美国零信任制度研究及启示

姚相振，李彦峰，孙　彦，羡喻杰
（中国电子技术标准化研究院，北京 100007）

摘　要：梳理分析了美国国防部和联邦政府的零信任政策相关标准情况，介绍了我国零信任相关政策标准以及产业发展情况。在此基础上，提出了加快零信任体系架构相关国家标准研制、开展零信任试点示范工作、推动零信任安全评估体系建设、积极推动零信任产业发展等建议。

关键词：零信任；政策标准；产业发展；能力成熟度
中图分类号：TP393　　文献标识码：A　　DOI：10.20044/j.csdg.2097-1788.2022.02.006
引用格式：姚相振，李彦峰，孙彦，等. 美国零信任制度研究及启示[J].网络安全与数据治理，2022，41(2)：35-40，67.

Research on American zero trust and its enlightenment

Yao Xiangzhen，Li Yanfeng，Sun Yan，Xian Yujie
(China Electronics Standardization Institute，Beijing 100007，China)

Abstract：This paper analyzes the standards related to the zero trust policy of the United States Department of Defense and the federal government，and introduces the zero trust related policy criteria and industrial development in China. Based on the analysis，some suggestions are put forward，such as accelerating the development of national standards related to the zero trust architecture，carrying out zero trust pilots and demonstrations，promoting the construction of the zero trust security evaluation system，and actively promoting the development of the zero trust industry.

Key words：zero trust；policy criteria；industrial development；maturity model

0 引言

随着网络环境日益复杂，基于固定边界的网络安全防护策略面临越来越严峻的挑战，例如，难以防御内部网络攻击、对数据泄露风险缺少有效防护措施等[1]。为应对日益复杂的网络安全挑战，美国国防部和联邦政府制定了一系列政策标准，推进相关领域信息系统零信任架构改造。

零信任作为一种安全理念，通过对访问发起方进行认证授权、持续监测和评估，动态调整访问控制策略，以实现对访问发起方的动态细粒度访问控制，有效管控安全风险。2010 年，咨询公司 Forrester 推出零信任(Zero Trust)概念，首次提出通过对每次访问过程进行评估建立信任关系的安全理念[2]。基于零信任理念，一批企业开展了落地实践工作，其中 Forrester 提出了零信任扩展(Zero Trust eXtended，ZTX)和零信任边缘(Zero Trust Edge，ZTE)[3]；Gartner 设计了零信任网络(Zero Trust Network Access，ZTNA)[4]；谷歌推动了 BeyondCorp 零信任项目[5]；微软开发了 Azure 零信任架构；云安全联盟(Cloud Security Alliance，CSA)提出了软件定义边界(Software Defined Perimeter，SDP)协议等[6]。据 Forrester 统计，2020 年全球范围内零信任业务年营收超过 1 亿美元的厂商有 10 家，零信任架构主要应用于政府、金融、制造业、医疗、教育等领域[7]。

本文梳理了美国零信任相关政策标准情况，并基于零信任在我国发展现状，提出了推动零信任发展相关建议。

1 美国零信任政策标准情况

为推动信息基础设施现代化，自 2019 年起美国在国防信息化和联邦政府信息化领域分别出台一系列政策标准，推动零信任架构落地应用。美国零信任相关政策标准发展情况如图 1 所示。

