

基于零信任机制的工业互联网边界防护方案研究

王奕钧

(公安部第一研究所, 北京 100048)

摘要:随着互联网和信息技术的快速发展,传统的工业制造与新兴信息技术、互联网技术开始互相融合,“工业互联网”逐渐崭露头角,并广泛应用于能源、电力、交通、军工、航空航天、医疗等关系到国家安全、国计民生的重要行业。工业互联网涉及到众多国家关键基础设施,因此工业互联网的安全将影响到社会安全、公众安全甚至国家安全。该文对工业互联网中存在的网络安全风险进行分析,并提出一种基于“零信任”机制的边界防护方案,在兼容数量庞大、种类繁多的工业设备、操作系统以及生产应用的同时,为整个生产内网提供整体安全防护能力。基于零信任机制的工业互联网边界防护方案区别于传统防护思路,以白名单机制代替黑名单机制,以应用隐身代替技术对抗,以动态验证代替静态检测。最后,给出了基于零信任机制实现的工业互联网边界防护应用案例,并结合系统功能分析了该方案的技术优势。

关键词:工业互联网;零信任;边界防护;关键信息基础设施;白名单机制

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2024)03-0096-06

doi:10.3969/j.issn.1673-629X.2024.03.015

Research on Border Protection Scheme of Industrial Internet Based on Zero Trust Mechanism

WANG Yi-jun

(The First Research Institute of the Ministry of Public Security, Beijing 100048, China)

Abstract: With the rapid development of the Internet and information technology, traditional industrial manufacturing has begun to integrate with emerging information technology and internet technology. The "Industrial Internet" has gradually emerged and is widely used in important industries related to national security, national economy, and people's livelihood, such as energy, electricity, transportation, military industry, aerospace, and healthcare. The industrial internet involves many key infrastructure in countries, so its security will affect social security, public security, and even national security. We analyze the network security risks in the industrial internet and propose a boundary protection scheme based on the "zero trust" mechanism, which provides overall security protection capabilities for the entire production intranet while being compatible with a large number and variety of industrial equipment, operating systems, and production applications. The industrial internet boundary protection scheme based on zero trust mechanism is different from traditional protection ideas, using whitelist mechanism instead of blacklist mechanism, applying stealth instead of technical confrontation, and dynamic verification instead of static detection. Finally, we present an application case of industrial internet boundary protection based on zero trust mechanism, and analyze the technical advantages of this solution in combination with system functions.

Key words: Industrial Internet; zero trust; boundary protection; critical information infrastructure; whitelist mechanism

1 研究背景

互联网和信息技术经过近年来的快速发展,已开始与传统产业加速融合,“工业互联网”开始崭露头角。根据工业互联网联盟对工业互联网的定义:工业互联网是互联网和新一代信息技术与工业系统全方位深度融合所形成的产业和应用生态,是工业智能化发展的关键综合信息基础设施。工业物联网将物品、机器、计算机互联互通,辅助提供智能工业操作,改变商

业产出,现已广泛应用于能源、电力、交通、军工、航空航天、医疗等关系到国家安全、国际民生的重点制造行业,是国家关键生产制造基地的同时也是关键信息基础设施^[1]。在新冠肺炎疫情防控中,工业互联网平台有效支撑了防控应急处置,助力物资供需对接,推进企业复工复产,发挥了不可或缺的基础支撑作用^[2]。国家工业互联网的安全已经关系到了国家安全。但工业互联网打破了传统工业相对封闭但可信的制造环境,

收稿日期:2023-05-19

修回日期:2023-09-20

基金项目:国家重点研发计划项目(2020YFB1806500)

