零信任架构在医疗物联网安全建设中的应用

Application of Zero Trust Architecture in Security Construction of Internet of Medical Things

景鸿理/JING Hongli，屈伟/QU Wei，刘治平/LIU Zhiping
（天融信科技集团股份有限公司，中国 北京 100193）
(Topsec Technology Group Inc., Beijing 100193, China)

DOI：10.12142/ZTETJ.202206007
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20221208.1448.001.html
网络出版日期：2022-12-09
收稿日期：2022-10-16

摘要：提出了一种基于零信任架构和技术的医疗物联网（IoMT）融生安全框架。该安全框架利用零信任控制平台、物联网安全接入网关、医疗终端、医疗业务系统、相关辅助支撑系统等组件，实现访问主体、运行环境、访问客体的融合共生，能够形成以身份可信管理为中心，全面融合业务安全访问、持续风险评估和动态访问控制的安全能力，支撑IoMT的设备统一管理、安全准入控制、设备行为分析、终端安全检测、动态可信接入、安全加密通道等安全应用。

关键词：IoMT；智能医疗设备；零信任架构；融生安全框架

Abstract: A security framework for the Internet of Medical Things (IoMT) based on zero trust architecture and technology is proposed. Using the zero trust control platform, Internet of Things security access gateway, medical terminal, medical business system, and relevant auxiliary support system components, the security framework realizes the access subject, operating environment, and access object fusion symbiosis, which can form a security capability that takes identity trusted management as the center, fully integrate business security access, continuous risk assessment and dynamic access control, and support IoMT equipment unified management, security access control, device behavior analysis, terminal security detection, dynamic trusted access, secure encryption channel, and other security applications.

Keywords: IoMT; intelligent medical equipment; zero trust architecture; fusion-symbiosis security framework

医疗物联网是物联网技术在医疗行业的重要应用。医疗物联网模糊了传统的网络边界，通过可穿戴设备、传感器和专业工具等智能医疗设备，实时感知环境信息（包括人和物理环境等），或将数据传输数据给用户，并在网络中完成数据加密、数据传输和数据分析等，从而协助人们完成医疗物联网平台数据采集和数据分析等工作[1]。但大量支持物联网技术的智能医疗设备数量激增,容易受到未经授权访问和其他恶意活动的攻击[2]；物联网技术的异构性和设备的动态管理特点，使得医疗物联网系统容易受到不同的动态环境攻击者的数据窃取和篡改[3]。从某种意义上讲,基于物联网的医疗行业应用放大了安全边界，带来了访问控制和数据资源的安全风险。因此，加强医疗物联网的身份管理和边界防护，提高医疗物联网平台、用户、设备等资产的身份认证和访问控制安全能力，保护医疗物联网环境下的应用和数据资源安全,是当前亟待解决的问题。

随着数字化转型的不断深入，以信任为核心的安全理念迎来发展机遇，零信任机制成为一种有前景的解决方法，可有效应对行业数字化转型过程中医疗物联网系统的各种隐私、安全和认证挑战。医疗物联网与零信任机制的融合，能够打破网络边界位置和信任间的默认关系，解决在不可信环境中可能出现的智能医疗设备身份可信和业务数据动态管理问题，提升医疗物联网对基础网络层和数据中心层的安全管控力度，隐藏被攻击区域，减少攻击面，最大限度保证资源被可信访问。

本文中，我们主要对医疗物联网建设中的可信安全防护进行详细研究，融合新兴的零信任架构和技术，结合医疗物联网的安全风险，分析适用于医疗物联网的动态身份管理机制设计，提出零信任-医疗物联网融生安全框架，并解决以下问题：

（1）医疗物联网边界模糊带来的安全性问题。随着移动办公、万物互联等技术的广泛采用，医疗物联网的网络边界越来越模糊，安全防护边界逐步被打破，已无法清晰定义安全的网络。工作方式移动化、数据资源集中化、资源访问云