1.1 国防信息系统领域

2019 年 7 月，为了在全球网络安全威胁格局不

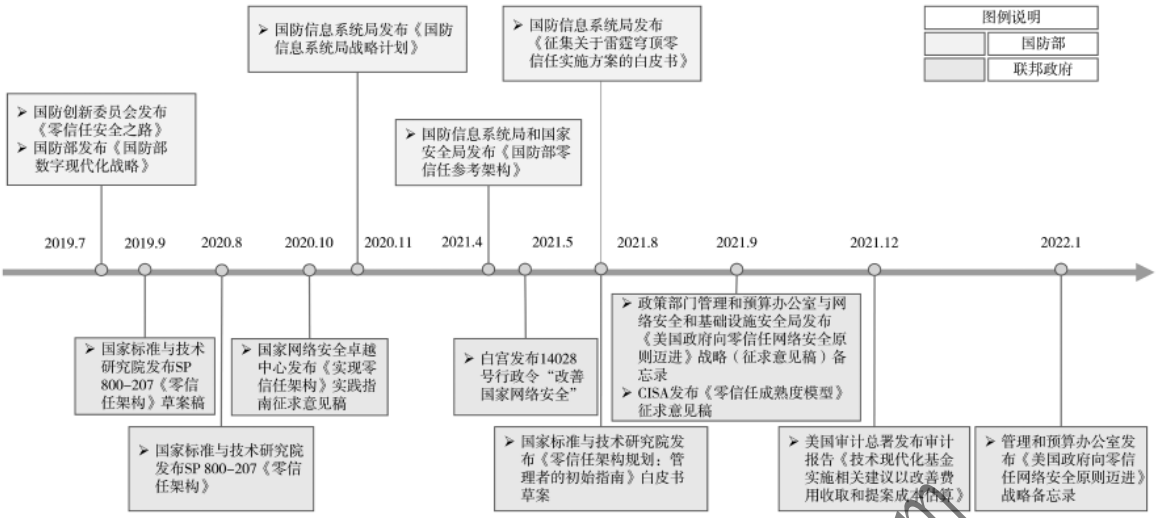

图 1 美国零信任相关政策标准发展情况

断演变的环境下保持竞争力，美国国防部(DoD)发布《国防部数字现代化战略》[8]，希望通过提高技术能力增强数字领域的竞争力，推动美国国防领域信息化建设的顶层设计。该战略提出通过创新获得竞争优势、优化效率和提升能力、发展网络安全实现灵活弹性的网络安全态势、培养数字化人才四项战略目标。在云计算、人工智能、指挥控制和通信、网络安全 4 个领域，提出了支持国防战略实施的路线图。在《国防部数字现代化战略》中，零信任安全被认为是 15 个重点发展技术之一。

落实《国防部数字现代化战略》，国防部下属国防创新委员会(Defense Innovation Board，DIB)和国防信息系统局(Defense Information Systems Agency，DISA)等机构先后发布了文件指导零信任架构在国防领域应用。

在国防创新委员会方面，2019 年 7 月发布了《零信任安全之路》白皮书[9]，用于指导国防部网络零信任架构的实施。该白皮书指出随着国防部网络规模和复杂性的快速增加，用户和端点数量不断增长，网络攻击面不断扩大，现有的基于固定边界的防护策略难以有效应对。零信任使用“角色”作为访问权限设计的核心，通过最小访问控制模型实现对特定资源的访问控制，包括用户验证、设备验证、权限验证三个基本验证步骤，可以有效提升国防信息系统安全性。

2019 年 10 月，国防创新委员会发布了《零信任架构建议》[10]，进一步指出零信任架构是美国国防部网络安全架构的演进方向，要求非机密互联网协议路由网络(Non-classified Internet Protocol Router Network，NIPRNET)和机密互联网协议路由网络(Secret Internet Protocol Router Network，SIPRNET)均应向零信任安全架构迁移。为实现基于用户属性的多因子认证、最小权限访问模式和持续验证设备状态等长期目标，《零信任架构建议》在《零信任安全之路》白皮书基础上进一步给出了同步实施零信任、用户授权、设备授权、最小权限授权四个方面的实施建议。

在国防信息系统局方面，2020 年 11 月，发布了《国防信息系统局战略计划》[11]，提出为抵御不断演变的网络安全威胁，将通过零信任架构项目整合现有安全解决方案，增强安全防御体系，有效防御内外部攻击，实现横向攻击的检测。国防信息系统局、国家安全局(National Security Agency，NSA)、网络司令部(U.S.Cyber Command)和国防部首席信息官合作开发零信任实验室环境，并通过现有技术测试零信任安全能力。

