基于可信身份构建可扩展内生安全防护系统

An Extensible Endogenous Security Protection System Building Based on Trusted Identity

谢国涛，范云飞（中讯邮电咨询设计院有限公司，北京 100048）
Xie Guotao，Fan Yunfei（China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China）

摘 要：
面对海量异构、复杂动态的物联网应用场景，构建内生安全防护体系是满足其安全防护需求的必由之路。密码服务能力、终端系统级安全能力、终端安全适配能力、高效准确的威胁洞察与自动化编排处置能力、可扩展的安全服务能力是实现内生安全及其演进的基础能力。提出一种内生安全防护体系架构，该架构能够实现强身份认证、可信计算、内生系统级安全、海量设备适配和基于环境适应的安全能力适配。

关键词：
物联网安全；内生安全；操作系统安全；可信计算
doi：10.12045/j.issn.1007-3043.2025.10.015
文章编号：1007-3043（2025）10-0082-06
中图分类号：TN915.08
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
In the face of massive heterogeneous，complex and dynamic IoT applicationscenarios，building an endogenous security protection system is the only way to meet its security protection needs. Cryptographic service capabilities，terminal system-level security capabilities，terminal security adaptation capabilities，efficient and accurate threat insight，automatic orchestration and disposal capabilities，and scalable security service capabilities are the basic capabilities for realizing endogenous security and its evolution. An endogenous security protection architecture is proposed to achieve strong identity authentication，trusted computing，endogenous system-level security，massive device adaptation，and security capability adaptation based on environmental adaptation.

Keywords：
IoT security；Intrinsic security；Operating system security；Trusted computing

引用格式：谢国涛，范云飞. 基于可信身份构建可扩展内生安全防护系统[J]. 邮电设计技术，2025（10）：82-87.

0 前言

所谓内生安全，是指具有内生或内源性安全功效的构造、算法及体制机制[1]。按字面意思，内生是依靠自身构造因素而非外部因素得到的内源性效应[2]。内生安全就是利用系统的架构、算法、机制、场景等内在因素获得的安全功能或属性[2]。它是网络拥有自身免疫力的一种重要方式[3-7]。本文针对物联网安全场景，从密码服务能力、终端系统级安全能力、终端安全适配能力、高效准确的威胁洞察与自动化编排处置能力以及可扩展的安全服务能力等5个层面构建立体纵深的物联网内生安全防护体系。

收稿日期：2025-08-29

1 物联网内生安全分析

物联网市场规模快速增长，联网设备数量大幅增加，随之而来的安全事件愈加频繁。必须构建设备内生安全防护体系，从根本上提升设备安全能力，以应对不断演进的网络攻击技术和动态变化的安全防护需求[5,8]。这其中的关键能力在于密码服务能力、终端系统级安全能力、终端安全适配能力、高效准确的威胁洞察与自动化编排处置能力以及可扩展的安全服务能力。

a）密码服务能力。在万物互联时代，应采用更加轻量、高效、广泛适配的密码技术或服务，以实现身份认证、数据加密、网络安全通信等密码应用。但以PKI/CA为主的密码体制无法满足上述要求。因此，必须提供一种广泛适配的密码服务，以应对安全对象的异构性。本文采用一种兼容并蓄的方法，实现对多种密码体制的支持，同时结合安全对象的特征和密码服务需求，实现密码服务的广泛适配。

b）终端系统级安全能力。任何安全对象，包括物联网终端、服务器、虚拟机、容器等，其操作系统都会对资源进行调度调配，虽然部分操作系统已具备安全机制，但这些安全机制往往存在环境适应性差、无法动态调整等缺点。本文通过操作系统安全子系统增强操作系统安全能力，通过可信适配系统实现运行环境感知并做出适应性调整；利用安全服务模块，实现协同联动和动态调整。

c）终端安全适配能力。当前大多数安全防护产品是针对特定或某类安全对象、操作系统等进行设计的。本文中的可信适配系统，可实现运行环境隔离，在安全对象中为安全服务提供统一基础平台。

d）高效准确的威胁洞察与自动化编排处置能力。现代安全防护产品中存在部分态势感知、自动化编排与处置等能力，但大多存在以下问题：以失陷指标作为安全对象被攻击的标识，实时性差；无法充分结合安全服务平台能力和安全对象能力，自动化编排能力弱；只能针对网络的部分节点进行调控，处置的覆盖面和深度不够。本文基于ATT&CK模型，通过实时检测主动识别威胁，并充分利用网络效应，传播威胁特征。基于安全对象中的可信适配系统和安全服务平台的统一编排管理系统，将安全对象和平台各单元全部纳入编排系统，充分调动节点资源。同时基于可信适配系统，使处置能力能够触达安全对象操作系统层面。

