网络内生安全研究现状与关键技术

Research Status and Key Technologies of Network Endogenous Security

王瀚洲/WANG Hanzhou，刘建伟/LIU Jianwei
（北京航空航天大学，中国 北京 100191）
(Beihang University, Beijing 100191, China)

DOI：10.12142/ZTETJ.202206002
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20221129.0829.002.html
网络出版日期：2022-11-30
收稿日期：2022-10-15

摘要：网络正处于融合开放的发展趋势中，传统的由安全事件和等保合规驱动的外挂式、被动式的安全机制已无法满足业务的需求。认为以“架构决定安全”为核心理念的内生安全已成为下一阶段网络安全领域的发展方向。从现有安全技术出发，分析了前内生安全技术的缺陷及发展内生安全技术的必要性，介绍了内生安全的概念与演进阶段，梳理总结了包括拟态防御、可信计算、零信任、DevSecOps等路线在内的主流内生安全路线的研究现状，并从原理层面介绍了各路线的关键技术。

关键词：内生安全；拟态防御；可信计算；零信任；DevSecOps；物理层安全

Abstract: The network is in the development trend of integration and opening. The traditional external and passive security mechanism driven by security events and equal guarantee compliance cannot meet the needs of business. The endogenous security with "architecture determines security" as the core concept has become the development direction of the network security field in the next stage. Starting from the existing security technology, this paper analyzes the defects of the former endogenous security technology and the necessity of developing endogenous security technology, introduces the concept and evolution stage of endogenous security, and summarizes the research status of mainstream endogenous security routes including mimicry defense, trusted computing, zero trust, DevSecOps, etc. The key technologies of each route are introduced from the principle level.

Keywords: endogenous security; mimicry defense; trusted computing; zero trust; DevSecOps; physical layer security

随着信息通信技术的迅猛发展，信息网络系统已成为不可或缺的基础设施。然而，与网络发展相伴而生的网络安全问题也被急剧推到前所未有的高度。网络安全已经成为社会发展、国家安全的基础需求，也成为决定网络能否发挥最大化潜能和价值的关键因素[1]。

在网络架构融合开放的发展趋势下，网络安全从过去主要由安全事件驱动的静态被动式安全，到当前主要由等保合规驱动的动态主动式安全，正在向着下一阶段由具体场景需求驱动的内生智能安全演进。网络安全领域逐步达成共识——“架构决定安全”。也就是说，安全能力应在网络顶层设计构建时就做出充分考虑。对此，以网络系统的架构、机制、场景、规律等先天构建安全能力，并可后天自成长、自适应的“内生安全”理念应运而生。

基金项目：国家重点研发计划（2021YFB2700200）；国家自然科学基金（U21B2021、61972018、61932014）

1 前内生安全技术评析

网络安全技术的发展具有明显的代际发展效应。在内生安全技术之前的网络安全发展主要经历了3个阶段：以阻止入侵为目的的系统加固阶段、以限制破坏为目的的检测响应阶段、以系统顽存为目的的网络容侵阶段[2]。每一阶段的安全技术都呼应了其所面临的安全问题。在网络规模化部署中，这对已知特征和固化模式的攻击具有重要防护意义，但各阶段均以网络攻防对抗为核心思路，缺乏安全的顶层结构化设计，难以逃脱“道高一尺，魔高一丈”的安全困境[3]。

第1阶段的安全技术主要通过划分明确的网络边界，利用各种保护和隔离技术手段，例如用户鉴权与认证、访问控制、信息加解密、网络隔离等，在网络边界上部署，防止外部非法入侵与信息泄露，达到系统加固的目的。此类技术在确保网络系统的正常访问、鉴别合法用户身份和权限管理、机密数据信息安全方面有较强的防护作用，但这一阶段技术对部分攻击行为如用户身份假冒、系统漏洞后门攻击等显得

无能为力。

第2阶段的安全防护融合了保护、检测、响应、恢复四大技术。此阶段主要采用特征扫描、模式匹配等手段对系统状态进行检测与报警，寻找被植入的恶意代码并进行查杀，找出导致恶意代码可被植入的原因并用补丁的方式进行修补，发现不规范的蓄意行为和特征并加以抑制。此阶段技术高度依赖检测能力，且攻击方发展出对应的伪装欺骗技术，导致不可能发现全部攻击。

第3阶段的安全防护在前两阶段的基础上叠加了信息生存技术。此阶段网络在假设漏洞后门不可避免，攻击和意外事故已然、必然发生的条件下，通过实时状况感知与响应，实时调整安全策略，采用自我诊断隔离、还原重构等手段，仍可在限定时间内完成全部关键使命。容侵技术可以作为网络系统的最后一道防线，使攻击侵犯的影响降到最低。但目前容侵技术主要基于门限密码秘密共享理论的容侵模型设计，尚未达到规模化实用的程度，并且模型的建立依赖大量先验知识与实际经验，对于未定义的攻击行为仍然较难防范。

2 内生安全概念

2.1 定义及特征

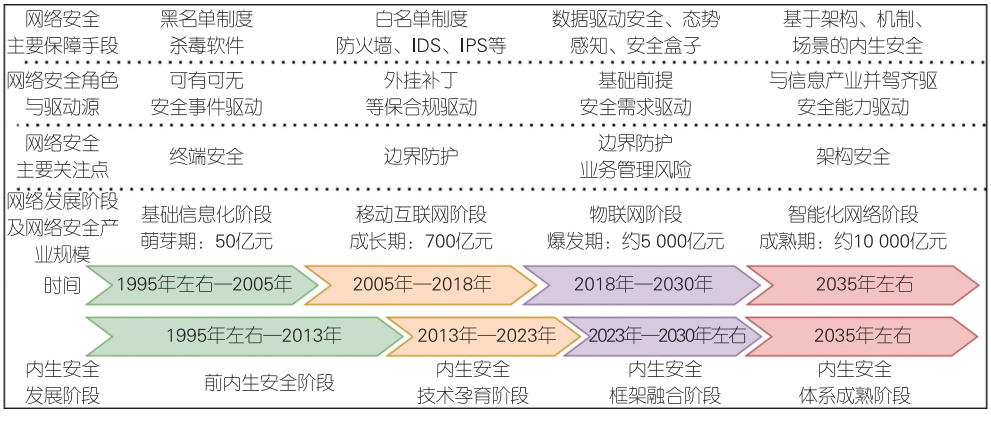
内生安全最早于2013年由邬江兴院士提出。经过学术界、产业界的持续关注，内生安全概念与愿景逐步清晰——内生安全是以网络中各类网元设备自身的安全能力为基础，利用系统架构、算法、机制或场景等内部因素获得安全功能或安全属性，协同配合构建的综合安全体系。内生安全系统至少具有以下基本特征：（1）先天构建。安全能力需要与网络系统的设计与建设同步进行、同步建成，同时安全能力应与网络业务功能全面、紧密耦合。（2）后天成长。系统能够通过与运行环境的交互作用，使自己能够适应环境，应对安全事件，随网络环境变化动态提升安全能力[1,4]。