作者简介:王奕钧(1983-),男,副研究员,硕士,研究方向为网络安全。

所面临的安全风险和对工业生产的威胁与日俱增。

近年来,针对工业互联网的网络攻击不断攀升,受攻击的目标范围不断扩大。2015年12月,乌克兰电力系统遭到恶意软件攻击,攻击者利用系统漏洞获取了SCADA系统控制权限,远程控制系统跳闸,最终造成大面积停电^[3];2017年5月,罗马尼亚汽车制造商契亚、西班牙 Iberdrola 电力公司、尼桑桑德兰工厂等多家知名企业工业设施遭遇 WannaCry 勒索软件攻击,造成停工停产的严重后果^[4];2018年2月,以色列工业网络安全企业 Radiflow 公司发现四台接入欧洲废水处理设施运营技术网络的服务器遭遇恶意挖矿软件的入侵,并因此导致了废水处理设备中的 HMI 服务器瘫痪;特斯拉的云服务器也遭到入侵,入侵黑客通过攻击 Kubernetes 框架,在特斯拉公司基础设施的计算资源中植入挖矿软件挖掘门罗币^[5];同年5月,有关安全人员披露:全球超过54个国家,近50万台设备遭遇了利用新型恶意软件 VPNFilter 的入侵攻击,该恶意软件利用被感染设备组成僵尸网络,搜集网络流量和数据、执行命令和控制设备、拦截数据包、监控 Modbus 协议等,是利用 SCADA 系统的新型攻击软件^[6]。

由此可见,针对工业互联网的攻击已经将攻击目标从 SCADA 等传统的工业控制系统,向工业设备、云服务器、IT 设备等波及蔓延,针对工业互联网的攻击方式也越发多样,由针对性很强的 APT 攻击开始向包括勒索软件、挖矿病毒、僵尸网络等泛化攻击演变。随着工业互联网的开放化发展,设备层中的设备从资源还是运算能力上都得到了极大的提高,同时,为了便于增加新的应用功能,越来越多的设备采用了 Linux 开

源操作系统,针对工业互联网的攻击门槛也越来越低。并且工业互联网还在不断发展深入,云平台、IPv6、SDN 等新技术也会逐步加入工业互联网,相应地也会有越来越多的攻击逐渐延伸到工业云平台、网络、数据等层面。

2 工业互联网边界防护现状

工业互联网常见结构可以分为信息技术层 (Information Technology, IT) 和操作技术层 (Operation Technology, OT)。OT 层包括工程师站、PLC、执行设备、传感器等现场设备,用于实现工控网络中对资源、流程、工艺及事件的管理控制,覆盖生产运营、能源运营、设备资产运营以及服务运营等层面内容^[7]。IT 层则包括软件配置管理 (SCM)、企业资源管理 (ERP)、客户关系管理 (CRM)、企业生产过程执行管理 (MES) 等管理系统,通过采集大量 OT 层数据并加以处理利用,达到优化 OT 层生产流程,提高工业互联网生产运行效率的目的。但随着工业互联网的发展,OT 层与 IT 层互通互联成为的新的发展趋势,过去传统工控网络中 OT 网络与 IT 网络的明显隔离变得越来越模糊,更多的数据在工厂内部的 OT 层与 IT 层之间流转,同时,在工厂外也衍生出更多的定制业务、协同业务、产品服务工业云平台的功能,工厂内部的数据也因为业务需求而流转到工业云平台。而为了保证工厂外与工厂内数据的流转交互,通常需要使用 VPN 或白名单绑定的方式来建立动态或静态网络访问准入机制,以缩小工厂互联网暴露面,应对来自互联网中的网络攻击。工业互联网边界防护示意如图1所示。

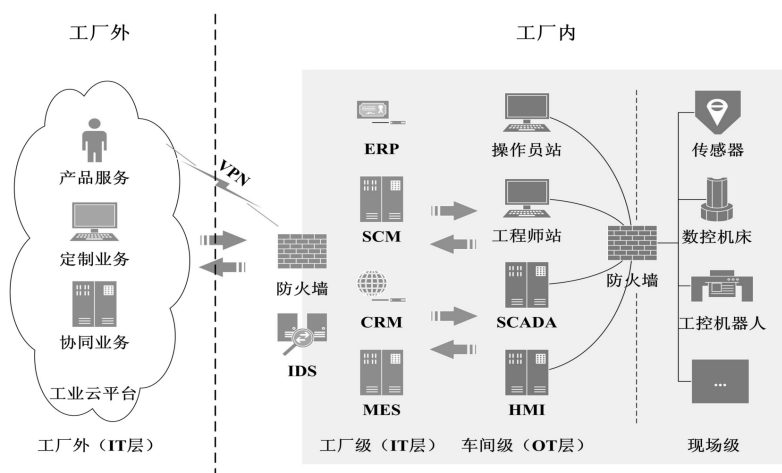


图1 工业互联网边界防护示意图

由此可见,当前工业互联网的安全防护理念相信所有网络访问是合法的,通过规则过滤结合行为检测的技术手段过滤掉网络攻击和恶意请求,从而建立防御入侵渗透的南北向攻击和内网漫游的东西向攻击的安全防护边界。南北向防御主要通过在网络出口处部