化等，进一步导致业务数据的访问超出了传统的物理边界，增加威胁暴露面。

（2）医疗物联网传统安全架构缺陷问题。医疗物联网仍然按照传统网络安全架构将网络划分为内部网络和外部网络。内部网络受信任，外部网络则不受信任，整体安全防护通过静态配置来实现。在受信任区域，大量的移动用户和设备接入导致业务暴露面扩大，一旦被渗透，受信任区域所有数据资产无法进行有效隔离和防护；内部网络部署的大量设备缺少信息共享和安全联动，受信任区域实质上处于割裂状态下的静态安全防护。在不受信任区域，随着数据资源集中，价值增加，存在大量绕过或攻破网络访问权限的内部横向攻击破坏行为；以高级可持续威胁（APT）为代表的高级攻击层出不穷，大型组织甚至国家的攻击者可以利用大量的漏洞“武器”，对重要目标进行攻击，这类攻击往往防不胜防[4]。

1 医疗物联网架构和安全概述

中国信息通信研究院将医疗物联网定义为 Internet of Medical Things（IoMT），是指面向医疗机构全方位的运营和管理，将传感器、近距离通信、互联网、云计算、大数据、人工智能等物联网相关技术与医学健康领域技术相融合，实现医疗健康服务智能化的综合系统。IoMT 通过结合广域网、局域网、无线网络等网络领域，使得物联网技术越来越广泛地应用于医院信息系统，如人体传感技术、医疗装备定位、移动医疗技术、精准疫情防控等，已形成基于医疗信息平台的，具有创新应用模式、系统高度集成、数据资源高度整合的医院管理应用生态链[5]。

1.1 医疗物联网架构

IoMT 架构一般沿用通用物联网的感知、网络、应用 3 层体系，结合大数据、云计算等医疗实际环境，把管理和业务平台建设独立出来，形成了 IoMT 的感知层、网络层、平台层和应用层 4 层体系架构，如图 1 所示。

感知层主要通过医疗健康感知设备和信息采集设备，对 IoMT 中的医患人员设备节点进行感知识别，并利用多种生理信号采集方式，协同完成对医疗信息的采集和数据传输。

网络层实现物联组网和控制，利用以太网技术、移动通信技术、机器通信（M2M）技术等，以无线或者有线的通信方式，将感知采集的数据信息进行实时、无障碍、高可靠的传送。

平台层主要通过设备管理平台、信息集成平台、应用服务平台、业务分析平台、数据支撑平台等，实现终端设备和资产的“管理、控制、运营”一体化，向下通过连接管理平台连接感知层，向上通过开放管理平台提供面向医疗应用服务的开发能力和统一接口管理。

应用层面向医院业务管理、个人健康管理、网络运营管控、辅助决策支撑等提供具体的业务应用[6]，如婴儿防盗、资产定位、人员定位、移动医护、智能输液、体征监测、就诊导航、废弃物监测、掌上医院等。

▲图1 医疗物联网架构

1.2 医疗物联网安全防护现状

IoMT安全防护一般参考物联网安全架构有关标准要求进行建设，主要包括对资产标识与配置管理、数据加密与保护、逻辑访问控制、设备安全状态等安全基线控制要求[7]。经过多年的信息化建设，IoMT基本实现了环境数据感知采集、业务过程全周期控制、医疗全程跟踪追溯、医院体系化安全管理等[8]。物联网技术给医疗行业带来网络化、智能化、自动化的同时，也存在着物理感知节点控制伪装、医疗信息数据可能被破坏或用户隐私泄露等安全隐患[9]。