2.2 演进阶段

在技术层面如何实现内生安全，目前仍未形成统一的技术框架与构建方案。内生安全的演进需经历3个阶段的技术与产品革新（如图1所示），才能使真正具备内生安全的网络系统实现落地[1]。

在内生安全发展的初级阶段——技术孕育阶段，基于不同技术路线的内生安全方案逐渐涌现。多样的内生安全方案被提出，并初步实现积累、融合。此阶段的目标是构建一个基本完备的、融合的内生安全体，逐步由分散式的建设转向统一架构的、可规划的建设。在网络层面，该阶段网络架构特征为端到端、分层网络，但未形成统一的安全构架。在技术层面，该阶段基于拟态防御、零信任、可信计算等技术，初步构建网络内生安全能力；基于DevSecOps、软件安全开发周期等框架，初步实现网络中软件应用安全；基于改良互联网协议（IP）协议、软件定义安全、网络功能虚拟化（NFV）等技术，初步实现具备原子化安全能力的网元；基于密码、量子密钥分发（QKD）等技术，初步实现数据安全能力；基于安全管理、人工智能、威胁模型、关联分析模型等，初步进行免疫能力构建。

在内生安全发展的中级阶段——框架融合阶段，内生安全发展的主要形式是架构的健全化与智能化。随着对未来融合网络架构的研讨，人们将形成内生安全架构的共识方案。在孕育期发展产生的各项成熟的安全技术之间并非竞争择优的关系，而是联合协作的关系。单一封闭的技术实现方案将不适用于未来智能、融合、开放的网络体系，各项安全技术将封装为原子化安全能力。借助人工智能调配，为业务量身打造最适合、最安全的网络，将有助于实现网络适配业务。在网络层面，该阶段初步形成了功能开放的架构底座，可为上层原子化安全能力提供支撑。在技术层面，原子化安全能力逐渐成熟，人工智能会逐步与网络安全能力相结合以提升网络免疫能力，此时边界、网元、应用、数据等安全能力将



▲图1 网络安全代际发展特征[5]与内生安全发展阶段

向智能化、协同化的方向发展。

在内生安全发展的高级阶段——体系成熟阶段，网络已具备健全的先天内生安全体系和全网一体化的后天免疫。随着与人工智能的进一步结合，网络将实现安全的弹性自治。网络的安全能力将形成高共识度的安全度量标准，网络也将形成泛在的、系统化的内生安全保障体系。

3 内生安全研究现状

解决现有网络内生安全问题的思路包含重新设计网络架构与进行增量式修补两种鲜明路线，并兼存寻求折中的演进路线。总体而言，目前已提出的解决方案均在某种程度上具备内生安全特性，实现内生安全的技术方案处于“多强并进”的状态。但目前内生安全研究在硬件、软件或协议层面均未达成足够共识，缺乏将不同技术路线下的内生安全解决方案整合起来的统一框架。各种内生安全路线及其特征如表1所示。

3.1 基于拟态防御的内生安全路线

基于拟态防御的内生安全最早由邬江兴院士提出。他认为带来安全问题的漏洞与后门是未知且不可避免的，同时一切技术都存在内生安全问题（包含伴生的显式副作用或隐式暗功能）。例如，可信计算在目标对象行为不都是可知或可预期的情况下难以保证安全可信，零信任架构难以消除分布式认证节点系统中的漏洞和后门威胁等。因此他提出一种结构或算法。该算法能在不依赖先验知识的条件下，将针对目标对象内生安全的网络威胁归一化为由可靠性和鲁棒性控制理论与方法能够处理的未知扰动。拟态防御通过条件规避的方法让攻击者无法形成有效的攻击，使必然存在的内生安全问题不会成为系统的安全威胁[6]。拟态防御作为一种通用安全技术正在逐步实现应用落地与产品化。基于拟态防御的云基础设施、网络切片防护方案、区块链安全增强方案等层出不穷。拟态构造的域名服务器、Web服务器等已经部署投入使用。以拟态服务器为例，图2展示了拟态防御与传统安全技术相结合的部署架构。

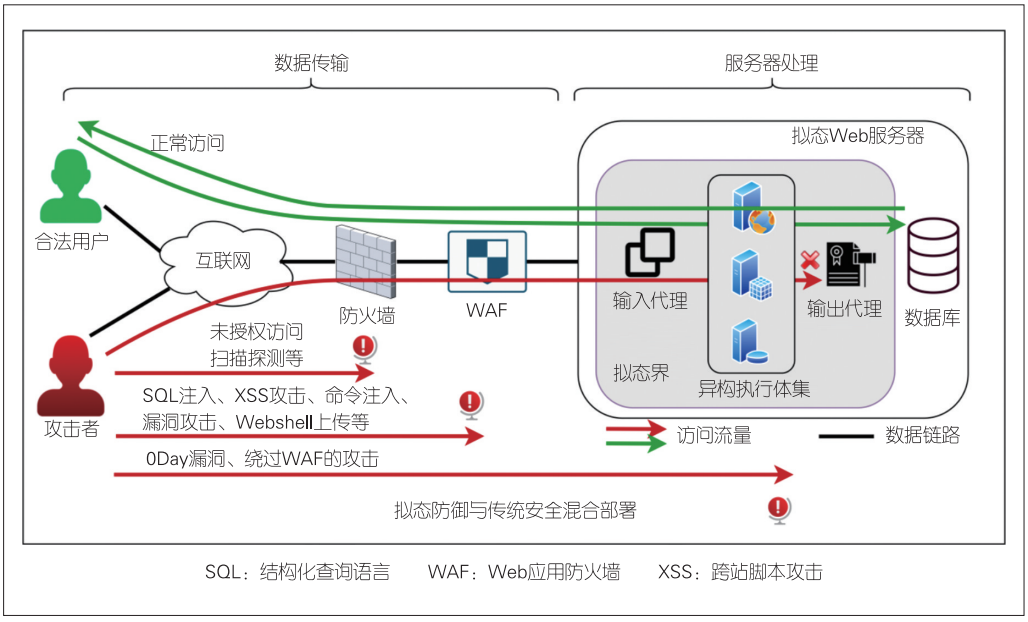
3.2 基于可信计算的可信网络内生安全路线

可信从行为预期的角度被可信计算组织（TCG）定义为：可信实体的行为总是以预期的方式，朝着预期的目标进行，产生的结果总是与预期一致。可信计算中存在一个由底层硬件确保安全性的信任根和一个在系统硬件层面上独立于原宿主系统的可信子系统。可信节点以监控者的身份，主动逐级从可信根向上层执行安全策略，实施行为控制，并返回审计信息，建立由硬件结构到操作系统、应用系统的信任链。上层只有获取底层信任后才能正常运行[7]。