署防火墙、IPS等设备建立外网防护的边界,而东西向防御主要依赖在内网划分出多个功能分区,并在各分区之间进行安全隔离,从而规定出内部网络的网络安全边界^[8]。但是,伴随着网络攻击手段变化层出不穷,这种传统的防护体系在一定程度上可以防御外部攻

击,但无法抵御更高强度、有针对性的 APT 攻击。同时,为了保证工业云平台中各业务的快速增长,工厂内部与外部的数据安全交互,工厂网络出口处的安全运维工作压力会持续增高,并且由于工厂内部网络的访问规则一旦这层网络防护被突破,针对工厂内部的横向渗透将很难被有效防护。

因此,为了推进工业互联网的健康发展,中国与时俱进发布了《GB/T42021-2022 工业互联网总体网络架构》国家标准。其中,第9章“工业互联网网络安全要求”提出设备安全防护要求和网络安全防护要求,主要是要遵循《YD/T3804-2020 工业互联网安全防护总体要求》相关规定,明确了工业互联网安全防护内容包括设备安全、控制安全、网络安全等多个方面的要求^[9]。

3 “零信任”的边界防护机制

2004年,一批IT安全管理者在Jericho论坛提出,在复杂的企业IT网络中,传统的网络边界正在消失,

防火墙和其他边界网关已成为阻碍电子商务发展的绊脚石,在建设企业网络时应该消除这种边界(即“去边界化”)。2010年,著名研究机构Forrester的首席分析师John Kindervag提出了零信任(Zero Trust)的概念,即“我们的网络无时无刻不处于危险的环境中,网络位置不足以决定网络的可信程度,在安全区域边界外的用户是不安全的,所有设备、用户和网络流量都应当经过认证和授权,遵循最小权限原则,确保所有的访问主体、资源、通信链路出于最安全的状态”。Google在BeyondCorp项目中率先应用了零信任的防护理念,很好地解决了传统边界安全理念难以应对的安全问题。零信任概念的提出为业界勾勒了零信任安全的蓝图,自此,越来越多的网络安全专家开始将目光转向“零信任”。2020年2月,美国国家标准与技术研究院发布《SP800-207: Zero Trust Architecture》(第二版草案),标志着“零信任”从理念走向工程实践甚至标准化^[10]。“零信任”的发展过程如图2所示。

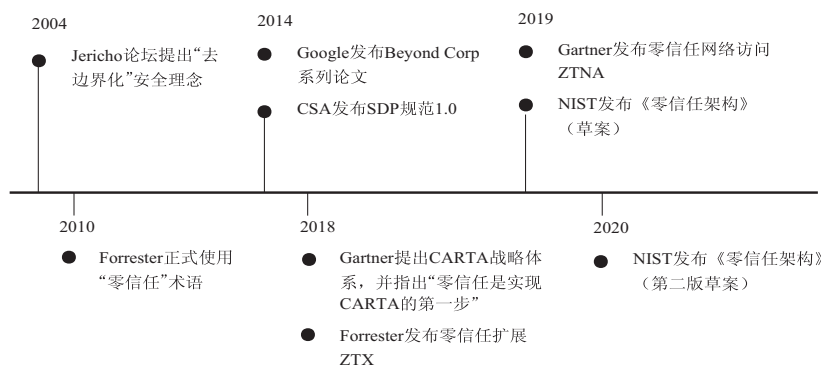


图2 “零信任”发展流程

相较于传统网络安全防护,“零信任”理念从信任准入出发,默认阻断一切连接,动态信任校验成功的连接,以隐身代替对抗,以准入代替检测。从根本上解决依赖安全策略配置导致的超量信任问题。通过假定所有的用户、终端、资源都是不可信的,所有用户、终端、

资源对资源的请求都需要通过动态的安全校验,在建立用户端到后台服务器的信任链后,方可具有对资源的安全访问权限,防止传统网络安全防护理念中超量信任带来的安全问题^[11]。零信任安全防护模型如图3所示。

