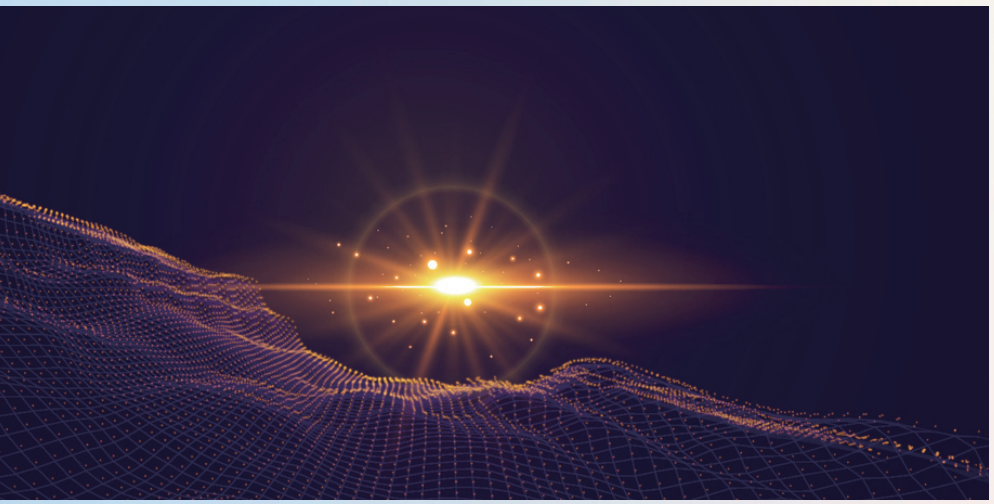

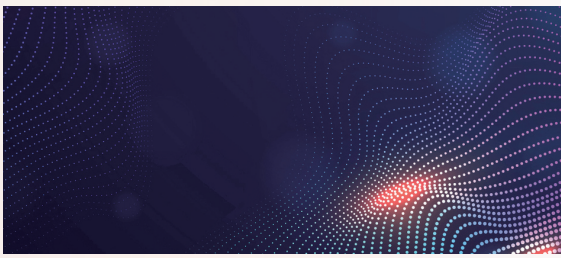

零信任安全架构研究综述

张泽洲　王　鹏　/　奇安信集团

【摘　要】本文首先对零信任安全的背景、定义及发展历史进行介绍。在总结相关零信任安全参考架构的基础之上，提出通用体系架构模型，并分析其依赖的关键技术。然后，基于零信任原则设计、规划低耦合高内聚的能力叠加模型，适配各类具有代表性的零信任安全应用场景。同时，通过引入成熟度模型，完成零信任的落地实施指引。

【关键词】零信任　身份安全　访问控制　访问代理　信任评估

【中图分类号】TP309　　【文献标识码】A

1 引言

随着企业数字化转型的深入，各企业的网络结构日趋复杂并且向云转化，以往基于边界的网关型身份和访问控制体系难以应对新型威胁；网络接入模式也更加多元化，移动办公、远程接入、云服务等场景在后疫情时代成为新常态，这大大增加了管理和维护的难度与成本。当企业以传统安全防护理念应对安全风险暴露出越来越多问题时，零信任理念为我们提供了新的安全思路。

零信任的最早雏形源于耶利哥论坛[1]。弗雷斯特咨询公司（Forrester）前分析师约翰·金德瓦格以“从不信任，始终验证”思想正式提出“零信任”这个术语，明确零信任架构的理念[2]，改进了在耶利哥论坛上讨论的去边界化的概念，认为所有网络流量均不可信，应该对访问任何资源的所有请求实施安全控制。谷歌公司基于这一理念启动了BeyondCorp项目实践，阐述了如何为谷歌内部员工构建零信任架构[3]，并陆续发表多篇研究成果论文。BeyondCorp项目的出发点在于针对企业物理边界构建的安全控制已经不足以应对攻击威胁，需要把访问控制从边界迁移到每个用户和设备。国际组织云安全联盟（CSA）在零信任理念的基础上提出了软件定义边界（Software Defined Perimeter，SDP）网络安全模型，并发布了SDP标准规范1.0[4]，进一步推动零信任从概念走向落地。高德纳（Gartner）发布自适应安全架构3.0：持续自适应风险与信任评估模型（Continuous Adaptive Risk and Trust Assessment，CARTA）[5]并提出零信任是实现CARTA宏图的初始步骤；紧接着发布了融合SDP安全模型的零信任网络访问（Zero Trust Network Access，ZTNA）概念[6]，对零信任在访问接入与访问方面的实践进行了研究。后延展为安全访问服务边缘（Security Access Service Edge，SASE）[7]，为新IT环境提供了一种管理风险和评估信任的框架。SASE可以理解为零信任的一种表现形式。Forrester提出的零信任扩展框架（Zero Trust eXtended，ZTX）[8]，则将零信任从网络层面扩展到了人员、设备、工作负载和数据，将能力从微隔离扩展到可视化、分析、自动化编排等。零信任边缘（Zero Trust Edge，ZTE）[9]模型则是在ZTX的基础上发展而来，与Gartner的SASE模型相似，但在实施路线与耦合程度上有区别。美国国家标准技术研究院（NIST）制定编写并发布的特别出版物《零信任架构》[10]，被业界认为是零信任架构的标准。

