAC. MAC (MediaAccessControl) POP3. Post Office Protocol Third Edition (PostOfficeProtocol3) SMTP. Simple Mail Transfer Protocol (SimpleMailTransferProtocol) TELNET. Telnet (TelecommunicationNetwork) URL. Uniform Resource Locator (UniversalResourceLocator)

5 Information Filtering Product Description

This standard defines the information filtering products is through the analysis of network data communications, focusing on the network for HTTP, FTP and mail and other application-layer protocols one or more real-time analysis, according to pre-defined rules to filter its content and interception.

Information filtering products are generally located between the access client and the target server, the inflow or outflow of information filtering policies were defined Control and protect critical data and information filtering product itself inside. The product is typically deployed in bypass mode or tandem guest access the client lies at the outlet of the network.

Preview: page 5 of 5 shown, 15 in the full document. Complete English PDF, instant download:
https://chinastandards.org/standards/ga-t-698-2014