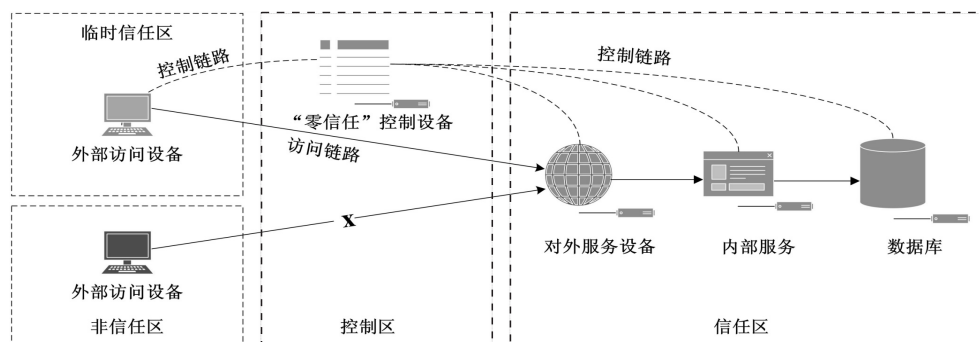


图3 “零信任”安全模型

相对于传统边界网络,“零信任”的安全模型将所有的外部访问设备定义为非信任区域,所有来自非信任区域内设备的访问请求都需要通过控制设备的鉴权

后才能分配到可以访问授信区域内服务节点的访问链路,没有获得合法访问链路的所有外部设备的访问请求都将在控制区域内被阻断,从而通过在边界动态授

权的方式,解决传统网络安全边界防护需要投入大量设备、运维、升级成本的根本问题。

4 基于“零信任”的工业互联网边界防护方案

4.1 方案设计

在以往安全解决方案中,网络和信息安全事件通常以“行为”作为攻防事件的核心焦点,从而形成了以网络安全行为防范为核心的安全治理模式。但是,工业互联网对外开放多种接口,使得许多工业控制行为被动连接到外部互联网。鉴于传统的安全防护仅是从信息安全或者功能安全的角度进行设计的,这使得 IT 环境与 OT 环境的信任边界变得模糊,导致风险防控问题更为复杂^[12]。

基于“零信任”的工业互联网边界防护方案的设计思路是在工厂内外部 IT 层之间、工厂内部 IT 层与 OT 层之间建立零信任的访问控制体系。工厂内的 IT 层默认阻断所有来自工厂外部的访问请求,从工厂外部应用需要访问工厂内部应用时,需要首先根据被访问服务的公钥文件、认证端口、校验码等信息初始化自身的鉴定请求,之后鉴定请求发往“零信任”控制设备

完成访问申请,“零信任”控制设备完成此条请求的身份鉴别后,向阻断设备发送允许建立此次链接的指令,阻断设备根据指令动态方向相关网络访问请求。同样的,工厂内部 IT 层与 OT 层之间也依据此种机制完成 OT 层对外隐藏自身应用,IT 层应用根据需要动态建立访问隧道的边界安全访问手段。

基于“零信任”的工业互联网边界防护方案的核心思路是围绕工业生产应用创建基于身份和上下文的逻辑访问边界,边界内部对外提供服务的应用是隐藏的,无法被直接发现和访问,使攻击者在网络空间探测或内网漫游时无法发现攻击目标,进而无法完成对其的攻击渗透。“零信任”控制设备会验证访问应用的身份、上下文和策略合规性,在不影响业务正常运行的同时,显著缩小攻击暴露面。

该方案可通过在网络出口核心交换处部署“零信任”控制设备和阻断设备,通过读取核心交换机的镜像流量,识别流量中特定的 SPA 认证包,进而完成后续的身份鉴定业务逻辑,阻断设备通过发送双向阻断的数据包实现默认阻断所有外部访问的阻断业务逻辑。部署结构及认证过程示意如图 4 所示。