综合分析零信任的发展，不难看出零信任安全的本质是以身份为基石的动态可信访问控制，聚焦身份、信任、业务访问和动态访问控制等维度的安全能力，基于业务场景的人、流程、环境、访问上下文等多维因素，对信任进行持续评估，并通过信任等级对权限进行动态调整，形成具备较强风险应对能力的动态自适应安全闭环体系。零信任能够有效应对企业数字化转型过程中的安全痛点，适配各类远程接入场景，发挥零信任安全作用和优势。本文从零信任基本原则、安全架构、核心组件、关键技术等方面阐明零信任安全理念及内涵。最后，基于零信任的应用场景化分析，探讨零信任低耦合高内聚的能力叠加模型、零信任成熟度模型，为零信任落地提供指引。

2 基本概念

2.1 假设

在《零信任网络》一文中，零信任

的定义建立在5个基本假设之上[11]。假设网络中存在威胁，在默认情况下网络内部和外部的任何人、设备、系统的信任度与网络位置无关，需要基于认证和授权重构访问控制的信任基础。

2.2 定义

NIST在《零信任架构》中指出，传统安全方案对授权用户开放了过多的访问权限。零信任的首要目标就是重建信任，基于身份实现细粒度的访问控制，解决越权访问的风险。对零信任安全做了如下定义：零信任安全提供一系列概念、理念、组件及其交互关系，以便消除针对信息系统和服务进行精准访问判定所存在的不确定性。此定义指出了零信任需要解决的关键问题：消除对数据和服务的未授权访问，强调了需要进行细粒度访问控制的重要性。

2.3 运行机制

结合NIST的《零信任架构》的抽象访问模型和组件架构，张宇、张妍对零信任的运行机制所包含的4个步骤进行了描述[12]。在零信任模型中，会为资源访问者制定和维护基于风险的动态策略，并建立一个系统来确保这些策略得到正确和一致地执行，并不断通过反馈机制，对策略进行动态调整。

3 架构

3.1 架构原则

零信任的原则可以理解为企业采用零信任和实施零信任架构的一套基本准则。核心原则的所有要素都必须符合业务战略和组织文化。

美国国防部的《零信任参考架构》在原则阐述中[13]假设环境中存在安全危险，存在恶意的攻击者，环境中的用户、设备、网络都视为不受信任，与其所处的网络位置无关。所以访问主体对数据源和计算服务的访问请求，默认情况下是被拒绝的。英国国家网络安全中心在《零信任架构设计原则》[14]中将身份理解为唯一可以代表用户（人）、服务（软件过程）或设备，因此需要在充分了解访问主体用户、设备和服务的身份，掌握其安全状况后，即确定访问主体身份的信任等级，进行身份验证。

再依据对其访问的资源本身的属性，授予最小访问权限，且访问权限由访问主体身份和请求资源的可观测状态上下文的动态策略决定。这在NIST《零信任架构》的原则中得到了表述。我国的零信任团体标准《零信任系统技术规范》[15]，做了更为具象化的表达：策略是一系列基于企业分配给身份、资源的访问规则集。资源访问和操作权限策略可以根据资源、数据的敏感性而变化，且在访问过程中要保证通信的安全、可靠，进行持续验证与授权。