2021 年 5 月，国防信息系统局和美国国家安全局联合发布了《国防部零信任参考架构》[12]，提出国防部下一代网络安全架构应以数据为中心并基于零信任架构，提出了国防部网络环境下的零信任原则、能力、成熟度、参照标准等，明确了零信任架构在国防领域落地实施的具体要求。在原则方面，提出“环境敌对假设、失陷假设、永不信任和始终验证、显式验证、应用统一分析”等 5 项原则，用于指导零信任架构设计。在能力方面，如图 2 所示，提出用户、设备、网络/环境、应用和工作负载、数据、可见性和分析以及自动化和编排 7 个方面能力，并给出了每个能力依托的关键技术和技术间的依赖关

系，用以指导零信任部署。在成熟度方面，如图 3 所示，梳理了从传统网络架构向零信任迁移所需的资产发现和现状评估等准备工作，提出了基线、中等、高级三个成熟度级别，用于指导零信任落地和评估。在参照标准方面，给出了零信任相关法律法规和政策标准，作为零信任实施部署的参考依据。

2021 年 8 月，国防信息系统局发布《征集关于雷霆穹顶(Thunderdome)零信任实施方案的白皮书》[13]，旨在通过该项目试点工作推动零信任架构在军方落地，标志着零信任架构已经在美国军方进入试点应用阶段。

1.2 联邦政府信息系统领域

2011 年，联邦政府提出联邦风险和授权管理计划(Federal Risk and Authorization Management Program，FedRAMP)，提供标准化的安全和风险评估方法，促进联邦政府采用安全云计算服务。2017 年，联邦政府提出“美国联邦政府信息技术现代化计划”，进一步推动联邦政府信息系统向云计算服务进行迁移。

2019 年 9 月，美国国家标准与技术研究院发布了 SP 800－207《零信任架构》草案稿，并于 2020 年 8 月正式发布该标准。SP 800－207《零信任架构》指出零信任架构具有对访问请求进行认证授权、持续监测和评估以及动态调整访问控制策略的特点。该标准给出了零信任架构的参考，并说明了零信任架构的主要技术实现方式和部署方式。

2020 年 10 月，美国国家标准与技术研究院下属机构国家网络安全卓越中心(National Cybersecurity Center of Excellence，NCCoE)发布《实现零信任架构实践指南》征求意见稿[14]，该指南在 SP 800－207《零信任架构》基础上提出了零信任架构的实施建议，用于指导零信任部署。

2021 年 5 月，美国总统拜登签署 14028 号行政令《改善国家网络安全》。为应对云计算服务在联邦信息系统领域规模化应用带来的系统访问边界模糊、运维安全、数据泄漏等问题，行政令在“联邦政府网络安全现代化”部分，提出联邦政府机构应加强对云计算平台保护，向云计算平台迁移的政府机构服务应尽量使用零信任架构等要求。行政令要求政府机构部门负责人参照美国国家标准与技术研究院发布的标准和指南中的零信任架构迁移步骤，于行政令发布后 60 天内制定实施零信任架构计划。同时，行政令要求行政管理和预算办公室(Office of Management and Budget，OMB)、国土安全部(Department of Homeland Security，DHS) 和总务管理局(General Services)于行政令发布后 90 天内制定联邦云安全战略，并向各机构提供指导，推动各机构向零信任架构迁移。

2021 年 8 月，美国国家标准与技术研究院发布《零信任架构规划：管理者的初始指南》白皮书草案[15]，在 SP 800－207 基础上，介绍了如何使用风险管理框架实施零信任架构。

2021 年 9 月，落实 14028 号行政令，行政令要求行政管理和预算办公室与网络安全和基础设施安全局(The Cybersecurity and Infrastructure Security Agency，

