

内禀安全：网络安全能力体系化构建方法

陈训逊¹, 李明哲^{1,2}, 吕宁², 黄亮¹

(1. 国家计算机网络应急技术处理协调中心, 北京 100094; 2. 长安通信科技有限责任公司, 北京 102209)

摘要: 目前主流的网络安全防护体系是外嵌的, 安全体系与业务体系分离, 安全产品相互孤立, 在防护能力上难以高效应对越来越复杂的网络安全挑战。网络安全从外向内进行强基, 势在必行。将网络安全的业务场景归纳为组织、厂商、监管和威胁四方视角, 各视角具有不同的业务目标。从四方视角的共性和个性出发, 系统性归纳网络安全生态的能力需求, 提出内禀安全方法论。内禀安全能力是指ICT组件原生支撑监测、防护和溯源等安全功能的能力。内禀安全能力对网络安全具有基础支撑作用, 本身不是最终的安全功能实现, 与现有的“内生安全”“内设安全”等方法论所针对的问题不同。内禀安全强调网络组件内在的安全赋能禀赋, 有两种方式可以发掘这种禀赋, 一是通过先天安全能力激活, 二是外嵌能力内化, 对外在逻辑上表现出自体免疫。此类组件的优势之一在于业务与安全的内聚, 能够透明化感知安全态势、定制化配置安全策略、贴身化执行安全保护; 优势之二在于将业务功能与安全功能进行合并封装, 简化整体工程架构, 降低网络管理复杂度。进一步提出了内禀安全支撑能力框架, 对符合内禀安全理念的安全能力进行归纳和枚举, 将安全支撑能力分为采集、认知、执行、协同和弹复5类, 并进一步介绍各类能力的子类型和基础ICT技术。基于该框架, 介绍了典型安全业务场景在内禀安全理念下的增强实现。

关键词: 内禀安全; 网络安全框架; 内生安全; 安全能力

中图分类号: TP309.1

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023010

Intrinsic assurance: a systematic approach towards extensible cybersecurity

CHEN Xunxun¹, LI Mingzhe^{1,2}, LYU Ning², HUANG Liang¹

1. National Computer Network Emergency Response Technical Team/Coordination Center of China, Beijing 100094, China

2. Chang'an Communication Technology Co., Ltd., Beijing 102209, China

Abstract: At present, the mainstream cyber security systems are laid out in an alienated style, where security functions are separated from business processes, and security products are isolated from each other. It is difficult to effectively cope with increasingly complicated cyber threats in this architecture. Therefore, it is imperative to move

收稿日期: 2022-04-23; 修回日期: 2022-12-04

通信作者: 吕宁, lvning@chanct.com

基金项目: 国家重点研发计划(2022YFB3102905)

Foundation Item: The National Key R&D Program of China (2022YFB3102905)

引用格式: 陈训逊, 李明哲, 吕宁, 等. 内禀安全: 网络安全能力体系化构建方法[J]. 网络与信息安全学报, 2023, 9(1): 92-102.

Citation Format: CHEN X X, LI M Z, LYU N, et al. Intrinsic assurance: a systematic approach towards extensible cybersecurity[J]. Chinese Journal of Network and Information Security, 2023, 9(1): 92-102.