最后，要尽可能收集资源、网络基础设施、通信的安全状态信息及其他可能影响访问策略等信息，通过分析这些信息来进行持续的评估和安全响应。

因此，基于对已有零信任原则的分析，我们总结出如下原则。

原则1：任何访问主体，在访问任何资源前，都应经过身份认证和授权，与所处的网络位置无关。

原则2：持续评估所有参与对象的

安全状况。

原则3：对每一个访问请求构建安全通道。

原则4：对访问主体的权限分配遵循最小权限和动态策略的原则。

3.2 相关参考架构

NIST给出的架构接近ISO国际标准中经典的访问管理架构（Access Management，AM），将访问控制分为策略决策点（Policy Decision Point，PDP）和策略执行点（Policy Enforcement Point，PEP）。用户或计算机在访问企业资源时，需要通过策略决策点（PDP）和策略执行点（PEP）授予访问权限。零信任架构下，资源访问控制策略不再仅基于网络位置，而是基于风险。在NIST-NCCoE的零信任架构实现[16]中，给出了一个基于标准实现的零信任架构。美国国防部《零信任参考架构》给出的零信任架构，则明确了零信任架构的运行机制、组成元素及实施阶段。

3.3 通用体系架构模型

综合NIST、美国防部的零信任参考架构、其他业界模型[4-9]，以及实践经验，我们认为目前业界对零信任架构的理解正在趋于一致，总结通用零信任架构，如图1所示。

（1）访问主体

访问主体是指主动发起资源访问行为的人员、设备、应用、系统。

（2）访问客体

访问客体是指由企业控制并受零信任系统保护的应用程序、数据、文档或工作负载。将所有的数据源和计算服务都视为“资源”。

（3）可信代理

可信代理作为零信任架构的数据平面的组件，是动态访问控制能力的策略执行点。可信代理通过动态访问控制引

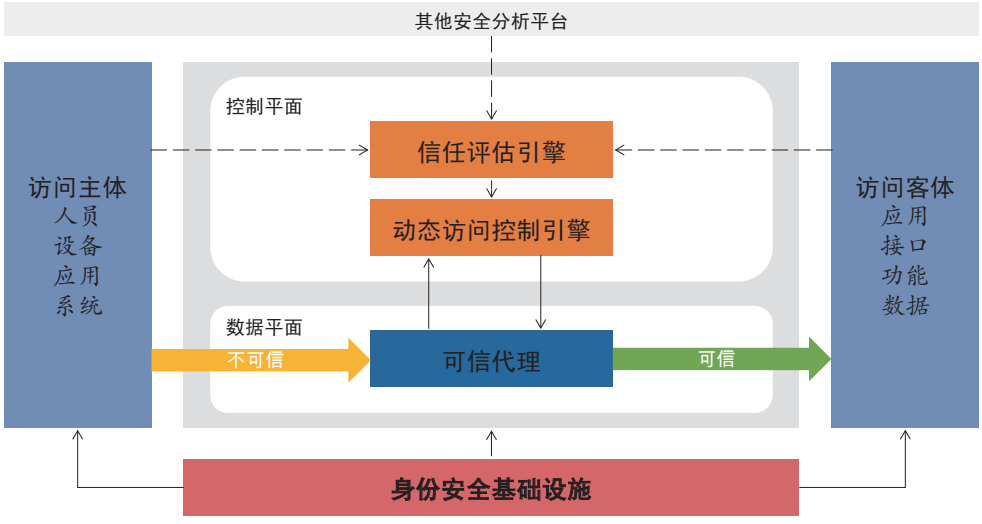

图1 通用零信任架构

擎对访问主体进行认证，对访问主体的权限进行动态判定。同时，可信代理需要对所有的访问流量进行加密。

（4）动态访问控制引擎

动态访问控制引擎和可信代理联动，对所有访问请求进行认证和动态授权。动态访问控制引擎的权限判定既可基于简单的静态规则，也可基于上下文属性、信任等级和安全策略进行动态判定。动态访问控制进行权限判定的依据是身份库、权限库和信任库。

（5）信任评估引擎

信任评估引擎作为零信任架构中实现持续信任评估能力的核心组件，提供信任等级评估能力。信任评估引擎接收可信代理、动态访问控制引擎的日志信息，结合身份库、权限库数据，以及外部安全信息源数据，对主体信任持续评估，为动态访问控制引擎提供决策依据。

（6）身份安全基础设施

身份安全基础设施作为实现零信任架构以身份为基石能力的关键支撑组件，至少包含身份管理和权限管理功能组件。它通过身份管理实现各种实体的身份化及身份生命周期管理，而通过权限管理可对授权策略进行细粒度的管理和跟踪分析。