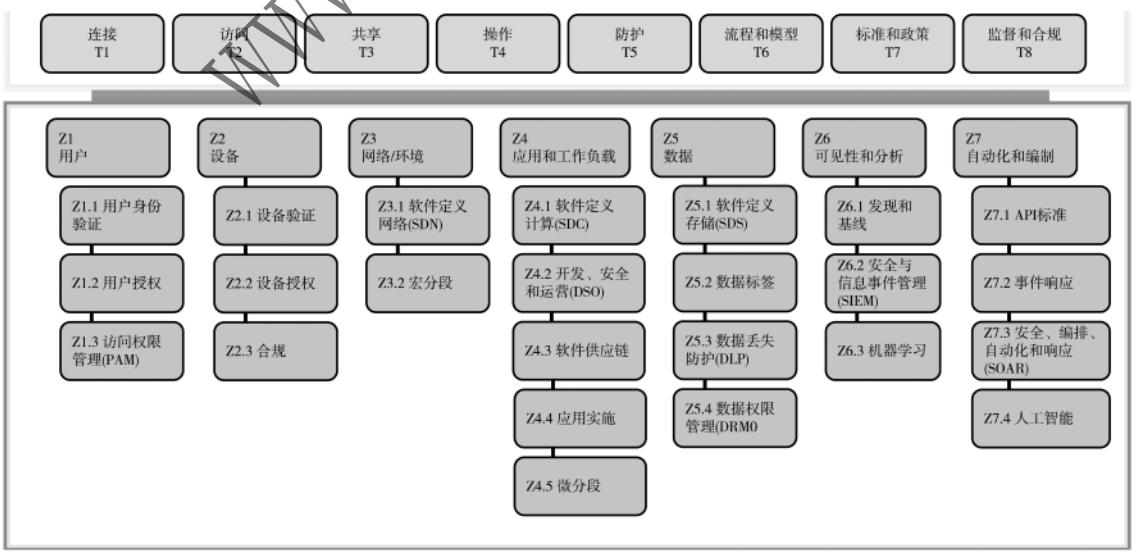

图 2 美国国防部参考架构零信任能力

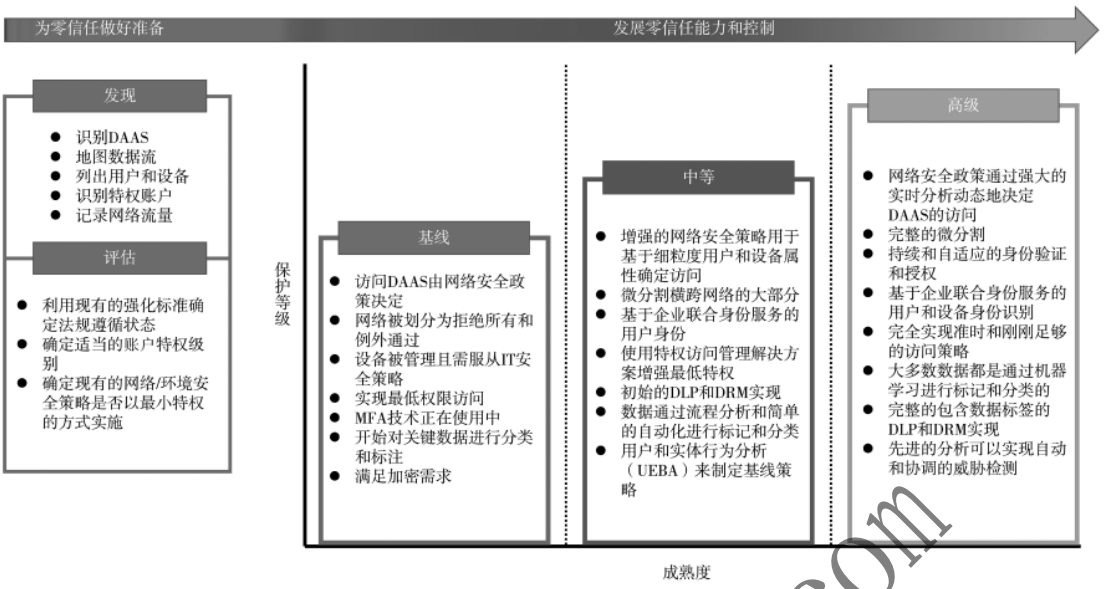

图 3 美国国防部零信任能力成熟度模型

CISA)发布《美国政府向零信任网络安全原则迈进》战略备忘录(征求意见稿)[16],要求联邦政府机构在2024年9月30日之前实现零信任安全目标。该备忘录于2022年1月26日正式发布。

