GB

NATIONAL STANDARD OF THE

PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GB/T 43696-2024

Cybersecurity Technology - Zero Trust Reference Architecture

网络安全技术 零信任参考体系架构

Issued on: April 25, 2024 **Implemented on: November 1, 2024**

Issued by: State Administration for Market Regulation;

Standardization Administration of the People's Republic of China.

Table of Contents

Cybersecurity Technology - Zero Trust Reference Architecture

1 Scope

This document specifies the zero trust reference architecture and describes the subject, resources, core components and supporting components, as well as their correlations.

This document is applicable to the planning, design, development, application and evaluation of information systems that adopt the zero trust architecture.

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through the normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 25069 Information Security Techniques - Terminology

3 Terms and Definitions

The terms and definitions defined in GB/T 25069 and the following are applicable to this document.

3.1 zero trust

A network security philosophy with resource protection as the core.

NOTE: this philosophy holds that when a subject accesses a resource, regardless of whether the subject and the resource are trustworthy, the trust relationship between the subject and the resource needs to be built from scratch through continuous status perception and dynamic trust evaluation to implement end-to-end secure access control.

3.2 zero trust architecture

Information system architecture established based on zero trust.

NOTE: it includes system components that constitute the architecture, as well as the relations among the components.

3.3 subject

The entity that initiates the access request.

3.4 resource

The object accessible to the subject.

4 Typical Features

The zero trust architecture has the following typical features.

a) Continuous status perception:

Continuously collect relevant information on the subject, resources and the environment, and analyze the security situation.

b) Dynamic trust evaluation:

In the process of the subject accessing resources, in accordance with the changes in the security situation of the subject, resources and the environment, etc. that are continuously perceived, trust evaluation is continuously performed to maintain or change policy decisions.

c) Minimum authority:

In accordance with the task requirements and policy decisions, combined with the time window and the granularity of the accessed resources, the minimum authority is granted to the accessing subject.

d) Encrypted transmission:

Adopt cryptographic technology to establish an end-to-end data security channel for the subject to access resources.

5 Reference Architecture

The zero trust reference architecture consists of subject, resources, core components and supporting components, as shown in Figure 1.

6 Core Components

6.1 Policy Decision Component

The policy decision component consists of a policy engine and a policy manager, and its main functions are as follows.

a) Policy engine: responsible for determining the subject's access rights to resources. Based on the information provided by the security policy and the supporting components, it continuously performs trust evaluation, and makes access control decisions of permission, rejection or revocation.

b) Policy manager: responsible for issuing control commands for the connection between the subject and the resources. Relying on the access control decisions made by the policy engine, it issues a command to the policy execution component to establish, maintain or block the data security channel.

6.2 Policy Execution Component

The policy execution component implements identity authentication and controls the data security channel between the subject and the resources under the management of the policy decision component.

a) Identity authentication: in accordance with the command of the policy decision component, it coordinates with the supporting components to implement identity authentication for the subject.

b) Control of data security channel: in accordance with the command issued by the policy manager, it starts, monitors and terminates the data security channel between the subject and the authorized resources.

7 Supporting Components

7.1 Task Management Component

Coordinate the subject's purpose of access, drive the subject's task of accessing resources, including task objectives, task responsibilities and task processes, etc., link up entity access rights, and provide associated task lifecycle management services, collaborative services on task and resource access rights, task approval services, task identification services, task audit services and task-related information for the subject, resources, core components and other supporting components, including subject task attribute information, resource task attribute information, task status information, task approval information and task audit information, etc.

7.2 Identity Management Component

Provide entity identity management services, entity identity attribute association services,

personal entity identity authentication services, device identity authentication services, entity access rights management services and identity-related information for the subject, resources, core components and other supporting components, including entity identity identification, entity identity information, entity attribute information, entity access rights information, etc.

7.3 Resource Management Component

Provide data resource management services, device resource management services, network resource management services, computing resource management services, application resource management services, resource entity identity authentication services, resource attribute association services, resource business collaborative management services and resource-related information, resource rating and classification information, device configuration information, resource identity information, resource access rights information, resource access context information, etc. for the subject, resources, core components and other supporting components.

Resource management takes resource unit as the smallest unit, and several resource units are combined into the accessed resource. Resource units are associated with the same resource identifier, have unified resource attributes, and implement common security policies.

7.4 Environment Perception Component

During the process of the subject accessing resources, by collecting network traffic, asset information, logs, vulnerability information, user behavior, threat information and other data, the network behavior and user behavior in the process of accessing are analyzed to obtain, understand, trace back, and display the status changes and trends of the subject, resources and access environment for the subject, resources, core components and other supporting components.

7.5 Cryptographic Service Component

Ensure the authenticity of the entity identity of the subject, resources, core components and other supporting components, the confidentiality and integrity of the data, and the non-repudiation of the operation behavior, and provide cryptography-related network and communication security services, equipment and computing security services, application and data security services for the subject, resources, core components and other supporting components.

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

------ The End ------