（7）数据平面和控制平面

数据平面完成各场景、不同层次数据流量的统一代理，按照受保护资源的不同，可以是物理化设备、虚拟化设备，也可以以容器、插件等形态存在。

控制平面负责对数据面进行动态访问控制。控制平面的核心组件分为访问控制组件、环境感知组件、身份分析组件等。

4 核心技术

4.1 身份安全

身份安全提供身份管理、身份认证和授权能力，作为零信任的技术组件之一，对应零信任架构的“身份安全基础设施”。

（1）身份管理

身份管理是对身份数据的管理。身份管理包含身份识别、数据同步、身份存储、密码管理、特权管理等能力，覆盖了身份全生命周期管理、身份属性自定义、电子身份唯一化、电子身份自动化等方面。

（2）身份认证

身份认证技术是确认操作者真实身份过程中使用的方法或手段[17]。在零信任安全模型下，对用户访问行为的监控是持续进行的，能够根据用户的行为实时调整策略。因此，基于公钥密码算法的身份认证技术仍将被广泛应用的同时，多因子认证、动态认证等身份认证技术会更多地被采用[18]，并且在全面身份化的背景下，物联网设备大多采用基于区块链的认证技术[19]。

4.2 访问代理

零信任访问代理融合了传输加密、业务隐藏、访问代理、流量检测等技术。

（1）传输加密

对业务访问流量进行加密，保证数据通信安全，有效抵抗中间人攻击。

（2）业务隐藏

融合SDP的端口隐藏技术，可以对应用资源和服务进行“端口隐藏”。

（3）全场景的访问代理

零信任访问代理需要支持Web访问流量转发、网络层流量转发、API调用转发等使用场景。

（4）流量检测

检测、认证、授权所有访问流量。

4.3 访问控制

零信任架构的核心即对资源的访问控制。访问控制是通过某种途径显式准许或限制主体对客体访问能力及范围的一种方法，其目的在于限制用户的行为和操作。当前应用比较广泛的访问控制技术包括基于角色的访问控制（Role-Based Access Control，RBAC）和基于属性的访问控制（Attribute-Based Access Control，ABAC）[12]。零信任模型下，需要解决对用户的最小化授权、动态授权控制等问题。现有的零信任实现方案虽有采用RBAC模式，但多基于ABAC实现，也有采用了RBAC和ABAC结合的授权方式，即基于策略的访问控制（Policy Based Access Control，PBAC）[20]，既兼顾RBAC的简单、明确的特性，也具备ABAC的灵活性，实现了基于主体属性、客体属性、环境风险等因素的动态授权。

4.4 信任评估

持续信任评估是零信任体系从零开始构建信任的关键手段。通过建立包含信任评估模型和算法的信任评估引擎，实现基于身份的信任评估能力。同时利用环境感知技术，获取终端环境及身份的信任评分，结合身份属性信息，对访问的上下文环境进行风险判定，对访问请求进行异常行为识别，并对信任评估结果进行调整，覆盖“运行态”访问安全。当访问上下文和环境存在风险时，需要对访问权限进行实时干预，并评估是否需要对访问主体的信任降级。

美国国防部在《零信任参考架构》中将信任算法分为基于条件的评估、基于分值的评估、基于独立请求信息的评估和基于上下文的评估 。理想情况下，零信任架构应采用上下文相关的信任算法。但在定义和实现信任算法时，必须根据应用场景，平衡安全性、可用性和成本效益。

5 应用场景

任何企业环境都可基于零信任原则来设计规划。根据用户类型、终端类型、数据敏感程度等各典型业务场景，在零信任参考架构的指引下，通过低耦合高内聚[21]的能力叠加建设，将零信任架构的控制平面、数据平面分别由不同的零信任组件逐步叠加，应用于远程访问、大数据平台的数据交换、物联网泛终端接入[22]等现代IT场景。

5.1 低耦合高内聚能力叠加和场景扩展

（1）数据平面纵深扩展

数据平面对不同粒度的受保护资产，以不同形态、层次、能力实施保护措施，各层数据平面均具备水平扩展能力，可与具体场景层级深度结合，并能结合新兴场景、实际需求进行持续演进，解决用户在访问应用、数据交换、工作负载、物联网接入等场景下，收缩暴露