目前，IoMT安全防护建设主要基于网络安全等级保护的物联网安全扩展要求，采用传统网络隔离的安全模型，用防火墙、入侵检测系统（IDS）/入侵预防御系统（IPS）、虚拟专用网（VPN）、行为审计等边界防护设备划分出医疗内网和外网，形成以账户管理和边界防护为核心的防御体系。从防范外部攻击的角度，防火墙和VPN的模式形成了深度防御态势，增加了黑客攻击的难度，但是对内部人员实施的窃密行为无法管控，存在内部人员攻击和绕过边界防护的APT等攻击行为；同时，IoMT也模糊了内外网的边界，存在逻辑外部人员实际已在内网进行操作，以及逻辑内网设备实际已在外网存在的可能。随着IoMT对云计算、移动互联网、大数据、人工智能等技术的融合应用，IoMT联网设备一般无法配备足够的存储空间和计算能力，不能通过部署安全防护软件来保障自身安全；大量智能设备不间断收集数据并存储到云端，会带来医疗数据泄露、非授权访问、隐私泄露等新的安全隐患。医疗行业用户需要面临医疗数据泄露、应用账号密码泄露、特权账号共享、网络终端木马、内部员工违规操作等内部风险，以及APT攻击、网络钓鱼邮件等外部威胁。现有安全防护手段与业务结合不紧密，资产管理、户身份认证、访问控制、数据资源保护以及终端安全状态等安全措施缺乏统一融合管理，亟需优化和重构。

2 零信任架构和关键技术

零信任是一种建立安全战略的理念、方法和框架，代表着当前正在演进的网络安全最佳实践，力求通过全新的去中心化安全架构，应用更细粒度的规则来解决网络中特定数据的安全威胁[10]。2020年8月，美国国家标准与技术研究院（NIST）发布的《零信任架构》指出了传统安全架构基于边界安全的问题，并将零信任架构确定为一种包含身份、凭证、访问控制、操作、互联基础设施等所有网络要素的端对端安全体系方案[11]。经过多年发展，数字化时代网络安全威胁比以往任何时候都更加复杂和险恶，安全架构的薄弱环节正是身份安全基础设施的缺失。建设以身份为基石的零信任网络安全体系，成为覆盖云环境、大数据中心、微服务、万物互联等众多场景的新一代安全解决方案。

2.1 零信任架构

零信任架构本质就是以身份为中心，根据受限资源访问需求，在访问主体和访问客体之间，实现临时、动态、可信的安全访问体系，如图2所示。

基于零信任建立的网络以受限资源安全保护需要为出发点，将安全能力抽象为可信代理、动态访问控制、身份管理、权限管理及身份分析等功能组件，形成主客体间的动态可信安全访问平台，同时与其他安全分析平台协同联动，保障主体对客体业务、数据访问的安全可信闭环[4]。

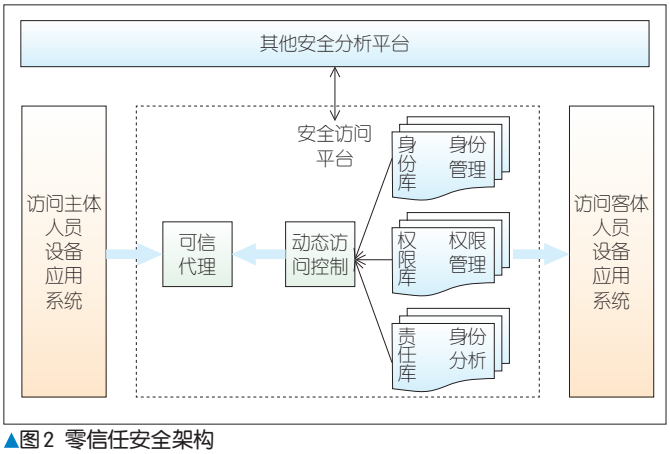
2.2 零信任关键技术

零信任关键技术包括身份管理、终端环境感知、主体行为分析、信任推断、动态控制等。

（1）身份管理。身份管理分为认证和授权两大组件，可为零信任体系提供身份认证服务和安全授权服务。身份管理可以将用户身份和访问权限做到细粒度对应，确定用户最小访问权限。对主客体的身份认证可以为业务系统提供统一的身份认证服务，支持多种常用认证协议，建立多权限模型，从而满足不同业务场景[12]。

（2）终端环境感知。终端环境感知需要针对业务终端进行统一管理和分组，查看所有终端的状态，对终端的操作系统版本、核心进程号、指定文件、木马、蠕虫、病毒等指定监测因子进行持续监控与检查，并针对终端进行安全策略集中下发等，为零信任体系提供终端风险状态的判定。