e）可扩展的安全服务能力。在网络或服务碎片化的安全现状下，安全对象的粒度和形态差异大，且处于动态变化之中，同时安全需求也在不断变化。当前，安全防护产品既无法应对不断变化的安全需求，也无法全面覆盖海量异构的安全对象。本文通过可信适配系统（安全对象中的可扩展基础）和统一编排管理系统（安全服务平台中的可扩展基础），共同构建统一可扩展的基础框架。

面对海量异构的联网设备安全性保障问题，安全防护系统必须具备上述5个能力。其中，密码服务能力是身份认证、数据加密以及网络安全通信的基本保证；终端系统级安全能力是构建终端内生安全的基础，也是终端运行环境安全性的基本保障；终端安全适配能力是应对异构联网设备的关键，也是承载终端安全服务的基石；高效准确的威胁洞察与自动化编排处置能力是应对不断演进的网络攻击技术的关键；可扩展的安全服务能力是构建环境适应性安全防护的基石，可有效应对被防护系统和防护需求的差异性与动态性。这些能力单元并非各自为政，而是动态关联，共同构建终端内生安全防护系统。

但当前安全防护系统仅具备上述能力中的部分能力。终端系统级安全能力是建立安全对象内生安全能力的基石，如果无法顾及，内生安全只能是空中楼阁。终端安全适配能力是提供海量异构安全对象内生安全能力，保障安全对象中安全服务模块可动态扩展，将安全对象纳入统一编排调度的基础。若缺乏安全适配能力，安全服务的广泛适配性、动态扩展性、调度的统一性和全局性将没有存在的基础。

2 可扩展内生安全防护系统设计

2.1 总体设计

本文的主要思路为：通过密码服务平台，为安全对象、安全服务平台等身份实体构建安全凭证，形成身份识别、安全通信的基础能力。在安全对象中通过可信适配系统，搭建安全对象基础服务能力，感知并适配安全对象运行环境（包括硬件、操作系统等），为安全对象中的系列安全服务模块提供统一运行环境。安全对象中的系列安全服务模块运行于可信适配系统之上，它们会根据安全对象运行环境和安全需求，实现环境适应的灵活性与动态的功能扩展性；在安全服务平台中，通过统一编排管理系统，构建统一且可扩展的框架，基于该框架形成功能灵活扩展、性能动态伸缩的统一安全分析与处置能力。具体结构及交互示意如图1所示。

在图1中，“①、②”表示密码服务平台为安全对象和安全服务平台提供密码相关服务，包括注册认证和授权，密钥的生成、分发、更新、注销以及多种密码体制或跨域互信交换等；对密码服务平台而言，安全服务平台和安全对象一样，都被视为需要被识别的身份实体，且需要与外界进行安全通信。“③”表示安全对象与安全服务平台之间的交互，包括安全对象上报安

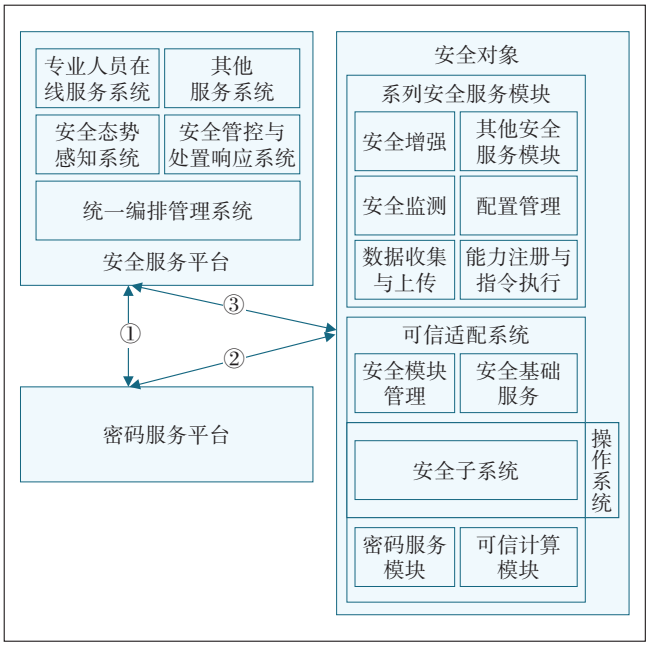

图1 系统整体结构和交互示意

全对象运行环境数据和安全态势数据，安全服务平台为安全对象提供安全相关服务（包括分析安全对象的安全需求，结合基于可信适配系统的数据收集与上传模块上报的运行环境数据，分发安全服务模块，根据局部或全局安全态势更新可信适配系统和安全服务模块中的策略、配置等元数据，根据局部或全局安全态势下发指令，指导可信适配系统和安全服务模块完成安全服务功能）。