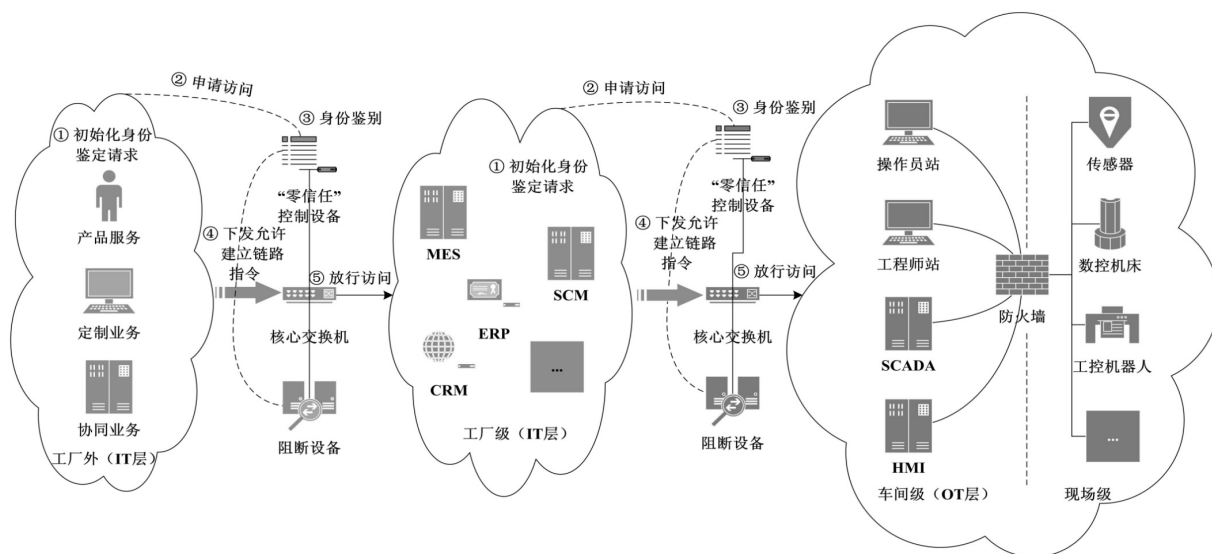


图4 基于“零信任”的工业互联网边界防护方案部署结构示意图

基于“零信任”的工业互联网边界防护方案涉及三个业务流程:应用隐身、身份鉴别、访问控制。

(1) 应用隐身。

基于 TCP/IP 协议中三次握手成功后建立访问连接的机制,通过向未经授权的通信两端发送 SYN RST 和 SYN ACK RST 包的方式^[13],可以阻断所有未授权访问的来自边界外部的扫描探测行为,从而达到将应用隐身的效果。

(2) 身份鉴别。

身份鉴别基于国产加密算法 SM9 实现^[14], SM9

现已成为中国商用密码国家标准,同时, SM9 数字签名算法和加密算法也已成为 ISO/IEC 国际标准^[15]。身份鉴别过程中边界外的应用将需要访问的应用 IP、端口、校验码、时间戳通过边界内应用的公钥使用 SM9 加密算法加密后形成申请授权的 Token,并以 UDP 协议发往“零信任”控制设备的指定端口,“零信任”控制设备在镜像流量中捕获有效 Token 后,根据对应边界内应用的私钥将 Token 解密,然后验证校验码的正确性和时间戳的有效性,如均验证成功,则向阻断设备发送指令,针对边界外应用 IP、边界内应用 IP