（3）主体行为分析。主体行为分析是指对主体的日常访问行为进行持续审计和监控，构建行为模型和综合评分机制，以形成主体行为访问基线，对主体访问偏离基线的程度



▲图2 零信任安全架构

进行上报，从而为零信任体系提供主体行为偏离度的判定。

（4）信任推断。信任判断是指综合多种判定因子，实现基于身份、权限、主客体安全等级模型的关联；建立主体访问客体的信任模型，为动态访问模块提供可信访问的判断依据；实时接收、统计终端环境风险的评估数据，判断当前用户风险状态。

（5）动态访问控制。动态访问控制与信任推断联动，将网络安全等级与业务安全策略进行自动匹配，将最小权限下发到相应的策略执行点。主体行为分析系统提供的风险评估等级，可以提供多因子认证方式的访问控制策略和执行，实现动态决策授权。基于访问主体和访问客体安全属性的风险评估结果可以进行动态决策。

3 基于零信任架构的医疗物联网融生安全框架

3.1 零信任–医疗物联网融合解决思路

结合 IoMT 架构和安全风险，融合零信任架构和技术，以身份为中心，建立访问主体（合法设备、合法用户等）、运行环境（通信网络和计算环境）、访问客体（业务应用及数据资源）之间的安全可信关系，能够持续验证主体的访问权限信任度。基于设备代理/网关部署隐藏互联访问交互，可以实现对医疗终端到业务系统的主体访问、应用访问、访问控制 3 个阶段的持续动态评估，从而能够确保访问主体安全可信和业务访问动态安全，达到零信任和医疗物联网融合共生安全的效果。零信任–医疗物联网融合解决思路如图 3 所示。

3.2 零信任–医疗物联网融生安全框架

我们按照零信任–医疗物联网融合解决思路，设计了零信任–医疗物联网融生安全框架，具体如图 4 所示。

零信任–医疗物联网融生安全框架包括零信任控制平台、物联网安全接入网关、医疗终端、医疗业务系统、相关辅助支撑系统 5 部分，分别部署于医疗物联网的控制平面和数据平面。