2021年9月,支撑《美国政府向零信任网络安全原则迈进》战略备忘录落地,网络安全和基础设施安全局发布了《零信任成熟度模型》征求意见稿[17],将零信任基础分为身份、设备、网络、应用、数据5个维度以及贯穿所有维度的可视化分析、自动化编排、治理3个通用要素,并给出了零信任的成熟度模型,将零信任成熟度分为传统、先进和最佳3个成熟度等级,给出了各等级需满足的功能、关键技术和效果要求,为指导和评价零信任应用水平提供依据。图4给出了美国网络安全和基础设施安全局零信任成熟度模型。

2021年12月,美国审计总署(Government Accountability Office,GAO)在审计报告《技术现代化基金实施相关建议以改善费用收取和提案成本估算》中指出,行政管理和预算办公室下属的技术现代化基金在2021年9月批复了零信任相关项目经费597万美元。其中,总务管理局(General Services Administration)298万美元、教育局(Department of Education)200万美元、人事管理局(Office of Personnel Management)99万美元,用于推进零信任架构在联邦政府部门落地实施。该审计报告说明,在联邦政府信息系统领域零信任架构已进入实质性部署阶段。

2 国内政策及标准化情况

2.1 政策情况

2020年8月,工业和信息化部发布《工业和信息化部办公厅关于开展2020年网络安全技术应用试点示范工作的通知》(工信厅网安函(2020)190号),提出面向新型信息基础设施安全类、网络安全公共服务类重点方向,以及拟态防御、可信计算、零信任、安全智能编排等前沿性、创新性、先导性的重大网络安全技术理念,汇聚产学研用等创新资源,具备核心技术攻关、产业化应用推广等关键环节协同创新环境和载体的网络安全技术创新或试点示范区。

2021年3月,北京市科学技术委员会发布《北京市“十四五”时期智慧城市发展行动纲要》,提出建立健全与智慧城市发展相匹配的数据安全治理体系,探索构建零信任框架下的数据访问安全机制。

2021年7月,工业和信息化部公开征求对《网络安全产业高质量发展三年行动计划(2021-2023年)(征求意见稿)》的意见。该征求意见稿在“发展创新安全技术”一节提出“积极探索拟态防御、可信计算、零信任安全等网络安全新理念、新架构,推动网络安全理论和技术创新”,在“加强共性基础支撑”一节提出“针对5G虚拟专网、5G共建共享等网络建设模式,积极推进安全资源池、零信任安全架构、资产识别等安全解决方案应用,构建按需供给的安全能力”,在“推动关键行业基础设施强化网络安全建设”一节提出“推进零信任、人工智能等技术应