和端口进行放行。同时,“零信任”控制设备还将在镜像流量中监测该链路的访问情况,当超过空闲阈值时,将向阻断设备发送指令,恢复对该边界内应用的应用隐身操作。

(3) 访问控制。

阻断设备在收到放行指令后,将针对指令中的源

IP、目的 IP、目的端口建立临时白名单,停止对白名单中的访问双方发送 SYN RST 包,从而允许建立该访问链路的效果。

以工厂外 IT 层访问工厂级 IT 层为例,详细访问流程如图 5 所示。

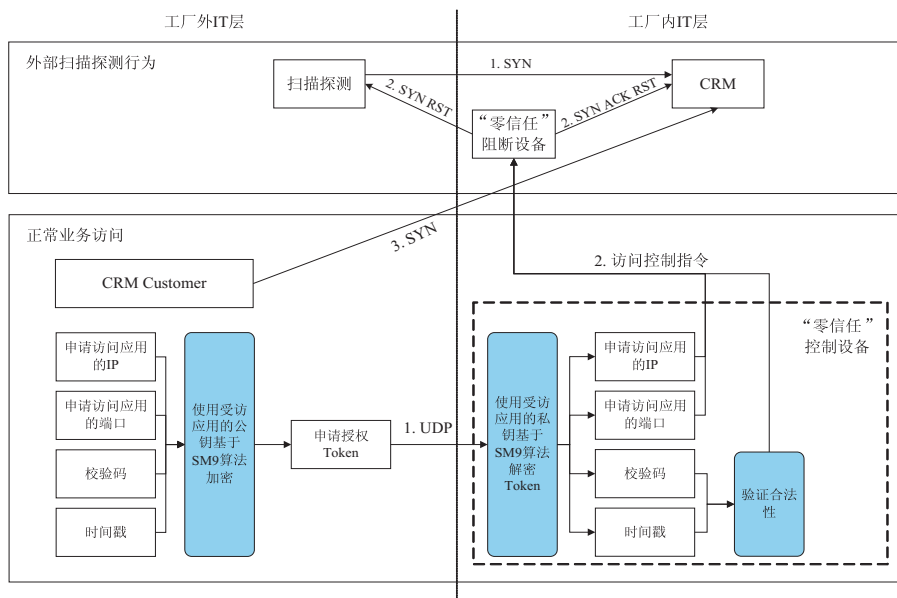


图 5 基于“零信任”的工业互联网边界防护方案访问流程

4.2 应用案例

该方案已经在某重要行业单位试点应用,可以通过配置应用名称、应用 IP、应用端口、校验码、准入时长来保证工业互联网中的应用基于“零信任”机制对外提供服务,确保工业互联网中的应用在互联网上不可被扫描探测发现。配置规则如图 6 所示。

当互联网上有主机设备试图探测访问工业互联网中的应用时,零信任授权设备将直接阻断该请求连接,并形成告警日志,告警日志如图 7 所示。

基于“零信任”的工业互联网边界防护方案相较于传统的网络传统边界安全具有安全性高、部署灵活、兼容性好的特点,具体优势如下:

添加应用隐身配置

应用名称*

请输入

应用 IP *

请输入

应用端口 *

请输入

校验码 *

请输入

准入时长 *

请输入

(分钟)

备注

请输入

保存

取消

图 6 零信任授权设备规则配置详情

时间	源IP	源端口	应用IP	应用名称	协议	应用端口	日志类型	处理动作	日志摘要
2022-04-06 10:04:06	123.232.102.155	33107	10.10.10.10	K...	TCP	443	未授权访问	阻断	--
2022-04-06 10:04:06	58.34.205.139	54370	10.10.10.10	I...	TCP	443	未授权访问	阻断	--
2022-04-06 10:04:04	221.212.198.192	34914	10.10.10.10	I...	TCP	443	未授权访问	阻断	--
2022-04-06 10:04:03	123.232.102.155	39856	10.10.10.10	I...	TCP	443	未授权访问	阻断	--
2022-04-06 10:04:02	223.71.147.8	6130	10.10.10.10	I...	TCP	443	未授权访问	阻断	--
2022-04-06 10:04:01	112.103.18.150	11904	10.10.10.10	I...	TCP	443	未授权访问	阻断	--
2022-04-06 10:03:59	112.125.90.60	57066	10.10.10.10	K...	TCP	443	未授权访问	阻断	--
2022-04-06 10:03:58	124.64.17.144	56509	10.10.10.10	T...	UDP	443	校验通过	通过	认证通过
2022-04-06 10:03:55	123.232.102.155	39801	10.10.10.10	I...	TCP	443	未授权访问	阻断	--
2022-04-06 10:03:54	124.64.22.95	5311	10.10.10.10	I...	TCP	443	未授权访问	阻断	--

图 7 告警日志页面

(1)无需改变工业互联网中生产网络与外部网络的网络结构,不用改造被保护的工业生产应用,即可实现工业生产应用在外网网络中隐身的边界防护效果;

(2)通过在镜像流量中过滤授权请求的方式无需在外网暴露零信任授权服务,避免遭受有针对性的攻击,进而授权任意用户访问;

(3)“零信任”控制设备和阻断设备采用旁路部署的方式,接入交换机镜像流量,降低串行部署的带来的性能、安全、可靠性瓶颈;

(4)可以通过镜像内网流量的方式,实现对内部用户访问内部应用时的零信任授权功能,有效抵御内部攻击。

5 结束语

当传统的工业制造与新兴信息技术、互联网技术相融合后,一个全新的工业时代正在人们面前徐徐拉开序幕,工业互联网的发展也呈现出顶层布局形成共识、“平台+”集群式转型、“链式”融合创新、智能技术规模化应用等发展趋势^[16]。由于工业互联网广泛运用于能源、电力、交通、军工、航空航天、医疗以及市政等领域,涉及到众多国家关键基础设施,因此对工业互联网的安全防护工作就显得尤为重要。但根据 Common Vulnerabilities & Exposures (CVE)、National Vulnerability Database (NVD)、中国国家信息安全漏洞共享平台 (CNVD) 及国家信息安全漏洞库 (CNNVD) 四大安全漏洞共享平台发布的工控系统安全漏洞分布可见,制造业、水务、能源、商业设施、医疗、轨道交通、航空等关键基础行业都存在大量漏洞隐患^[17]。由此可见,国内工业互联网急需一套自主可控、兼容性好、安全性高的防护方案来应对当前形势下面临的网络安全风险。