2.2 密码服务平台

密码服务平台为安全对象、安全服务平台等身份实体构建安全凭证，形成身份识别、安全通信基础能力。密码服务平台至少应具备注册认证和授权，密钥生成、分发、更新、注销，以及多种密码体制或跨域互信交换等能力，安全对象和安全服务平台都应设置密码服务模块，以实现安全凭证管理和安全数据处理服务，包括凭证申请、存储、更新、注销，数据签名与验证，数据加密与解密，并且可以具备多种密码体制或跨域互信交换能力。密码服务及交互示意如图2所示。

本文强调通过密码服务模块与密码服务平台，建立起基础身份识别、数据加解密、安全通信能力，从而实现安全对象之间，安全对象与安全服务平台（及其构成单元）之间，以及安全服务平台构成单元之间（尤其在分布式部署的情况下）基于身份的访问控制、重要数据的加密存储与交换以及安全通信等功能。本文并非针对一种特定的安全对象或安全服务平台（及其构成单元），而是通过广泛适配的密码服务模块，应对安全对象或安全服务平台（及其构成单元）形态的差异性和需求的差异性。

2.3 安全对象

安全对象表示需要安全防护的对象，它可以为物理实体，如物联网设备、主机、服务器等，也可为虚拟实体，如虚拟机、容器等；如图1所示，本文关注的安全对象主要是可信适配系统和系列安全服务模块。

2.3.1 可信适配系统

可信适配系统搭建安全对象基础服务能力，感知并适配安全对象运行环境（包括硬件、操作系统等），为安全对象中的系列安全服务模块提供统一的运行环境。它包括3个部分。

a）密码服务模块。上文已经对该模块进行了说明。

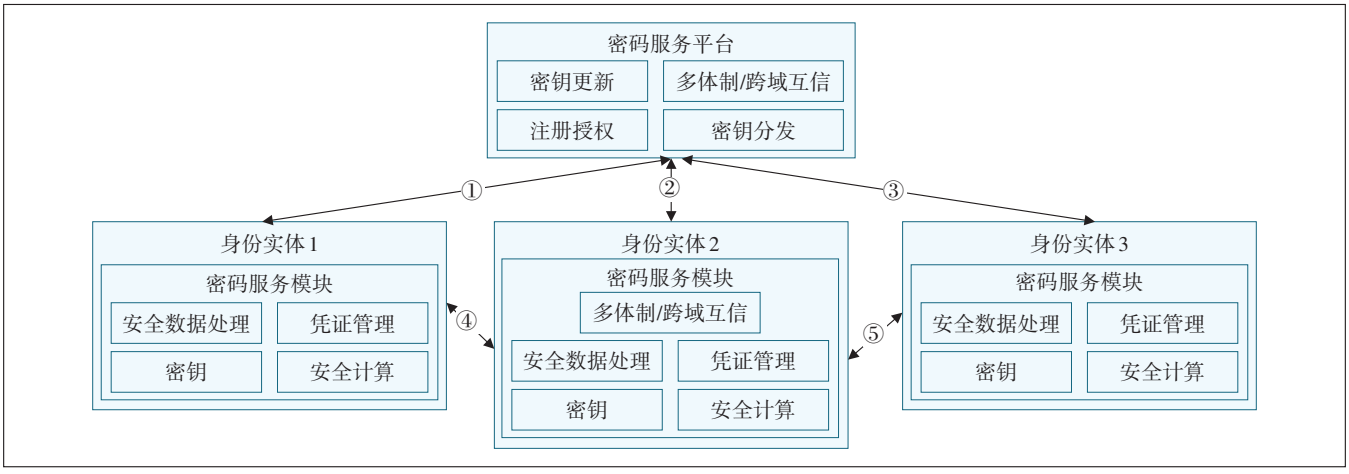

图2 密码服务结构与交互示意

b）安全子系统。安全子系统是作为操作系统一部分而存在的内核模块或服务，其主要职责分为3部分：其一，实现对密码服务模块的抽象，为操作系统及基于操作系统的应用提供密码服务；其二，对操作系统的安全性进行增强或更改。本文通过安全子系统替换原操作系统中存在的安全功能，或通过对原操作系统中存在的安全功能所暴露出的接口、配置项等内容进行适配、抽象，使其具备可动态调整的能力；其三，为可信适配系统中基于操作系统的其他上层模块和/或基于可信适配系统的系列安全服务模块提供统一的安全基础服务能力，包括密码服务和系统安全服务。