▼表1 各种内生安全路线特征

序号	技术路线	基本思想	关键技术/架构	技术优势	适用场景
1	拟态防御	通过执行体异构性使攻击者很难同时多点攻破；通过策略性的动态变化扰乱攻击链的构造和生效过程	动态异构冗余架构	能非特异性地免疫未知的安全威胁	理论上适用于全部软硬件信息化产品，但因其与现有架构差异较大、部署成本较高，常用于高安全需求的场景
2	可信计算/可信网络	通过规定限制接入终端的身份、状态、行为获取可信身份，通过可信传输、可信连接、身份认证等手段，将单个终端网元的可信状态扩展形成多个节点互联的可信网络	可信连接架构TCA	技术成熟、规模化部署基础较好、国产自主可控	主要应用于安全等级较高的集中管理场合，如局域网办公自动化环境、工控系统、云计算、物联网等领域
3	零信任	“永不信任，始终验证”；缩小到单个资源组的网络防御边界；动态认证授权+精细化的访问控制	软件定义边界、身份和访问控制、微隔离	契合企业服务上云后的安全需求、不依赖边界安全	目前常应用于企业网络，实现远程访问等，未来有望规模应用至物联网
4	DevSecOps	安全左移，源头风险治理；敏捷右移，安全运营敏捷化；人人为安全负责，安全嵌入开发整体流程体系中	CNAPP、RASP、IAST、BAS等	注重人员安全意识培训、安全运维更高效、安全可度量	目前多应用于软件供应链安全、云原生安全，实现应用级、软件级的安全
5	物理层安全	利用物理信道特征、终端制造容差、目标用户地理位置等物理特征，增强数据传输、鉴权认证、数据完整性保护等能力	物理层身份认证；物理层密钥生成；物理层安全传输	轻量化、安全与通信过程绑定、“一次一密”	多数技术应用于无线通信，未来有望大规模应用于6G通信
6	改进IP协议	针对现行IP协议存在的安全性问题，通过在扩展报头中增加身份标识、服务标识等通过改进协议增强网络内生安全性	IPv6、New IP等	在网络层提供安全增强服务、技术上部署难度小	面向宏观、全面的互联网，并借助5G和AI等构建一个智能化的全新互联网
7	伴生网络对抗学习	构建真实网络的1∶1平行数字伴生网络，通过对抗学习生成“网络疫苗”，并依靠智能化预测增强真实网络的安全能力	数字孪生网络、人工智能	降低试错成本、可进行预测性运维	易于建模的网络，可为单一网络域（如接入网、传输网、核心网、承载网等）子网，也可以是端到端的跨域网络

AI：人工智能
BAS：入侵与攻击模拟
CNAPP：云原生应用程序保护平台
IAST：交互式应用安全测试
IP：互联网协议
RASP：应用运行自我保护
TCA：可信网络连接架构



▲图2 拟态防御与传统安全技术相结合的部署架构

可信计算仅提供设备层面的可信，在网络层面以某个或多个可信网元为基础，通过可信传输、身份认证、可信网络连接等手段，构建可信网络连接架构，将单个终端、网元的可信状态，扩展到多个节点互联的可信状态。其核心的思路是对访问者的身份、状态、行为加以规定限制，以接入的自由性换取网络其他节点的信任[8]。2004年TCG提出可信网络连接（TNC）[9]。如图3所示，2007年中国可信计算标准网络组提出可信网络连接架构（TCA），并于2013年将其正式发布为国家标准GB/T 29828–2013《信息安全技术 可信计算规范 可信连接架构》[10]。

3.3 基于零信任架构的内生安全路线

零信任架构最早由Forrester首席分析师J. KINDERVAG提出，是一种基于“永不信任，始终验证”与最低权限原则的网络安全体系，如图4所示。它将网络防御的边界缩小到单个资源组，不再依据用户所处网络位置来决定是否安全可信，而是在对行为的精细化安全风险评估的基础上，强制性地通过动态认证和授权来重构访问控制的信任基础，实现网络系统内生安全。零信任执行以下3个基本原则：（1）所有用户均需要基于访问主体身份、网络环境、终端状态等尽可能多的信任要素进行持续验证和动态授权；（2）所有授权的访问均应遵循最低权限原则按需授权；（3）所有的访问请求都应当被记录和跟踪[11]。零信任安全是安全策略从静态向动态转化的结果，对现有网络安全架构进行了改良。相比于拟态防御，零信任架构对网络架构的改动较少，得到了较为广泛的应用。

零信任是近年来互联网、网络安全企业研究推进的热点技术，并在发展中产生了不同的技术路线，例如Google的Beyond Corp模型、Beyond Prod模型，Gartner的持续自适应风险与信任评估（CARTA）模型、零信任网络访问（ZTNA）模型，Forrester的零信任架构等[12]。远程访问是实施零信任的主要驱动与优先选择。零信任在企业专网安全保障场景下有较为广泛的应用，例如远程办公、远程运维、远程分支机构接入、第三方协作等场景[13]。

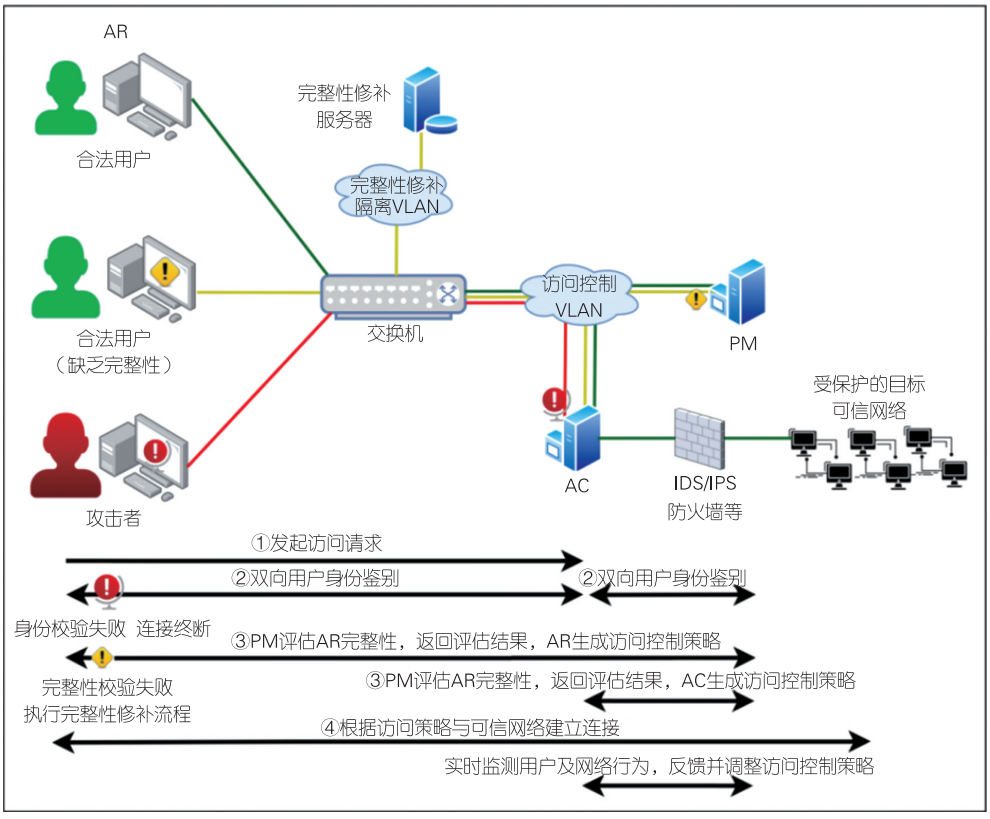
3.4 基于DevSecOps的内生安全路线

DevOps是一套将开发、运维、质量保障相结合，通过实施自动化流程与高效沟通合作，使软件开发整体过程更加快捷可靠的理念，如图5所示。DevSecOps是DevOps概念的延续，它将安全无缝集成到软件开发运维过程中，要求软件开发团队和运营团队与安全团队密切合作，人人参与软件的安全治理，对DevOps周期中每个阶段的安全负责。