面、保护资产、访问控制的安全诉求。

（2）控制平面水平扩展

控制平面的核心组件具有高度的一致性，控制平面具备统一控制调度能力，即对于数据平面统一的控制能力、管理能力、分析能力。零信任架构除了自身能力构建，还需同时具备完整的开放性，通过OpenC2、Restful API等通用协议接口与外部进行信息交互、完成策略与指令控制。

5.2 远程访问

远程访问场景，可细化为业务、办公远程访问、开发测试、特权运维、面向用户的公共访问等几类场景。该场景是通过在主体和客体之间的访问路径上构建完整的信任链，实现访问控制过程的安全可控。对远程接入的用户和设备实施身份验证和持续授权，解决远程安全接入、动态授权和可控业务访问的问题。

5.3 大数据平台的数据交互

大数据平台主要的数据交互场景有两类：一类是用户或者外部系统通过数据中心网络出口访问内部系统数据；另一类是大数据平台内部工作负载之间交互。

（1）外部数据出入交换

在大数据平台的外部设置安全接入区，部署API代理控制服务，所有外部数据的交换都通过安全接入区才能访问，实现内部、外部用户和应用对于大数据平台API服务的安全接入，并且可根据访问主体实现细粒度的访问授权。

（2）内部工作负载交互

使用微隔离的技术手段实现服务器之间的隔离，一个服务器访问另一个服务器资源时需要进行身份认证。解决传统环境、虚拟化环境、混合云环境下内部流量的识别与访问控制问题。

5.4 物联网泛终端接入

在物联网实施零信任安全，是通过部署边缘物联接入管理设备，建立物联设备标识管理机制，生成由主体属性、环境属性和客体属性构成的物联设备身份指纹，建立物联设备安全基线库。持续主动扫描、被动监听检测、安全接入控制区等方式，解决终端的身份认证和访问控制。允许身份可信、经过动态授权的物联设备入网，并对物联终端进行持续信任评估、访问控制，解决物联终端的身份仿冒和恶意访问。

6 落地实施

零信任安全是一个持续进化的过程[23]，实施零信任安全也是一个长期的过程，而不是全面替换基础设施或流程。在这个过程中，零信任安全会遵循零信任成熟度模型，将其作为辅助工具，从制定零信任规划开始，技术性地开始零信任战略分析和实现。企业应寻求逐步实施零信任的原则、流程变革和技术解决方案，以保护其最高价值的数据资产。

6.1 零信任成熟度模型

美国技术委员会工业咨询委员会的成熟度模型[24]将零信任规划的实施阶

段分为5个阶段，对应用户信任、设备和活动可视性、设备可信、自适应策略、零信任5个能力实现阶段，每个阶段的内容是相互递进的，下一级是上一级项目内容的实施基础。但是，在项目实施时，不是按照完成一个阶段才开始第二个阶段，而是采用百分比评估标定，对每个阶段项目进行评估、跟踪。美国国防部《零信任参考架构》对零信任的实施划分了低、中、高3个阶段，明确在设计零信任体系结构之前，必须实现符合现有IT安全策略和标准的基线保护级别。美国国家安全局（NSA）将零信任工作规划为一个不断成熟的路线图[25]，从初始准备阶段到基本、中级、高级阶段，随着时间的推移，网络安全保护、响应、运营将得到改进。Microsoft的成熟度模型则将零信任规划的实施阶段划分为传统、先进、优化3级。

6.2 零信任落地指引

零信任理念在企业落地的具体场景和安全需要，将分为全新建设零信任架构网络和在已有网络架构上改造升级两种情况[26]。全新建设是指企业准备在新业务系统和网络的规划、建设过程中引入零信任理念，将零信任落地与企业网络建设过程同步进行，在企业网络建设完成时就满足了基本的零信任特性和安全能力要求。已有网络架构升级是指企业将现有的网络，根据零信任理念进行改造，逐步打造零信任安全能力（对现有能力的升级、替换或者全新部署），并将业务系统逐步迁移到零信任网络中。这种情况下，零信任网络和企业已有的传统网络可能并存一段时间，并最终完全过渡到零信任网络。

7 结语

零信任安全是一种全新的安全理念和架构，革新了以物理为边界的安全架构思想，定义以身份为基石的细粒度访问控制，并且访问控制策略需要基于对请求上下文的信任评估进行动态调整，是一种应对新型IT环境下已知和未知威胁的“内生安全”机制，拥有广泛的应用前景。本文对零信任的理念、定义、发展历史、模型进行介绍，提出通用化安全架构，深入分析该架构依赖的核心技术，并基于低耦合高内聚方式进行能力叠加建设，适配场景扩展，满足实际需求。同时在落地实施上，通过引入成熟度模型，完成零信任的落地指引。