c）可信适配系统中的基于操作系统的应用层模块主要包括安全基础服务和安全模块管理。其中，安全基础服务是对操作系统安全能力和密码服务能力的适配与抽象，对安全子系统的安全服务能力的封装，该模块与安全子系统的区别至少有2点。

（a）安全子系统是操作系统的一部分，安全基础服务基于操作系统，属于应用层范畴。

（b）安全子系统能够清晰了解其运行环境（包括操作系统、运行硬件环境、密码服务等），能够根据运行环境、安全需求、安全态势等信息进行系统级安全调整。安全基础服务主要接收系列安全服务模块下发的调整指令，进行转换下发，其调整能力局限在应用层。

安全模块管理是为基于可信适配系统的系列安全服务模块提供统一扩展的基础能力，包括系列安全服务模块下载、安装、运行生命周期管理、资源隔离等。

可信适配系统的作用主要在于为终端建立基础安全能力、为安全模块提供基础安全环境；对于终端安全模块而言，可信适配系统屏蔽了终端差异性，但异构终端的适配压力并没有消失，而是由可信适配系统承担。

总之，可信适配系统通过密码服务模块和操作系统安全子系统实现对安全对象运行环境的适配，为安全对象提供统一安全基础服务，同时作为安全对象中的可扩展基础平台，对系列安全服务模块进行管理，并提供统一运行环境。

2.3.2 系列安全服务模块

系列安全服务模块运行于可信适配系统之上，根据安全对象运行环境和安全需求，实现环境适应的灵活性与动态的功能扩展性；安全对象形态各异，其所处环境和安全需求也处于不断变化之中；可信适配系统提供了一个适配和可扩展的基础平台，基于此平台的统一接口，系列安全服务模块无需获知其所处的安全对象形态和安全对象所处的环境；基于可信适配系统提供的统一接口与模块管理，安全服务模块可根据需要动态增加或减少，调整安全服务配置等。可信适配系统充分了解安全对象形态和安全对象所处环境，结合安全需求，调低优先级低的安全服务模块运行时间、调低优先级低的安全服务模块或安全消息的网络资源占用等。系列安全服务模块包括但不限于下列模块。

a）数据收集与上传模块。负责收集安全对象安全态势数据，并将其上传到安全服务平台。其数据收集内容和频率等配置信息，随安全对象形态、安全对象所处环境、安全态势局部或全局状态、安全需求等动态变化，接受安全服务平台调度指挥。

b）能力注册与指令执行模块。可信适配系统提供统一指令执行基础能力和指令执行安全性保障。能力注册与指令执行模块基于此基础安全能力，结合安全对象形态、安全对象所处环境、安全态势局部或全局状态、安全需求等因素，向安全服务平台注册并汇报安全对象当前的能力集合及执行限定条件。

c）安全监测模块对安全对象中的威胁、漏洞进行实时监测。它根据ATT&CK模型描述的攻击链执行过程，基于安全对象运行行为进行检测，如权限提升行为等。其监测内容，随安全对象形态、安全对象所处环境、安全态势的局部或全局状态以及安全需求等动态变化，接受安全服务平台调度指挥。

d）配置管理模块对安全对象中所有策略与配置进行管理，包括安全对象操作系统、可信适配系统、系列安全服务模块、安全对象应用程序等。

e）安全增强模块对安全对象中存在的威胁、漏洞等进行处理，或根据安全需求提高安全对象安全等级或配置信息。

f）其他安全服务模块。基于可信适配系统提供的统一适配及可扩展平台，安全对象中的安全服务模块，随安全对象形态、安全对象所处环境、安全态势的局部或全局状态、安全需求等动态变化，接受安全服务平台调度指挥。

2.4 安全服务平台

安全服务平台是为安全对象提供安全服务的统

一可扩展分布式系统，它包括统一编排管理系统、安全态势感知系统、安全管控与处置响应系统以及其他服务系统等。平台及其组成部分均具备密码服务模块，基于密码服务平台提供的密码服务，能够实现与安全对象、安全服务平台中的子系统之间的双向身份认证、安全通信、数据加解密等功能。下面对安全服务平台构成单元进行分述。