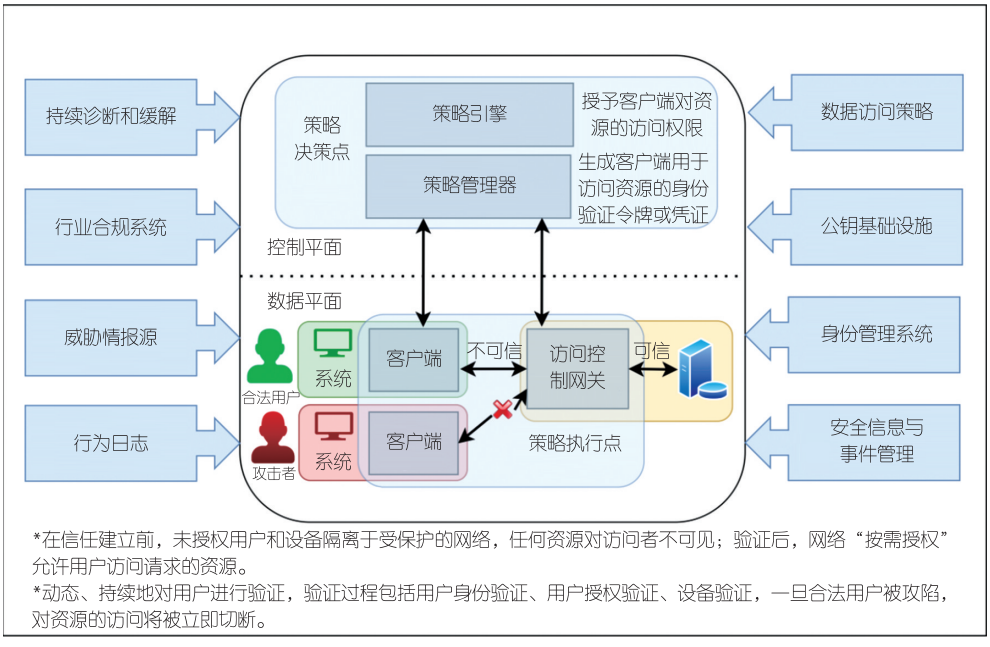
DevSecOps是一种基于安全治理的应用级内生安全实施方案，在两个层面上保障软件开发全流程的内生安全：（1）基于安全左移的理念，在软件架构设计阶段充分考虑安全因素，并基于应用运行自我保护（RASP）技术、软件成分分析（SCA）技术、交互式应用安全测试（IAST）技术等，在开发环节使软件“天生”安全；（2）基于敏捷安全的理念，在运维过程中积极实施入侵与攻击模拟（BAS）以及安全度量，通过自动化技术实现敏捷自适应、软件与网络环境的共生进化。目前DevSecOps的应用场景主要为软件供应链与云原生的安全保障。因能够契合当前互联网行业产品迭代的需求，该技术已在微软、谷歌、腾讯等实现规模化应用[14]。

3.5 基于物理层安全技术的内生安全路线

随着5G网络的规模化发展，移动通信的网络安全问题成为研究的重点。物理层安全技术的本质是利用通信双方无线信道的特征、无线终端的制造容差、目标用户的地理位置



▲图3 TCA可信连接架构部署示例



▲图4 零信任安全架构[11]

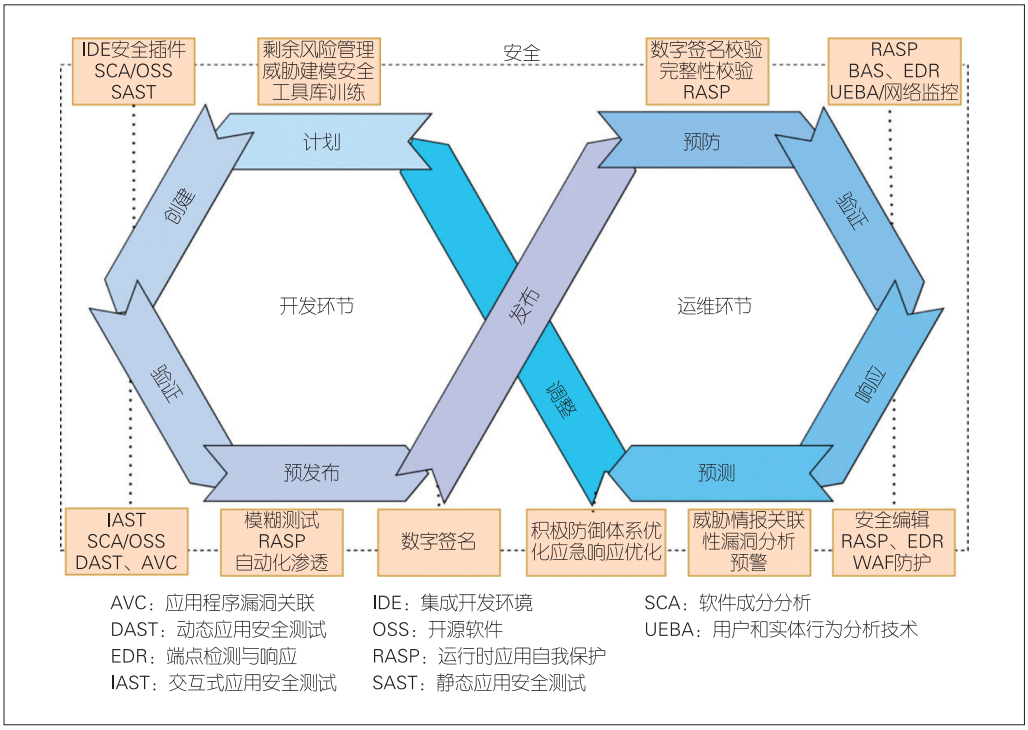
等物理特征，经过信号处理后，提取物理特征指纹，实现绑定于设备自身、通信信道上的身份识别、密钥生成、安全传输。与上层安全技术相比，物理层安全技术由于具备轻量级、难复制的特点，可以解决高速率数据传输加密、鉴权认证增强、数据完整性保护等多方面的难题。