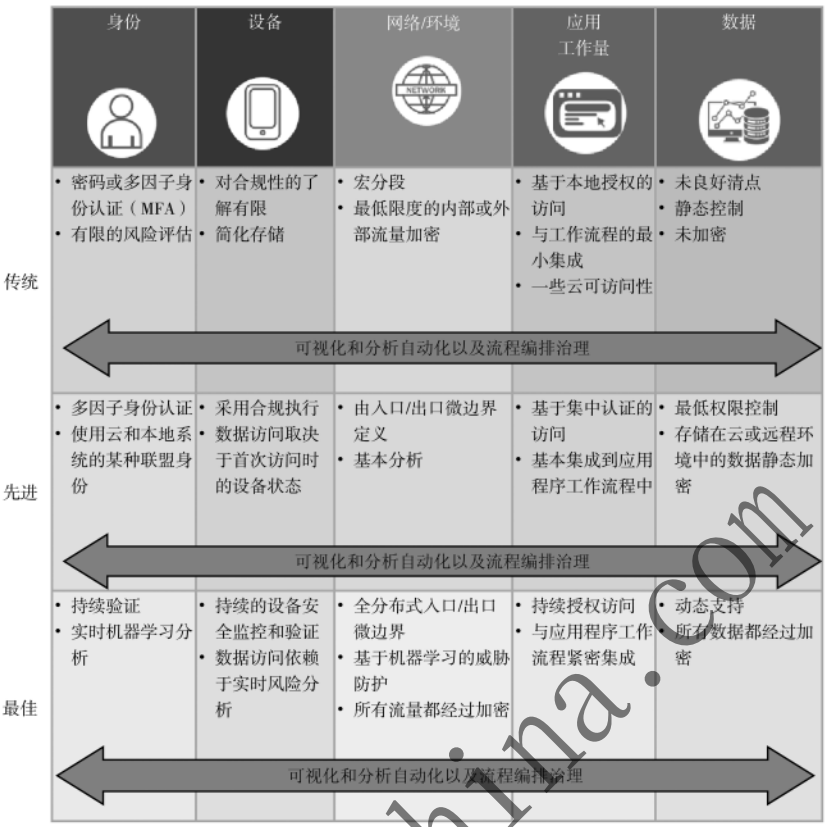

图 4 美国网络安全和基础设施安全局零信任成熟度模型

用，提升防护体系效能”等相关要求。

2021 年 7 月，工业和信息化部、中央网络安全和信息化委员会办公室等十部委联合发布了十部门关于印发《5G 应用“扬帆”行动计划（2021－2023 年）》的通知（工信部联通信〔2021〕77 号），在“5G 应用安全能力锻造工程”部分提出“推动发展内生安全、零信任安全、动态隔离等关键安全产品，创新开展风险识别、态势感知、安全评测、网络身份信任管理等 5G 应用安全服务，提升基于服务的 5G 应用安全保障能力。”

2.2 标准化情况

在国家标准方面，全国信息安全标准化技术委员会（简称“TC260”）提出并归口国家标准《信息安全技术 零信任参考体系架构》。该标准规定了零信任访问模型、整体框架、组件及组件之间关系，为采用零信任体系架构的信息系统的规划、设计、开发、应用提供参考。目前该标准处于草案稿阶段。主要零信任相关国家标准还包括：GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》，该标准规定了安全通信网络、安全区域边界以及可信验证等方面的要求；GB/T 38638—2020《信息安全技术 可信计算 可信计算体系结构》规定了可信计算基的功能、结构和工作流程等；GB/T 38644—2020《信息安全技术 可信计算 可信连接测试方法》规定了可信网络链接协议的要求和测试方法等。

2.3 产业情况

我国零信任产业处在起步阶段，据《2021 中国零信任全景图》统计，从应用场景看，我国零信任实施场景以远程接入为主，包括远程办公、远程分支机构接入、远程运维以及第三方人员访问和第三方系统连接企业内部资源等具体应用。其他场景还包括数据安全防护、应用程序编程接口（Application Programming Interface，API）安全防护、多云/多数据中心接入等。从已经实施零信任改造的行业分布看，政府机关、信息技术服务业、金融业和制造业占比相对较高，其他场景还包括教育业、批发零售业以及电力、热力、水利供应业、房地产业、旅游住宿业、交通运输业等。

据《2021 零信任落地案例集》[18]统计，现有的零信任解决方案主要采用软件定义边界（Software

Defined Perimeter, SDP)、基于身份识别与访问管理(Identity and Access Management, IAM)和微隔离(Micro Segmentation, MSG)三种方式,软件定义边界部署方式占比较高。25个厂商的26个零信任案例中,18个案例基于软件定义边界,4个案例基于身份识别与访问管理,3个案例基于微隔离,1个案例基于软件定义边界和身份识别与访问管理混合部署。

3 分析和建议

综合分析美国零信任发展情况,可以发现以下三方面特点:一是零信任架构应用是由美国大规模使用云计算环境的信息化现状所决定的,是保障信息化安全有序发展的重要措施;二是零信任标准确立了统一框架和实现评价方式,为零信任相关政策发布提供了技术支撑,有力推动了零信任架构在国防信息系统和联邦政府信息系统领域的落地应用;三是零信任是一种安全理念,实现方式并不受限于特定技术,可以通过多种技术方案实现。