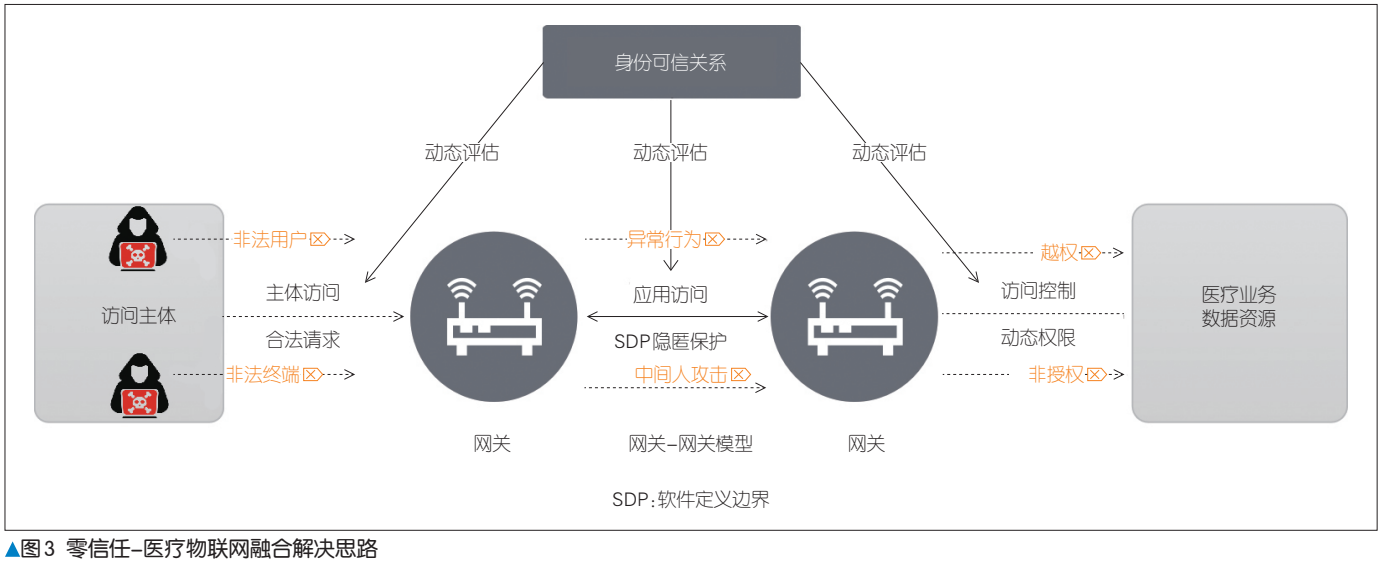
（1）零信任控制平台

零信任控制平台是整个框架的“大脑”和中心控制点，包括信任策略引擎、策略控制中心、物联环境感知、智能身份分析等组件。零信任控制平台负责医疗终端身份验证方的通信，统一协调身份验证和授权分发，定义和评估相应的访问策略，动态调整医疗终端的接入权限。零信任控制平台通过策略控制中心对用户和设备建立或关闭资源连接，进行自动配置、动态授权和策略决策；通过信任策略引擎为给定的主体授予访问权限，对策略控制中心下达信任指令和收集评估状态；通过物联环境感知识别环境和设备，进行风险通报；通过智能身份分析实现访问控制的日志上报和持续评估。