目前不少学者针对Wi-Fi、ZigBee、LoRa、长期演进（LTE）等常见的无线通信协议进行了设备指纹提取的研究，典型的研究方法包括信号功率谱方法、差分星座轨迹图方法等，但物理层安全技术并未得到规模化应用[15-16]。

3.6 基于改进IP协议的内生安全路线

现有的IP协议围绕着开放、互联、安全、可信的核心使命，具备无连接性、分组交换、尽力而为的转发、基于IP地址的寻址等特点，并且经过超半个世纪的补充与完善，形成了IPv6、IPsec、信息中心网络（ICN）、命名数据网络（NDN）等改进方案。这些方案以数千条请求评论（RFC）文档的形式，为IP协议打补丁或增加附加功能。

当前人们对IP协议的具体批判主要针对尽力而为的转发与基于IP地址的寻址，认为IP协议虽然完美地完成了开放与互联的使命，但是在安全与可信上有所欠缺。这是因为：IP协缺乏内生的可信和安全机制，无法保证



▲图5 将安全集成于开发运维的DevSecOps流程框架

用户信息的完整性和不可篡改性；IP协议缺乏内生的资源感知和管控能力。在B5G/6G、工业互联网等场景下，现有基于IP协议的网络体系已经很难适应未来的业务需求。因此，针对下一代网络架构的设计，如何在开放与互联主题不变的条件下，实现安全与可信是IP协议的改进方向。IPv6、NewIP是两项改进IP内生安全性的热门方案。

IPv6的初衷是为了解决IPv4地址枯竭的问题。相比于IPv4，IPv6的头部长度从32位扩容到128位。地址扩容使得IPv6的安全性得到极大提升，这主要体现在以下几方面：

（1）可溯源与防扫描。攻击者若要实现像在IPv4条件下的网段主机地址扫描是极其困难的。同时IPv6终端之间可建立点对点连接，无需地址转换，在攻击发生后易于及时处置，因而系统能够实现高效的信息安全治理。

（2）IPv6默认支持IPsec协议。IPv6通过扩展认证报头（AH）和封装安全载荷报头（ESP）实现加密和验证功能，不需要额外对IPSec扩展包头进行处理。

（3）IPv6支持真实源地址验证体系结构（SAVA）[17]（RFC5210）。相比于IPv4协议只基于目标地址进行路由选择的转发机制，IPv6可通过SAVA体系识别并阻止伪造的源地址报文被转发，使每一个转发分组的IP源地址都是真实的。与IPv4相比，IPv6在安全性方面进行了预先设计与考虑，但仍然存在一些难以解决的安全风险。虽然使网络的安全性有一定的提升，但IPv6的改进仍然是增量式的，内生安全机制仍然是不完备的[18]。

New IP由华为网络技术实验室于2019年提出，旨在提供万网互联、万物互联的新连接能力、确定性传输及大吞吐量传输的新服务能力、安全可信及用户可定义的新内生安全能力，在保留原IP协议高生存性、高可达性、尽力而为的核心优势的前提下，提升确定性转发、高互联、内生安全等新能力，实现能力的增强与扩展，满足更高要求、更复杂的应用业务需求。其基本实现思路是在包头中增加服务标识与身份标识，使得网络可以根据标识优先级，实现更适配业务特征的资源调配及安全保障[19]。在内生安全能力提升方面，New IP架构主要提升了端到端通信业务安全与网络基础设施安全两大方面。New IP基于可信身份管理、真实身份认证、审计溯源、访问控制、密钥管理等安全模块，构建了由可信节点参与的、可审计的安全域。同时，New IP采用去中心化技术构建网络基础设施，提供不依赖于根节点的证明，从而解决了美国根节点权限过大、单点失效等问题[20]。

3.7 基于伴生网络对抗学习的内生安全路线

伴生网络是基于数字孪生技术将物理网络在数字空间中映射出1∶1平行运行的数字化虚拟网络。伴生网络通过采集网络设备实时数据，利用模型构建、修正与融合技术，构建与物理网络一致的数据模型，进而可以实现低成本试错与智能化预测。于全等提出类生物免疫机制的网络安全架构。该网络架构搭载了其自身的数字孪生体——平行伴生网络，并在伴生网络中加载高强度的人工智能攻击，通过攻防对抗学习生成“网络疫苗”，依靠强于攻击者的超级算力动态构成先于攻击的防御策略，从而获得网络空间的对抗优势[21]。

然而，在机理上网络空间的安全防护与生物体的免疫是否可以类比，目前仍然存在疑问。此外，基于目前人工智能的发展水平，人们尚未能构建可以发现创造性的、超出现有人类认知的攻击方式的框架，只能就某一维度的攻击方式进行挖掘。

因此，基于伴生网络对抗学习的安全能力并不具有完备性，不能完全取代其他安全工具，而是起到相辅相成的作用。

4 内生安全关键技术

当前网络内生安全仍处于技术孕育阶段，因此梳理各发展路线上的关键技术，开展未来网络内生安全的关键技术识别，将有利于技术的融合与统一架构的形成。本章将从技术层面对拟态防御、可信计算、零信任等路线的关键技术及其在内生安全领域的作用加以介绍。

4.1 拟态防御关键技术

邬江兴院士等将移动目标防御（MTD）技术的动态性与*N*-变体系统的异构冗余特性相结合，提出了基于动态异构冗余的拟态防御模型[22]，如图6所示。系统通过分发器将输入复制*N*份，并通过动态选择算法将相同或相异的组件组合成*N*个异构执行体（每个异构执行体分别独立处理输入），之后将*N*份执行结果交给表决器处理。当至少有*K*个执行体正常工作时（*N*=3、*K*=2的三模冗余架构最为普遍），我们就可以认为整个系统是正常运行的。同时，系统具有动态切换机制，可根据运行过程中产生的告警/报错信息（或在固定时间后），将旧的异构执行体替换为可信的新重构的异构执行体，从而实现更高的动态性[23]。