security inward for more resilient and secure network infrastructures. Business scenarios of the cybersecurity sector can be categorized into four perspectives: organization, vendor, regulatory and threat, each of which has different business objectives. Starting from the commonness and individuality of the four perspectives, the needs of this sector was systematically summarized and then the goal of building an extensible cybersecurity capability ecosystem was recognized. As the key to this goal, the intrinsic assurance methodology was proposed. Intrinsic assurance capabilities referred to the abilities of ICT components to natively support security functions such as monitoring, protection and traceability. But intrinsic assurance is not the ultimate security implementation itself, which is a key difference from the existing “endogenous security” or “designed-in security” methodologies. Intrinsic assurance emphasizes the inherent security enabling endowment of network components, whether by activating an innate gift or by encapsulating a given one, both of which logically exhibit autoimmunity from an external viewpoint. One advantage of such a component is the cohesion of business and security, which leads to transparent security posture awareness, customized security policies, and close-fitting security protection. It also simplifies the overall engineering architecture and reduces management complexity through encapsulation of multiple functions into a singleton. Additionally, the Intrinsic Assurance Support Capability Framework was put forward, which summarized and enumerated the security capabilities that conformed to the intrinsic assurance concept. This framework classified the security capabilities into five categories, namely collection, cognition, execution, syndication and resilience respectively, together with their sub-types and underlying ICT technologies. Based on this framework, the enhanced implementations of typical security business scenarios was further introduced in light of intrinsic assurance.

Keywords: intrinsic assurance, cybersecurity framework, endogenous security, security capabilities

0 引言

当前，网络安全威胁持续升级。国家互联网应急中心发布的《2020 年我国互联网网络安全态势综述》^[1]指出：“安全漏洞、数据泄露、网络诈骗、勒索病毒等网络安全威胁日益凸显，有组织、有目的的网络攻击形势愈加明显，为网络安全防护工作带来更多挑战”。

目前主流的网络安全防护、监测、溯源体系都是“外嵌”的。网络安全防护体系多立足于边界防护，安全体系与业务体系分离，在防护能力上难以高效应对越来越复杂的网络安全挑战。简单地说，就是把安全系统作为独立的 IT 保安系统，使用一套软件或硬件系统把要保护的区域与不安全的网络环境隔离开，相当于在信息化系统的外面建造了一层一层的围墙。保安式安全思想一直发挥着积极的作用，直到目前仍然是安全防护的主体方法，但在数字化的生产环境中，在新的安全威胁形势下，特别是网络带宽、信息量爆炸式增长的条件下，保安式体系的建设越来越困难，成本越来越难以负担。网络安全监测的常用做法是通过在系统外部部署大量采集设施，集中

收集、集成存储，这导致日志传输开销大，存储成本高，采集视角片面，难以满足全方位感知需求。此外，溯源能力常常由外部驱动和执行，而业务系统本身并不具有标准化、体系化的溯源取证能力。这种工作架构制造了信息孤岛，导致协同迟缓和自动化受限，实时溯源困难。因此，网络安全能力必须实现“内化”，结合信息化系统自身进行强基固本。

本文提出内禀安全这一安全能力内化体系构建方法，自下而上地实现网络强基。内禀安全的基本思想是在网络组件内部发掘或引入对安全保障目标有支撑作用的机制，并通过体系化的协同实现各类网络的整体安全性。通过合理的方式对内禀安全进行实现，既能让安全机制贴合业务特性，又能避免业务功能被安全措施过度耦合。内禀安全的基本思想是针对当前网络的业务特性和保障需求，在各网络组件内部开发对具体安全保障目标有支撑作用的能力机制，并通过体系化协同方式进行整合，从而对整体网络安全性进行增强。软件定义网络(SDN, software defined network)等技术是内禀安全的重要实现基础。