基于美国在零信任应用推广方面的经验,为有效支撑我国网络安全保障体系和保障能力建设,推动零信任在我国落地应用,提出以下四方面建议。

一是应加快零信任体系架构相关国家标准标准研制,为零信任应用实施提供指导。零信任作为一种安全理念,国内学术界、产业界在技术框架、实现路径等方面尚未形成共识,应加快体系架构国家标准和配套实施指南等标准的研制,推动对零信任认识的统一,优化产业实践,降低产业发展成本,为零信任大规模应用奠定基础。

二是组织开展零信任试点示范工作,邀请零信任行业主要厂商、用户单位和网络安全领域专家,遴选一批可推广、可复制的零信任方案,摸清行业底数,为开展零信任架构改造提供参考。

三是推动零信任安全评估体系建设。针对零信任建设缺乏有效评价手段、安全能力提升较难量化的问题,探索开展零信任能力成熟度评估,推动零信任应用在相关行业实质落地,提升整体安全防护水平。

四是积极推动零信任产业发展,充分发挥零信任在构建现代化网络安全保障体系中的作用。我国正处在数字化转型的关键时期,随着数字化转型逐步深入,应用场景复杂化、设备类型多样化、身份管理碎片化的问题日益突出,应发挥零信任在身份管理、动态访问控制等方面的技术优势,推动国内零信任产业健康有序发展,为网络安全保障体系的高质量发展提供支撑。

参考文献

[1] 张宇,张妍.零信任研究综述[J].信息安全研究,2020,6(7):7.

[2] KINDERVAG J.Build security into your network′s DNA: the zero trust network architecture[Z].Forrester Research Inc,2010,27.

[3] CUNNINGHAM C,BLANKENSHIP J,BALAOURAS S,et al. The zero trust extended(ZTX) ecosystem[EB/OL].(2019-08-05)[2022-05-15].https://www.forrester.com/report/The-Zero-Trust-eXtended-ZTX-Ecosystem/RES137210.

[4] ORANS L,MACDONALD N,RILEY S.Market guide for zero trust network access[Z].2020.

[5] WARD R,BEYER B.BeyondCorp:a new approach to enterprise security[J].Login the Magazine of Usenix & Sage,2014(39):6-11.

[6] 软件定义边界(SDP)工作组.SDP标准规范1.0[EB/OL].(2019-05-xx)[2022-05-15]. https://c-csa.cn/u_file/photo/20200706/40c72deb73.pdf.

[7] CUNNINGHAM C,BLANKENSHIP J,BOUFFARD A,et al. Now tech:zero trust solution providers,Q2 2020[EB/OL].(2020-05-01)[2022-05-15].https://usermanual.wiki/m/15dd8b2fa296e671d936c4c12c13156edea8b5c94e99-2b187c789d685a87c55f.pdf.

[8] Department of Defense.DoD Digital modernization strategy[EB/OL].(2019-07-12)[2022-05-15].https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.

[9] DELBENE K,MEDIN M,MURRAY R.The road to zero trust(security)[Z].DIB Zero Trust White Paper,2019,9.

[10] DELBENE K,MEDIN M,MURRAY R.Zero trust architecture(ZTA) recommendations[Z].2019-10-24.

[11] DISA.DISA FY19-22 strategic plan version 2[EB/OL].(2020-xx-xx)[2022-05-15].https://www.disa.mil/About/Our-Strategic-Plan.

[12] Department of Defense.Department of defense(DOD) zero trust reference architecture[EB/OL].(2021-04-28)[2022-05-15].https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf.

(下转第67页)

参考文献

[1] 林伟芳,易俊,郭强,等.阿根廷“6.16”大停电事故分析及对中国电网的启示[J].中国电机工程学报,2020,40(9):2835-2842.

[2] 金戈.数据安全是工业互联网的新挑战[J].中国信息界,2021(4):80-83.