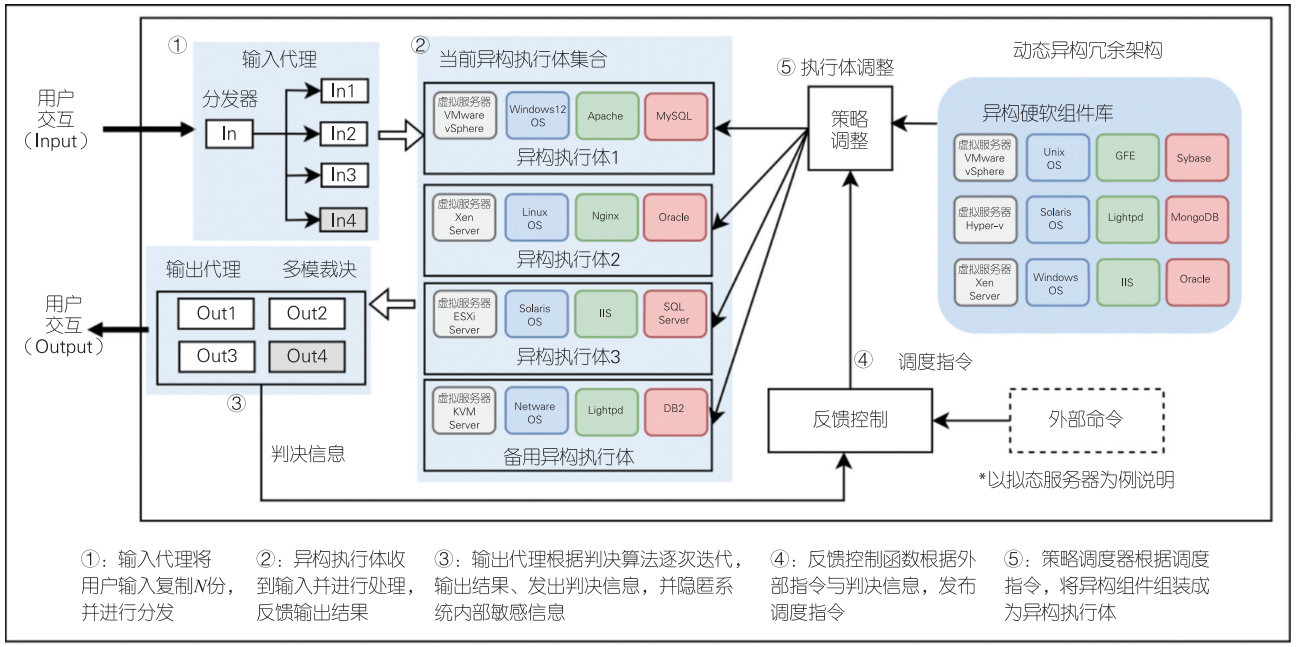
将动态异构冗余架构应用于网络内生安全的构件后，邬江兴院士等提出全维可定义多模态智慧网络[24]。该网络系统的异构资源池由平台、系统、部件、模块多层面上的网络功能组成，包括异构的网络拓扑、寻址路由、交换模式、网元形态、传输协议等。网络通过人工智能技术、智慧化网络管理机制，从异构资源池中选取不同层面上的网络技术，组成不同模态的网络执行体集，实现网络层面上的拟态防御。

4.2 可信网络关键技术

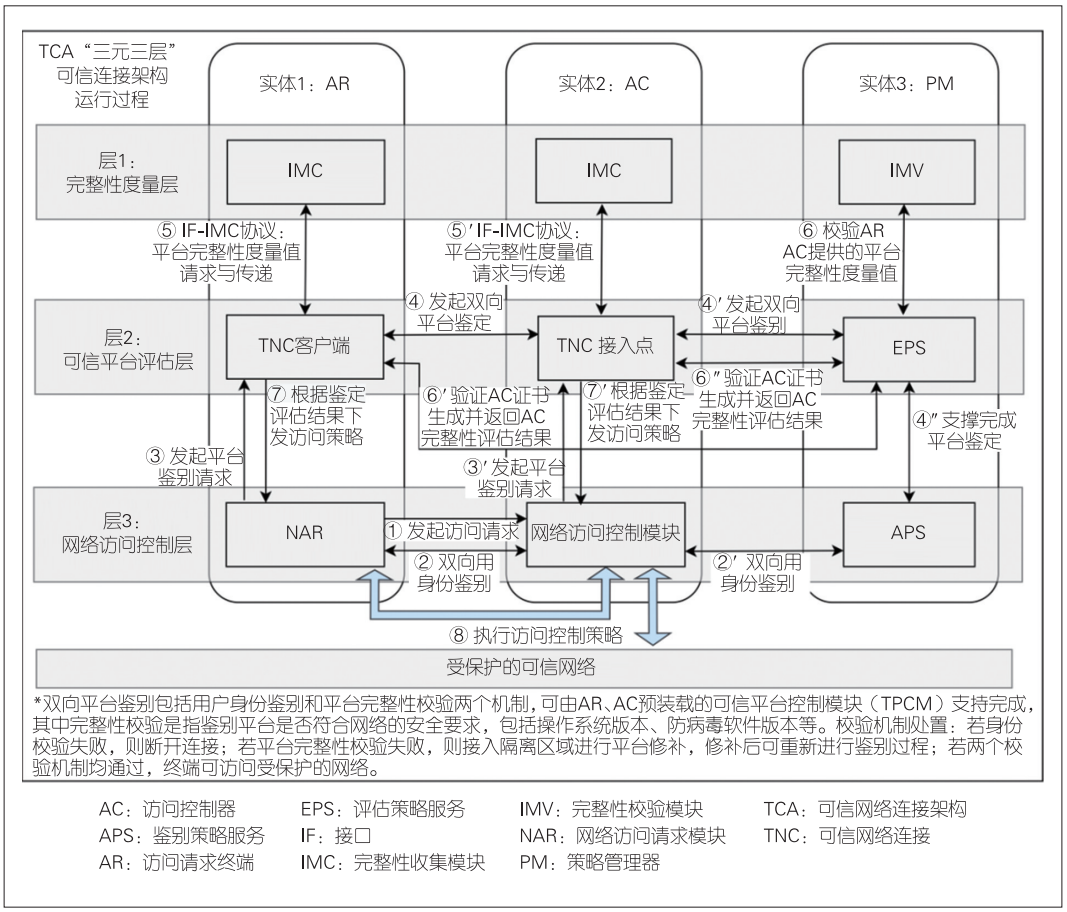
在可信计算与可信网络架构TNC基础上[9]，中国提出了具备主动免疫机制的TCA，如图7所示。TCA三元三层网络架构由实体、层、组件和组件间接口组成。通过多步骤的鉴别、认证，TCA可以实现身份鉴别、平台鉴别、完整性度量、策略管理、保密通信等功能。在鉴别身份、判断被授权允许访问网络的基础上，TCA还要检查终端当前的完整性及其他安全属性是否与网络要求的安全策略一致，从而为网络环境提供稳定可靠的保证[10]。

4.3 零信任关键技术

美国国家标准与技术研究院（NIST）将零信任的核心



▲图6 动态异构冗余架构



▲图7 可信网络连接架构关键流程

技术归纳为软件定义边界（SDP）、身份和访问管理、微隔离[11]，如图8所示。

SDP基于安全策略可灵活创建边界，用于将服务与不安全的网络隔离开，提供按需、动态的网络安全。区别于传统传输控制协议（TCP）/IP网络的默认允许连接，在没有经过身份验证和授权之前，受保护的资源对于终端用户是完全不可见。SDP主要由SDP控制器、SDP安全网关、SDP客户端三大组件构成。其中，SDP控制器用于认证和授权SDP客户端，并配置SDP网关的连接；SDP网关与控制器通信并强制执行策略，控制客户端的访问流量。

身份和访问管理可确认访问者身份的合法性，并为合法用户在规定时间内按照访问权限来要求受保护资源提供一种安全的方法。身份和访问管理技术的发展经历了从粗粒度到细粒度的转变，实现了设备内部不同端口之间的流量控制。此外，基于角色的访问控制（RBAC）、基于属性的访问控制（ABAC）、基于任务的访问控制（TBAC）等均各有侧重。对于零信任网络的身份与访问控制（IAM），目前人们正在提升策略的动态性，并尝试将已有技术的优势加以融合。