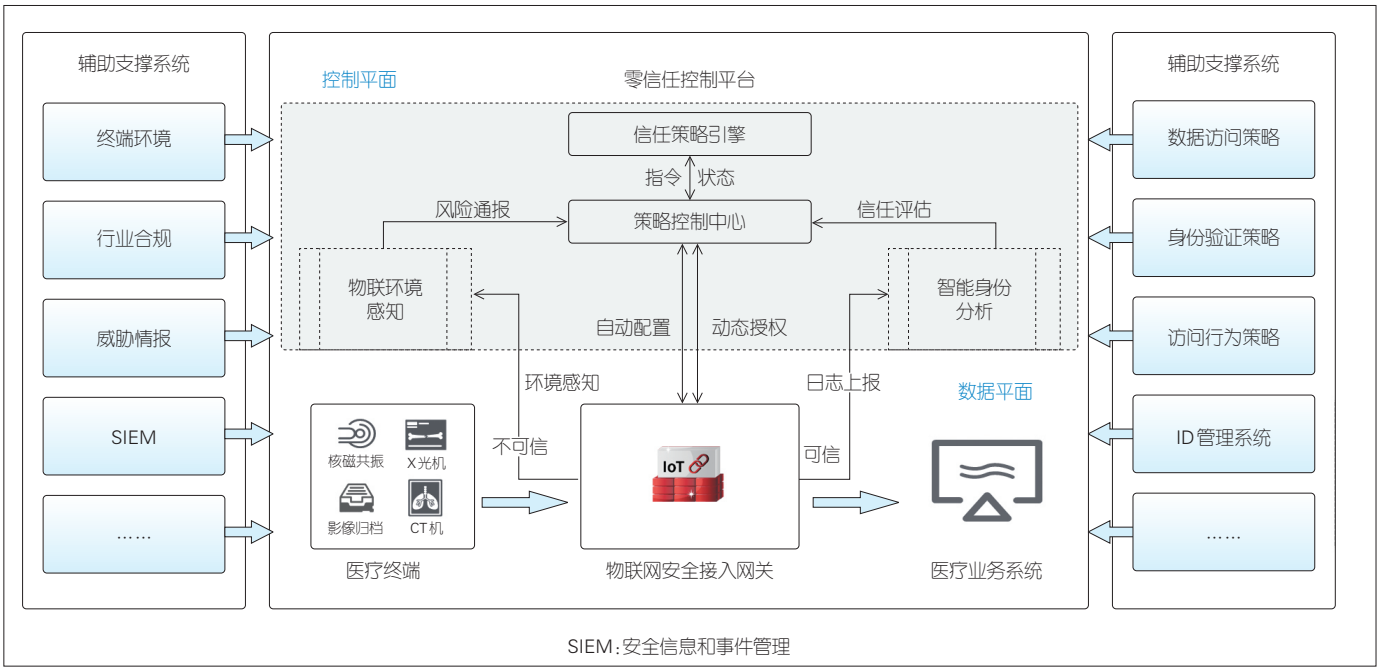
（2）物联网安全接入网关

物联网安全接入网关是确保业务安全访问的第一道关口，是动态访问控制能力的策略执行点。物联网安全接入网关主要负责监视主客体间的访问连接，建立安全传输通道，从零信任控制平台接收控制信息，并只接受经过零信任控制平台确认的医疗终端的用户访问连接请求，保证只有经过授权的主机才能访问到受保护的医疗业务系统。

（3）医疗终端



▲图 3 零信任–医疗物联网融合解决思路



▲图4 零信任–医疗物联网融生安全框架

医疗终端是访问主体，在主体实施信任评估前均处于不信任状态，通过策略引擎和策略控制中心实施信任评估。

（4）医疗业务系统

医疗业务系统是访问客体，初始的资源隔离、策略发现和自动化配置使得医疗业务系统始终处于受保护资源的资源访问状态。

（5）相关辅助支撑系统

除上述核心组件外，还需要引入辅助支撑系统，包括数据访问、身份验证、行为分析、ID管理、威胁情报、终端环境、行业合规、安全事件等。这样能够为零信任控制平台的策略生成及安全态势提供决策依据，从而达到安全联动效果。

4 零信任–医疗物联网融生安全框架的应用

基于零信任–医疗物联网融生安全框架的网络安全体系建设模糊了传统基于边界的物理或网络位置，而授予用户或设备认证和授权的隐式信任，符合网络安全应用趋势，能够在IoMT安全建设中支持设备统一管理、安全准入控制、设备行为分析3项安全基线应用，并实现终端环境安全检测、动态可信接入、安全加密通道3项安全创新应用。

（1）设备统一管理

设备统一管理需要对所有医疗终端进行统一分组管理，查看所有医疗终端的状态，并针对终端进行安全策略集中下发等，为零信任控制平台提供终端风险状态判定依据。

（2）安全准入控制

安全准入控制网络支持在边缘接入层采用安全隔离技术，对不同主客体之间建立物联网安全通道，设定必要的分布式安全访问控制措施，并利用先进的设备指纹、智能画像、精准识别等技术，对接入的设备进行安全准入控制，基于预设安全策略对接入节点进行安全访问控制，避免非法仿冒设备入侵。

（3）设备行为分析

物联网医疗终端形态多样化，地理位置分散，缺少值守，且一般携带敏感数据，因此容易发生设备盗用并以此为跳板侵入到医疗内部核心网络，从而造成重大损失。我们可通过智能学习和行为关联分析，构建医疗终端的正常行为模型，以达到安全管控的目标。

（4）终端环境安全检测（创新点）

IoMT终端环境安全检测具体包括对感知层网关自身环境检测、文件感知、容器感知、通信感知、状态感知、设备感知等，主要从终端环境出发，划分不同的终端安全等级，用于安全探测物联感知终端设备连接状态，监控设备数据传输安全，对终端的控制实现细粒度控制，改变以往的粗放式管理。

（5）动态可信接入（创新点）

动态可信接入可以融合零信任技术和IoMT接入的安全管控能力，将原有的静态防御改为动态防御，全面、动态、持续感知医疗终端和网关进程，能够实时度量和控制资源访

问行为，实现双向身份鉴别机制，支撑与业务的紧密结合，从而保证人员和医疗设备接入时身份的可信任。

（6）安全加密通道（创新点）

安全加密通道可以将零信任主客体间的动态可信安全访问能力赋能到IoMT中，建立医疗终端和医疗业务系统间的安全可信连接，改变传统的“先连接后认证”方式，向基于零信任的“先认证后连接”方式转变，实现对IoMT专用传输通道的安全加密，从而保障数据的传输安全。