2.4.1 统一编排管理系统

统一编排管理系统是安全服务平台统一、可扩展的基础，包括需求分析、安全态势度量、统一编排等模块，如图3所示。

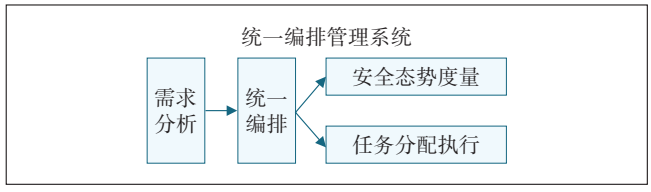

图3 统一编排管理系统主要组成模块

a）需求分析模块。对安全需求进行理解，基于安全目标多层级正交体系、优先级体系等设计方法，实现对安全需求的解读分解，形成可供统一编排管理系统衡量与执行的详细安全目标，输出给统一编排模块。

b）统一编排模块。基于需求分析模块输入的可衡量与执行的详细安全目标，调度安全态势度量模块，进行安全态势度量，获取目标与现状的差异；并根据当前获知的可编排能力单元的能力集合，制定执行计划，并输出给任务分配执行模块，由其进行具体调度执行。

c）安全态势度量模块。接受统一编排模块调度指挥，该模块结合安全服务平台中安全态势感知系统的态势感知结果数据，以统一编排模块可以理解的模式对态势进一步加工，将当前安全态势度量数据返回给统一编排模块。

d）任务分配执行模块。接受统一编排模块输入的编排执行计划，安排具体任务的执行。

统一编排管理系统是安全服务平台最重要、最基础的子系统；统一编排管理系统将安全服务平台和安全对象视为可被编排的能力单元，虽然这些能力单元在存在形态、能力内容、能力执行上下文等方面存在较大差异，但通过可编排能力模型的建模，形成可编排能力单元。统一编排模块根据当前安全目标和安全态势度量数据，综合权衡所有可编排能力单元，形成执行计划。可编排能力单元的覆盖范围包括安全对象和安全服务平台中除统一编排管理系统外的其他子系统。统一编排管理系统与可编排能力单元的关系示意如图4所示。

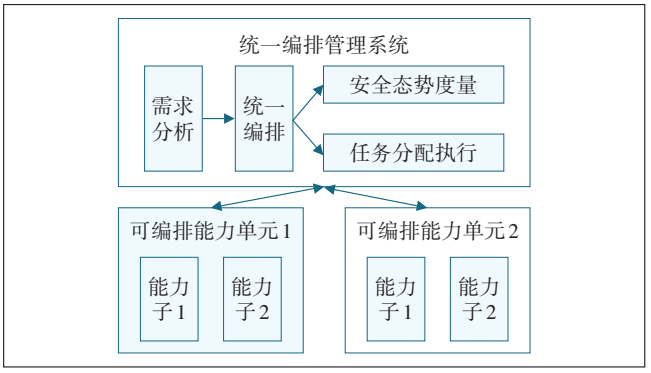

图4 统一编排管理系统与可编排能力单元的关系示意

其次，统一编排管理系统是安全服务协调指挥中心。安全服务平台的其他子系统和安全对象需要将安全能力主动或被动注册到统一编排管理系统中。因此，统一编排管理系统能够了解安全服务平台其他子系统和安全对象的安全能力。它基于对安全需求的理解、对安全态势的洞察，并结合安全能力，进行编排、调度、指挥等。

2.4.2 安全态势感知系统

安全态势感知系统结合第三方威胁情报、漏洞库、病毒库等信息，对安全服务平台收集的数据进行分析、处理，得出安全态势现状，并上报统一编排管理系统。

2.4.3 安全管控与处置响应系统

安全管控与处置响应系统维护安全对象的特征（包括基于可信适配系统和系列安全服务模块收集、上报的安全对象形态、网络等特征）、跟踪安全对象运行状况。当安全对象作为可编排能力单元被统一编排管理系统列入执行计划时，该系统督导、监测、反馈安全对象的执行情况，包括安全对象指令执行、安全服务模块增加或删除、安全配置更新等。