微隔离是一种细粒度的边界安全管理策略，是边界隔离不断向受保护资源靠近的结果，主要以软硬件结合的方式，通过虚拟化环境中划分逻辑域来形成逻辑上的安全边界，实现细粒度的流量监测、访问控制和安全审计功能。目前微隔离的实现方法主要分为物理安全设备（防火墙、IPS、IDS等）、主机代理、软交换（Softswitch）和虚拟机监视器（Hypervisor）等方式[25]。

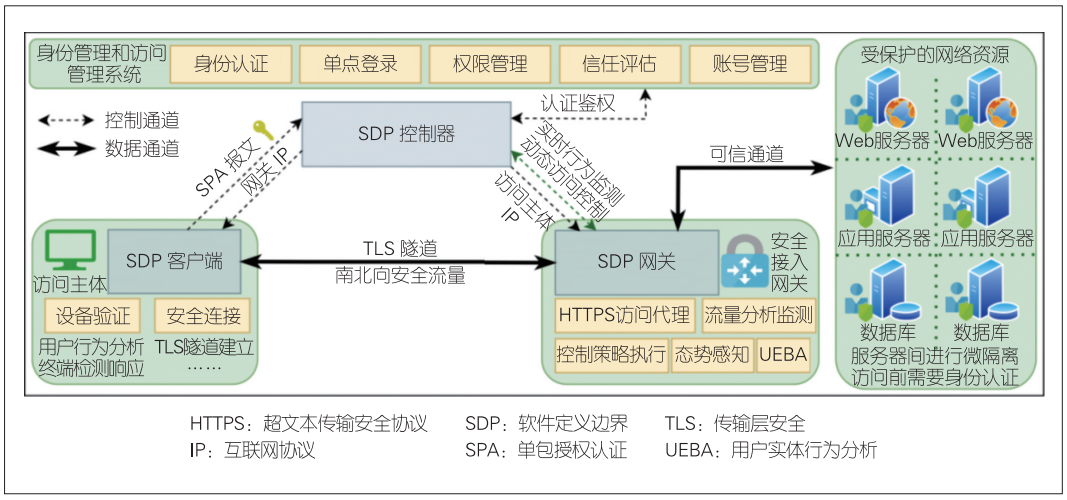
4.4 DevSecOps关键技术

DevSecOps将多项安全技术集成于软件开发的整体流程中，其基本技术架构如图9所示。其中，云原生应用程序保护平台（CNAPP）是一个整合了安全和合规方法的功能集，作为云原生应用安全开发的基础设施保障与框架；应用运行自我保护（RASP）内置于应用内部，通过钩子（Hook）关键函数，实时监测应用在运行时与其他系统的交互过程，可根据上下文环境识别并阻断攻击；交互式应用安全测试技术（IAST）通过在软件代码运行的中间件上插入探针，自动识别和判断应用中的安全漏洞；软件成分分析（SCA）通过对二进制软件的组成部分进行分析，清点开源软件的组件及其构成和依赖关系，识别已知的安全漏洞或者潜在的许可证授权问题，并把这些风险排查在应用系统投产之前，也适用于应用系统运行中的诊断分析；入侵与攻击模拟（BAS）通过持续模拟针对企业资产进行攻击的剧本及payload，验证企业安全防御的有效性[14]。

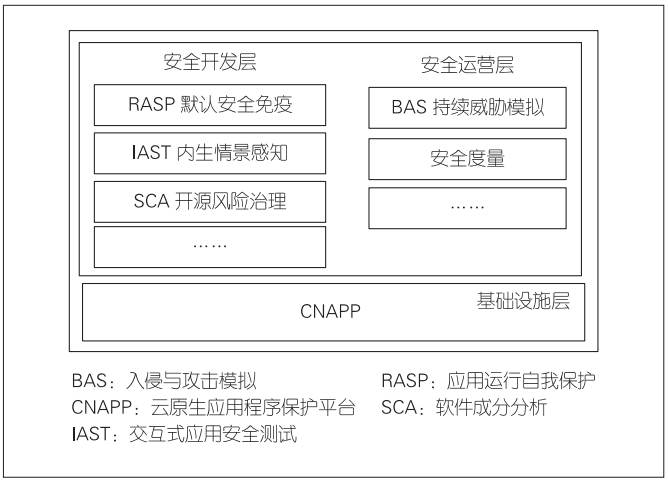
4.5 其他内生安全技术

4.5.1 增强的密码技术

密码技术是安全领域的基础，主要基于传统数学难题的诸多公钥密码体系。由于量子计算正面临严峻的安全威胁，



▲图 8 基于软件定义边界、身份和访问管理、微隔离三大关键技术的零信任网络架构



▲图 9 DevSecOps 安全技术栈架构

传统密码学又发展为两种：利用量子力学性质来保护数据的量子密码学和能够抵抗量子算法攻击的经典密码学，其中后者又被称为后量子密码学。

量子密码协议目前正处于量子密钥分配协议遥遥领先、其他协议有待突破的状态。量子密钥分配是一种通信双方通过传输量子态来建立密钥的协议。最著名的 BB84 和 E91 协议通过量子态纠缠协商安全密钥。如果攻击者试图读出基于纠缠的量子态中的信息，量子态将不再处于叠加态，通信双方将意识到攻击者可能存在，即抛弃本次协商并重新进行新的协商[26]。

后量子密码学算法的实现方法主要有 4 种：基于格、基于编码、基于多变量、基于哈希。当参数选取适当时，目前还没有已知的经典算法和量子算法可以快速求解这些问题。

4.5.2 物理层安全关键技术

物理层安全技术是十分有前景的上层密码学技术的替代/增强方案，主要包括物理层身份认证、物理层密钥生成、物理层安全传输。

物理层身份认证技术利用无线终端设备在生产过程中不可避免的容差，针对设备发射信号的瞬态、稳态部分，提取设备特异性的“指纹”，进而实现对海量终端的认证。物理层密钥生成技术利用通信双方私有的信道特征，提供实时生成、无需分发的快速密钥更新手段，实现一次一密的完美加密效果。物理层安全传输技术则利用无线信道的差异设计与位置强关联的信号传输和处理机制，使得只有在期望位置上的用户才能正确解调信号，其他位置上的用户解调后只能得到置乱加扰、不可恢复的信息[15-16]。

4.5.3 数字孪生网络关键技术

数字孪生网络是物理网络的虚拟表示，基于数据和模型与物理网络实时交互映射，从而提供诊断评估、决策分析、预测性运维等能力，新的安全技术可以更容易地在数字孪生网络中得到测试与验证。