[3] 冯涛,鲁晔,方君丽.工业以太网协议脆弱性与安全防护技术综述[J].通信学报,2017,38(S2):185-196.

[4] 蔡葆锐,曾丕江,何金定,等.考虑频率安全约束的云南电网新能源运行边界研究[J].云南电力技术,2021,49(5):17-22.

[5] 田立霞.高铁新能源微电网规划定容及调度优化研究[D].北京:华北电力大学(北京),2021.

[6] 杨超然.新能源电力系统小干扰同步稳定性分析和稳定裕度提升策略研究[D].杭州:浙江大学,2021.

[7] 蔡旭,杨仁炘,周剑桥,等.海上风电直流送出与并网技术综述[J].电力系统自动化,2021,45(21):2-22.

[8] 罗旋,李永忠.Modbus TCP安全协议的研究与设计[J].数据采集与处理,2019,34(6):1110-1117.

[9] 宋岩,胡志成,郝丽,等.基于生成对抗式网络的Modbus协议安全性测试方法[J].电网与清洁能源,2019,35(8):8-15,24.

[10] 王玉敏.MODBUS协议簇简介[J].中国仪器仪表,2019(12):21-26.

[11] CREMERS C J F.The Scyther tool:verification,falsification,and analysis of security protocols[C]//20th International Conference on Computer Aided Verification.Springer-Verlag,2008:414-418.

[12] CREMERS C J F,MAUW S.Operational semantics of security protocols[J].Lecture Notes in Computer Science,2005,3466:66-89.

[13] THOMAS B G,CONTROLS C.Introduction to the modbus protocol[J].The Extension,2008,9(4):1-4.

[14] SWALES A,ELECTRIC S.Open Modbus/TCP Specification[J].Schneider Electric,1999,29:3-19.

[15] FAGUNDES F D,DA CUNHA M J.Industrial network security[J].Journal of Control,Automation and Electrical Systems,2022,32:1-11.

[16] 张笑从,郭华,张习勇,等.SM4算法快速软件实现[J].密码学报,2020,7(6):799-811.

(收稿日期:2022-04-25)

作者简介:

田学成(1993-),通信作者,男,硕士,工程师,主要研究方向:工控网络安全、协议形式化分析、渗透测试。E-mail:1214tian@sina.com。

张五一(1976-),男,本科,高级测评师,主要研究方向:电力系统网络信息安全。

江楠(1990-),男,本科,助理工程师,主要研究方向:电力行业网络安全技术应用和检测。

(上接第40页)

[13] Defense Information Systems Agency(DISA) Other Transaction(OT) Agreement Team.Thunderdome Zero Trust Solution[Z].2021-08-16.

[14] National Cybersecurity Center of Excellence.Implementing a zero trust architecture[EB/OL].(2020-10-xx)[2022-05-15].https://www.nccoe.nist.gov/sites/default/files/legacy-files/zta-project-description-final.pdf.

[15] National Institute of Standards and Technology.Planning for a zero trust architecture:a starting guide for administrators[EB/OL].(2021-08-04)[2022-05-15].https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.08042021-draft.pdf.

[16] Office of Management and Budget. Moving the U.S. government toward zero trust cybersecurity principles[EB/OL].(2022-01-26)[2022-05-15].https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[17] Cybersecurity and Infrastructure Security Agency.Zero trust maturity model[EB/OL].(2021-09-07)[2022-05-15].https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf.

[18] 云安全联盟大中华区.2021零信任落地案例集[EB/OL].(2021-06-30)[2022-05-15].https://c-csa.cn/api/web/download.php?id=1674&path=/u_file/photo/2021-0708/f9c279746d.

(收稿日期:2022-05-31)

作者简介:

姚相振(1984-),男,高级工程师,主要研究方向:网络安全。

李彦峰(1984-),男,工程师,主要研究方向:区块链网络隐蔽信道、供应链安全。

孙彦(1986-),男,工程师,主要研究方向:供应链安全、关键信息基础设施保护。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部