2.4.4 专业人员在线服务系统

专业人员在线服务系统将专业人员队伍所提供的专业安全服务，作为可统一编排的子系统，列入安全服务平台。

2.4.5 其他服务系统

其他服务系统为统一编排管理系统提供了统一

可扩展基础能力，能够基于安全服务平台部署情况、整体安全需求、应用场景、安全服务平台能力状况等特点进行扩展。

3 优势分析

本文所述方案对应用行业、场景、部署模式、安全对象存在形式等不做限定，基于当前行业、技术等划分，至少支持物联网、互联网等多个行业和场景，支持云部署、独立部署、混合云部署等多种部署模式，支持模组、物联网设备、手机、PC、服务器、虚拟机、容器等多种存在形式的安全对象，其优势如下。

a）通过密码服务平台和密码服务模块为安全对象和安全服务平台（及其组成单元）提供密码基础服务。通过多密码体制、跨域支持的机制，实现对跨密码体制或跨密码域的支持，真正实现密码服务的广泛适配和支持。

b）在操作系统内增加安全子系统，实现操作系统内原安全子系统的替换或增强。通过操作系统安全子系统加强操作系统安全能力，通过可信适配系统实现运行环境感知，并进行适应性调整；通过安全服务模块，实现协同联动和动态调整。同时，通过内核级强化的安全能力，从操作系统层面强化安全对象安全防御能力，同时为安全协同提供纵深环境（传统安全协调一般无法达到操作系统级别）。

c）通过可信适配系统实现安全对象的安全基础适配，并为安全对象中的系列安全服务模块提供可扩展的安全基础平台；基于此基础适配平台，实现安全对象中安全服务模块的动态扩展。

d）通过统一编排管理系统，为安全服务平台中的安全服务子系统提供可扩展的、统一的基础平台。可扩展主要体现在，通过可编排能力模型，实现对安全对象或安全服务平台其他安全子系统的模型化，并通过注册机制实现安全对象或安全服务平台其他安全子系统的动态扩展与伸缩；统一主要体现在：统一编排管理系统通过对安全需求的理解和目标化，结合安全态势度量，通过可编排能力模型，实现对安全对象或安全服务平台其他安全子系统的全局调度和协作。

e）通过安全对象中的安全可信适配系统和安全服务平台统一编排管理系统，分别构建安全对象中的可扩展基础平台，以及安全服务平台中的可扩展基础平台，形成整个系统的可扩展基础，将安全对象和平台各单元全部纳入编排系统，充分调动节点资源；同时基于可信适配系统，使处置能力触达安全对象操作系统层面。

f）建立一种安全的、统一适配的、可扩展的机制，实现对不同形态安全对象的防护。

4 结束语

内生安全是物联网安全行业应对安全挑战的重要思路，本文提出一种物联网内生安全防护体系架构设计方案，该方案借助强身份认证、可信计算、系统级安全等技术手段构建物联网内生安全基础。基于适配系统实现海量异构终端适配应用，并通过终端服务模块扩展和可扩展服务平台，实现安全需求动态适应。当前物联网设备差异大、应用场景复杂，将本文提出的基于5种基础能力构建的内生安全防护体系广泛应用于物联网设备与行业并不现实。但针对物联网重要行业（如车联网）、网络边缘关键设备（如车载网关等）进行重点突破，将是内生安全应用探索的首选。

参考文献：

[1] 蔡侗辰. 我国开辟网络空间内生安全新领域[N]. 光明日报，2020-10-30(008).
[2] 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.
[3] 中国信息通信研究院.2021年中国网络安产业白皮书[R/OL]. [2025-03-23]. http://www. whwx. gov. cn/wlaq/wadt/202201/t20220125_1914001.shtml.
[4] 张伟丽，贺磊. 关于新型内生安全信息基础设施的思考[J]. 无线电通信技术，2020,46(4)：399-404.
[5] 曾梦岐，石凯. 基于动态信任的内生安全架构[J]. 通信技术，2022,55(8)：1036-1043.
[6] 江伟玉，刘冰洋，王闯. 内生安全网络架构[J]. 电信科学，2019,35(9)：20-28.
[7] 宋克，刘勤让，魏帅，等. 基于拟态防御的以太网交换机内生安全体系结构[J]. 通信学报，2020,41(5)：18-26.
[8] 徐恪，付松涛，李琦，等. 互联网内生安全体系结构研究进展[J]. 计算机学报，2021,44(11)：2149-2172.

作者简介：
谢国涛，毕业于浙江大学，工程师，硕士，主要从事5G物联网密码与数据安全创新技术研究与应用工作；范云飞，毕业于西华师范大学，工程师，学士，主要从事5G物联网态势感知创新技术研究与应用工作。