但零信任安全的发展仍将是一个长期持续的过程，特别是在零信任实施的效果评价、零信任模型自身的安全防御能力、零信任环境下的用户业务访问体验、零信任与其他现有安全系统的融合问题、基于区块链的自我主权、去中心化的身份管理范式和技术、基于深度学习技术的信任评估实时性与控制精度等，都将是需要重点关注的问题。

参考文献

[1] Forum J. Jericho Forum Commandments [EB/OL].(2020-05-31)[2021-03-05].http://gfffg4a1b3affdeac447dsu9pfuqxoupoq69f9.fgfy.eds.tju.edu.cn/jericho/commandments_v1.2.pdf.

[2] John Kindervag. Build Security into Your Network's DNA:The Zero Trust Network Architecture [EB/

OL].(2010-11-05)[2021-06-24].https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf.

[3] Ward R,Beyer B.Beyondcorp:A New Approach to Enterprise Security[J].Login the Magazine of USENIX&Sage,2014,39(06):6~11.

[4] Software Defined Perimeter Working Group. SDP Specification 1.0 [EB/OL].(2014-04-30)[2021-05-06].https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf.

[5] Gartner. Use a CARTA Strategic Approach to Embrace Digital Business Opportunities in an Era of Advanced Threats[R].2017-05-22.

[6] Gartner. Market Guide for Zero Trust Network Access[R].2019.

[7] Peter Liu, Neil MacDonald. The Future of Network Security Is in the Cloud [R]. 2020-02-28.

[8] Chase Cunningham, Joseph Blankenship, Stephanie Balaouras, etc. The Zero Trust eXtended (ZTX) Ecosystem[R]. 2018-01-19.

[9] David Holmes, Forrester. Take Security To The Zero Trust Edge [EB/OL].[2021-02-24].https://go.forrester.com/blogs/take-security-to-the-zero-trust-edge/.

[10] Rose S, Borchert O, Mitchell S, etc. Zero Trust Architecture[M]. Gaithersburg, MD:National Institute of Standards and Technology,2020.

[11] [美]埃文·吉尔曼(Evan Gilman),道格·巴斯(Doug Barth).零信任网络:在不可信网络中构建安全系统[M].北京:人民邮电出版社, 2019.

[12] 张宇,张妍.零信任研究综述[J].信息安全研究,2020,6(07):608~614.

[13] Department of Defense. Department of Defense (DOD) Zero Trust Reference Architecture[R]. 2021.

[14] The National Cyber Security Centre.Zero Trust Architecture Design Principles[EB/OL].(2021-07-05)[2021-07-30].https://www.ncsc.gov.uk/collection/zero-trust-architecture.

[15] 中国电子工业标准化技术协会.零信任系统技术规范(T/CESA 1165-2021).[S].2021-07-01.

[16] National Cybersecurity Center of Excellence National Institute of Standards and Technology, Implementing A Zero Trust Architecture[M].2020.

[17] 宋宪荣,张猛.网络可信身份认证技术问题研究[J].网络空间安全,2018,9(03):69~77.

[18] 周瑞瑞,王春圆,李华芳.身份认证专利技术综述[J].河南科技,2020(03):147~152.

[19] 陈亚茹.基于区块链的物联网身份认证研究[J].信息技术与标准化,2021(04):47~49+58.

[20] 沈海波,洪帆.访问控制模型研究综述[J].计算机应用研究,2005(06):9~11.

[21] 程春蕊,刘万军.高内聚低耦合软件架构的构建[J].计算机系统应用,2009,18(07):19~22.

[22] 云安全联盟大中华区.2021零信任落地案例集[R].2020-06.

[23] Microsoft. Implementing a Zero Trust security model at Microsoft [R]. 2019-03-19.

[24] ACT-IAC Zero Trust Project Team. Zero Trust Cybersecurity Current Trends [R].2019-04.

[25] Defense Information Systems Agency (DISA), National Security Agency (NSA),Zero Trust Engineering Team. Department of Defense (DOD) Zero Trust Reference Architecture[R].2021.

[26] 中国产业互联网发展联盟标准专委会零信任产业标准工作组.零信任实战白皮书[R].2020-08.