该文从工业互联网的边界防护为切入点,引入“零信任”的安全防护机制,为整个生产内网提供整体安全防护能力,同时兼容了数量庞大、种类繁多的工业设备、操作系统以及生产应用。通过将可信信道的建立与工业生产控制访问相剥离,在不调整已有应用服务的前提下,利用单包授权校验、二次信道授权等技术手段保证工业互联网上对外开放的服务不受影响的同时,黑客无法探测出对外开放的服务,从而实现保护服务不能被黑客攻击的目标。“零信任”的安全防护机制在数据中心内部访问、物联网、混合云、工业物联网机房对外访问入口等应有场景下有良好的防护效果^[18]。互联网的防护是一项长期性、高难度、高复杂性的系统工程,仍然需要通过完善指引工业互联网安全发展的网络安全制度、标准,提升工业互联网安全防护技术创新能力,打造工业互联网安全监测预警手段

等方式,全面提升国内工业互联网的安全防护水平,保证国内工业互联网的健康发展。

参考文献:

- [1] 方 芳,陆海婧.我国工业互联网技术发展路线研究[J]. 信息技术与网络安全,2022,41(1):42-46.
- [2] 何小龙,李 君,周 勇,等.工业互联网平台应用现状及发展对策[J]. 科技管理研究,2021,41(10):132-137.
- [3] RFE/RL. Russian hacker sandworm blamed for Ukraine power outage [EB/OL]. 2016-01-08. <https://www.rferl.org/a/russian-hacker-sandworm-blamed-ukraine-power-outage/27474835.html>.
- [4] 唐 岚.从 WannaCry 事件看网络空间国际规则的困境及思考[J]. 云南民族大学学报:哲学社会科学版,2019,36(6):145-156.
- [5] KOVACS E. Cryptocurrency miners not uncommon on industrial systems [EB/OL]. 2018-02-13. <https://www.securityweek.com/cryptocurrency-miners-not-uncommon-industrial-systems>.
- [6] 傅 扬.国内外工业互联网安全态势和风险分析[J]. 信息安全研究,2019,5(8):728-733.
- [7] 董 悦,王志勤,田慧蓉,等.工业互联网安全技术发展研究[J]. 中国工程科学,2021,23(2):65-73.
- [8] 张 勇,周慧涛.基于安全域的企业网络安全防护体系研究[J]. 科学与信息化,2021(25):96-98.
- [9] 吴青松,张 玉.基于 SDP2.0 的工业互联网安全接入技术研究[J]. 工业信息安全,2023(1):28-34.
- [10] 张 宇,张 妍.零信任研究综述[J]. 信息安全研究,2020,6(7):608-614.
- [11] ROSE S, BORCHERT O, MITCHELL S, et al. Zero trust architecture [R/OL]. [2022-03-25]. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>.
- [12] 宁黄江,郭翔宇,安 健,等.工业互联网公共服务平台信任架构建设探究[J]. 工业技术创新,2022,9(2):97-103.
- [13] JIN Hai, TANG Dan, ZHANG Youkun. SHAK: eliminating faked three-way handshaking in socket handoff [C]//Proceedings of the 18th international parallel and distributed processing symposium. Santa Fe: IEEE, 2004.
- [14] 姜 琳,周 亮,缪思薇,等.基于零信任架构的电力物联网安全接入方法[J]. 电力信息与通信技术,2023,21(1):40-46.
- [15] CHENG Z H. Security analysis of SM9 key agreement and encryption [C]//Information security and cryptology. Fuzhou: Springer, 2019: 3-25.
- [16] 张 宇.展望 2023 年工业互联网发展呈现八大趋势[J]. 通信世界,2023(3):31-32.
- [17] 蔡一鸣,夏 冀,韩潇哲.工业互联网渗透测试技术研究[J]. 自动化博览,2023(1):12-14.
- [18] 李涟漪.《零信任实战白皮书》学习,探寻工业互联网与零信任的结合 [EB/OL]. 2021-02-01. https://blog.csdn.net/weixin_41284310/article/details/113524666.