数字孪生网络架构可以分为物理网络层、孪生网络层、网络应用层。物理网络层主要包含构成端到端网络的物理实体，包括移动接入网、移动核心网、骨干网、数据中心网或端到端的跨域网络等。物理网络层通过接口实现与网络孪生体的网络数据和控制信息交互。孪生网络层包含 3 个关键子系统：数据共享仓库、服务映射模型和网络孪生体管理，分别提供网络数据采集和存储及统一接口服务、数据模型实例、全生命周期管理和可视化呈现服务。网络应用层通过接口将需求输入至孪生网络层，同时进行业务部署。充分验证后，孪生网络层将控制更新下发至物理网络层，以实现网络创新技术和应用低成本、高效率的快速部署[27]。

5 结束语

未来网络应具备内生安全属性已成为网络安全领域的共识，但目前内生安全概念的明确内涵（建设什么样的内生安全）与内生安全的技术路线（如何建设内生安全）尚未形成一致性方案。为此，本文从网络发展的角度分析了网络内生

安全建设的必要性，讨论了从当前多强并立状态到网络内生安全完全建成的演进阶段，简要介绍了当前包括拟态防御、可信计算、零信任、物理层安全在内的多条技术路线齐头并进的研究现状，并从架构的层面概述了各路线的关键技术，尝试梳理总结网络内生安全的现状。

参考文献

[1] 中兴通讯股份有限公司. 2030+网络内生安全愿景白皮书 [R]. 2021
[2] 吴礼发, 洪征, 李华波. 网络攻防原理与技术 [M]. 2版. 北京: 机械工业出版社, 2017
[3] 邬江兴. 网络空间内生安全发展范式 [J]. 中国科学: 信息科学, 2022, 52(2): 189–204
[4] WU J X. Cyberspace mimic defense: generalized robust control and endogenous security [EB/OL]. [2022–09–25]. https://www.doc88.com/p–9009953314809.html. DOI: 10.1007/978–3–030–29844–9
[5] 中国信息通信研究院. 2021年中国网络安产业白皮书 [R]. 2022
[6] 邬江兴. 网络空间内生安全(上册): 拟态防御与广义鲁棒控制 [M]. 北京: 科学出版社, 2020
[7] SHEN C X, ZHANG H G, WANG H M, et al. Research on trusted computing and its development [J]. Science China information sciences, 2010, 53(3): 405–433. DOI: 10.1007/s11432–010–0069–x
[8] MA J F, WANG C G, MA Z. Architecture of trusted network connect [M]// Security Access in Wireless Local Area Networks. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009: 401–423. DOI: 10.1007/978–3–642–00941–9_11
[9] 吕润璞, 郝福珍. TNC可信网络架构与元数据存取点研究 [J]. 计算机工程与设计, 2010, 31(2): 243–248. DOI: 10.16208/j.issn1000–7024.2010.02.037
[10] 李明, 李琴, 张国强, 等. 可信网络连接架构TCA的实现及其应用 [J]. 信息安全研究, 2017, 3(4): 332–338. DOI: 10.3969/j.issn.2096–1057.2017.04.007
[11] ROSE S, BORCHERT O, MITCHELL S, et al. Zero trust architecture [R]. 2020
[12] 张泽洲, 王鹏. 零信任安全架构研究综述 [J]. 保密科学技术, 2021, (8): 8–16
[13] 郭雪, 吴倩琳, 孔松. 零信任的行业应用场景分析研究 [J]. 中国信息安全, 2022, (2): 36–38. DOI: 10.3969/j.issn.1674–7844.2022.02.012
[14] 子芽. DevSecOps敏捷安全 [M]. 北京: 机械工业出版社, 2022
[15] 厉东明, 杨旋. 6G物理层安全技术综述 [J]. 移动通信, 2022, 46(6): 60–63
[16] 黄开枝, 金梁, 钟州. 5G物理层安全技术: 以通信促安全 [J]. 中兴通讯技术, 2019, 25(4): 43–49. DOI: 10.12142/ZTETJ.201904008
[17] WU J P, BI J, LI X, et al. A source address validation architecture (sava) testbed and deployment experience [R]. 2008
[18] DURDAĞI E, BULDU A. IPV4/IPV6 security and threat comparisons [J]. Procedia – social and behavioral sciences, 2010, 2(2): 5285–5291. DOI: 10.1016/j.sbspro.2010.03.862
[19] CHEN Z, WANG C, LI G W, et al. NEW IP framework and protocol for future applications [C]//Proceedings of NOMS 2020–2020 IEEE/IFIP Network Operations and Management Symposium. IEEE, 2020: 1–5. DOI: 10.1109/NOMS47738.2020.9110352
[20] 郑秀丽, 蒋胜, 王闯. NewIP: 开拓未来数据网络的新连接和新能力 [J]. 电信科学, 2019, 35(9): 2–11. DOI: 10.11959/j.issn.1000–0801.2019208
[21] 于全, 任婧, 李颖, 等. 类生物免疫机制的网络安全架构 [J]. 网络空间安全, 2020, 11(8): 6–10
[22] 秦俊宁, 韩嘉佳, 周升, 等. 基于异构冗余架构的拟态防御建模技术 [J]. 电信科学, 2020, 36(5): 31–38
[23] HU H C, WU J X, WANG Z P, et al. Mimic defense: a designed–in cybersecurity defense framework [J]. IET information security, 2018, 12 (3): 226–237. DOI: 10.1049/iet–ifs.2017.0086
[24] 邬江兴. 多模态智慧网络与内生安全 [J]. 网信军民融合, 2018, (11): 11–14
[25] 王群, 袁泉, 李馥娟, 等. 零信任网络及其关键技术综述 [EB/OL]. (2022–06–23) [2022–09–25]. https://kns.cnki.net/kcms/detail/51.1307.TP.20220622.0934.006.html
[26] 张雪, 高飞, 秦素娟, 等. 量子密码协议研究现状与未来发展 [J]. 中国工程科学, 2022, 24(4): 145–155. DOI: 10.15302/J–SSCAE–2022.04.015
[27] 孙滔, 周敏, 段晓东, 等. 数字孪生网络(DTN): 概念、架构及关键技术 [J]. 自动化学报, 2021, 47(3): 569–582. DOI: 10.16383/j.aas.c210097

作 者 简 介

王瀚洲，北京航空航天大学在读硕士研究生；主要研究领域为信息网络安全、网络体系结构。

刘建伟，北京航空航天大学网络空间安全学院教授、博士生导师、院长，享受国务院政府特殊津贴，现任国务院学位委员会第八届学科评议组成员、教育部高等学校网络空间安全专业教学指导委员会委员、中国密码学会常务理事、中国指挥与控制学会常务理事、中国电子学会网络空间安全专委会副主任委员、中国指挥与控制学会网络空间安全专委会副主任委员、中关村智能终端操作系统联盟副理事长；曾获国家技术发明一等奖、国防技术发明一等奖、中国指挥与控制学会科技进步一等奖等，所编写的教材获全国普通高校优秀教材一等奖、国家网络安全优秀教材、国家精品教材、全国优秀科普作品奖、第四届中国科普作家协会优秀科普作品金奖等；出版教材7部、专著2部、译著1部。