5 结束语

零信任–医疗物联网融生安全框架提供了一种全新的安全访问思路，形成了一种与网络位置无关的动态访问控制方案，支持用户建立全局的安全控制策略。根据被访问客体的安全信任状态对访问主体进行授权，持续监测评估访问过程安全性和信任状态，自动编排更新身份访问策略配置，动态调整访问权限，实现基于身份/属性/权限等级策略的细粒度访问控制，满足医疗物联网创新技术应用安全需求。零信任的深度应用将会催生策略智能调优的手段。如何针对目标资产、组件、访问实体等实现智能化的动态安全风险评估和策略配置，仍然需要我们在自动化系统、深度学习、智能控制等领域进行深入研究，从而应对零信任安全访问网络建设中的策略自动发现、有限访问控制、缺乏高效检测防御的应用挑战。

参考文献

[1] 杨惠杰, 周天祺, 桂梓原. 区块链技术在物联网中的身份认证研究 [J]. 中兴通讯技术, 2018, 24(6): 3–40. DOI: 10.19729/j.cnki.1009–6868.2018.06.007
[2] 蒋昆. 西京医院: 医疗物联网安全的思考与实践 [J]. 科技新时代, 2018, (4): 38–40
[3] 陈庆龙, 石春花, 郝文延. 物联网医疗系统安全和隐私保护方法研究 [J]. 医学信息学杂志, 2022, 43, (1): 67–72. DOI: 10.3969/j.issn.1673–6036.2022.01.013
[4] 田由辉. 基于零信任架构的网络安全防护思路 [J]. 信息技术与信息化, 2020, (5): 154–157. DOI: 10.3969/j.issn.1672–9528.2020.05.048
[5] 戴家刚, 杨胜利, 周玉宝. 医院物联网体系结构和关键技术研究 [J]. 中国新通信, 2015, 17(21): 20. DOI: 10.3969/j.issn.1673–4866.2015.21.016
[6] 张程.医院物联网方兴未艾 [J]. 检察风云 , 2022, (5): 72–73
[7] NIST. IoT device cybersecurity capability core baseline：NISTIR 8259A [EB/OL]. (2020–05–29) [2022–11–28]. https://csrc. nist. gov/publications/detail/nistir/8259a/final
[8] 郭丽娜, 路杰, 郭玮娜. 浅谈物联网在智慧医院建设中的应用 [J]. 中国卫生信息管理杂志, 2016, 13(3): 299–302. DOI: 10.3969/j. issn. 1672–5166.2016.03.016
[9] 沈志强. 医疗物联网的安全问题及策略 [J]. 信息与电脑, 2017, (21): 178–179, 183. DOI: 10.3969/j.issn.1003–9767.2017.21.069
[10] KINDERVAG J. Build security into your network´s DNA：the Zero Trust network architecture [EB/OL]. (2010–11–05) [2022–08–23]. https://www.yumpu. com/en/document/view/17914587/build–security–into–your–networks–dna–the–zero–trust–ndmnet
[11] NIST. Zero Trust architecturel: NIST special publication 800–207 [EB/OL]. (2020–08–10) [2022–08–23]. https://nvlpubs. nist. gov/nistpubs/SpecialPublications/NIST.SP.800–207.pdf
[12] 张宇, 张妍. 零信任研究综述 [J]. 信息安全研究, 2020, 6(7): 608–614

作 者 简 介

景鸿理，天融信科技集团高级副总裁；主要研究领域为安全操作系统、网络安全、密码理论及工程应用；曾获国家科技进步二等奖2次、军队科技进步一等奖1次、党政密码科技进步一等奖1次。

屈伟，天融信科技集团资深战略咨询顾问，高级工程师；主要研究领域为数字化安全体系规划、智慧城市安全运营、健康医疗安全、电子政务安全、教育安全等。

刘治平，天融信科技集团CSA零信任专家；参与多项零信任及商用密码安全领域的标准规范编写，成功交付多个大型零信任及商用密码项目。