1 相关研究

本节对研究人员针对网络安全能力内化展开的多方面探索予以介绍。零信任网络^[2]改善了由于传统边界模型过度信任造成的安全问题,核心思想是默认情况下不应该信任网络内部和外部的任何人、设备或系统,而是需要基于认证和授权重构访问控制的信任基础。可信计算^[3]是保障信息系统可预期性的技术体系,是指在计算的同时进行安全防护,使计算结果总是与预期值一样,使计算全程可测可控,不受干扰。这一安全防护方式的原理类似于人体的免疫系统,把系统中按照属主要求部署和运行以完成属主所需要功能的部分当作“自己”,可能干扰属主功能正常执行的部分定义为“非己”,在密码机制支持下实施身份识别、状态度量、保密存储,及时识别“自己”和“非己”部分,通过破坏和排斥“非己”部分确保信息系统的可信^[4]。美国有关专家提出动态目标防御(MTD, moving target defense)理念,通过降低信息系统的确定性、相似性和静态性,增加其随机性,降低其可预见性,从而构建持续变化、不相似、不确定的信息系统,使信息系统对外呈现不可预测的变化状态,攻击者难以有足够时间发现或利用信息系统的安全漏洞,更不容其持续探测、反复攻击,从而大大提高了攻击的难度和代价^[5]。郭江兴院士提出的拟态防御内生安全理论^[6],通过建造动态异构冗余(DHR, dynamic heterogeneous redundancy)系统来提升受保护目标的安全性。DHR即在异构冗余的基础上加入动态性和随机性,使系统呈现相当程度的不确定性,扰乱攻击者信息链,攻击难度非线性增加,攻击成功成为极小概率事件。对比MTD,拟态防御同时关注漏洞和后门,通过基于拟态计算的软硬件协同的技术加以实现,更具有一般性^[7]。齐向东^[8]提出的内生安全框架理论是一种工程体系化思路,强调安全能力组件化,并且让安全建设与信息化建设共同布局,从而实现安全能力与信息设施的架构级融合,更好地发挥安全潜能。云原生安全是指针对云原生信息系统的安全体系。针对云原生环境本身的特征建立安全机制,可以内置于云平台并利用云原生环境的特性。在

软件工程领域,还存在设计安全、预设安全等理念。设计安全是指软件系统在研发过程中即考虑安全需求,预防安全攻击,确保功能安全^[9]。这一理念应用非常广泛,微软公司提出的安全开发生命周期框架就是一种设计安全方法论^[10]。预设安全是指软件出厂时的默认设定即最安全配置^[11]。内设安全是2011年12月美国国家科学技术委员会提出的研发目标之一,是指“设计、开发和演化高保障软件密集系统并同时有效管控风险、开销、进度、质量和复杂性的能力”,通过安全开发工具、环境和最佳安全实践措施,“确保安全系统的开发,并能够同步产生该系统可抵御漏洞、缺陷和攻击的证据”。内设安全不仅涵盖了设计安全,还强调了对设计安全的赋能技术和证明技术。

为解释上述工作与本文提出的内禀安全理念的区别,需要先澄清安全能力的概念。采集、分析、溯源等安全能力在单独部署时并不能直接达成系统的安全性目标,而是起到间接支撑作用。因此,安全能力更应称作安全支撑能力。本文将网络攻防相关的安全能力划分为战略、运营、战术和技术4个层次,称之为四层能力;并将网络安全社区活动归纳为威胁、组织、监管和厂商4类,称之为四方视角。在战略层面,四方视角下的意图都是围绕保密性、完整性、可用性等安全保障目标展开,区别在于对这类目标的态度,如威胁视角下的动机无论是财富、意识形态、受迫还是自我满足感,均体现为对这些安全保障目标的侵害意图。在运营层面,组织机构需要采用一系列安全控制措施,以保障安全目标的实现;监管机构会检查企业单位的安全控制措施是否满足合规要求;而威胁行为体则会策划和发动一系列攻击战役,可能会触发安全告警并被认知为安全事件。在战术层面,组织机构需要部署安全支撑能力,这些能力是对具体技术的抽象,用于对安全控制措施加以支撑,如采集汇聚、协同联动、关联分析都属于防御战术。威胁行为体的战术则表现为检测逃避、指挥控制回连、横向移动等攻击手法的抽象,这些攻击战术在Mitre公司的对手战术、技术与通用知识库项目中有详细的枚举。技术层面包含战术层面的具体实现方法和实

现工具。例如，攻击者就地采用 PowerShell 程序执行恶意行为是检测逃避战术的一种具体实现技术，而 NetFlow 则是一种日志采集技术。安全厂商通过利用安全防护技术，为其客户组织提供安全支撑能力。四方视角下的安全能力层次如图 1 所示。内禀安全支撑能力是战术层能力，本身不等于安全保障目标的实现。

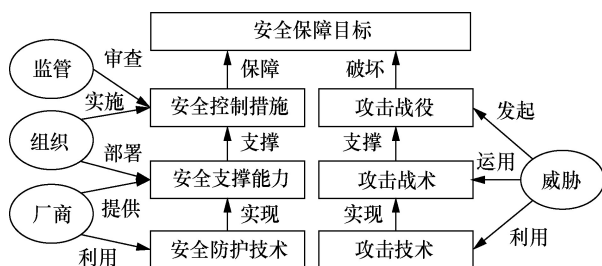


图1 四方视角下的安全能力层次

Figure 1 Level of security capability in the quadrilateral perspective

通过探究对现有安全内化工作的本质和共性，本文提出内禀安全理念，在战术理念层面对上述多种理论进行归纳和统一，以支持广泛的业务场景。内禀安全同上文中的内生安全框架均属于系统工程领域方法，但内生安全强调达到自身安全状态，而内禀安全则旨在供给安全支撑能力。在机械电子领域存在内禀安全这一研究课题^[12]，但相关研究关注的是物理安全，本文则关注网络空间中的信息安全。

安全框架是对安全技术及能力的归纳，防御类的安全框架包括 Mitre 公司的 D3FEND^[13]和 Engage^[14]、美国国家标准与技术研究所（NIST）提出的网络安全框架^[15]及 NIST SP 800-53 安全控制框架^[16]。本文在内禀安全理念基础上提出了内禀安全支撑能力框架，对基于内禀安全理念的安全能力进行枚举和归类。这些安全能力以具体的安全技术为底层支撑。云原生安全、MTD、拟态防御、可信计算等技术体系中的一些战术层理念均被纳入内禀安全支撑能力框架的能力组成项。

2 内禀安全理念

如上文所述，安全支撑能力意在保障某个受保护客体的安全目标，能力主体自身的安全保障则在主旨之外。内禀安全的特点是要求安全支撑能力的主、客体统一，即能力主体必须等同于或隶属于受保护的客体。由此可推知，主体对客体

输出的安全支撑能力必将服务于主体本身或主体所属的集体。需要强调的是，主体所输出的是安全支撑能力，并不直接提供客体所需的安全保障功能，而是仅提供底层支持。

内禀安全支撑能力是网络组件原生支撑网络安全监测、防护和溯源的能力。其中，原生具有两重含义，既可以指挖掘组件自身潜能，从而就地取材构造安全支撑能力；也可指将外部提供的安全功能加以封装内嵌，与原有环境融为一体，对外形成伪原生的安全能力。本文中的“组件”泛指网络空间中各类可感知的实体，既可以是软硬件模块、系统、服务、设备，也可以是人、机房、组织机构等管理域概念，还可以上卷到区域网络、行业等概念。各组件通过隶属关系形成上下层级。

内禀安全支撑能力的核心特征是对内可用和对外透明。对内可用强调业务适配性，即安全能力已针对当前环境加以本土化定制，确为网络所需，而非无关功能；对外透明是指安全保障机制隐藏在组件内部，无须用户刻意关注。有两种方式可以发掘出网络组件的内禀安全支撑能力。一是先天能力激活，以就地取材的方式实现自体免疫力或其他原生的安全支撑能力，如通过 SDN 方式在原有平台基础上扩展安全保障功能；二是外嵌能力内化，将业务组件与安全组件实施一体化封装，对外在逻辑上表现出伪原生的自体免疫，如将新增的安全设备隐藏在原有接口之后，从外部视角看网络拓扑未发生变动，在不干扰原有对外业务流程的前提下实现安全能力扩展。外嵌安全与内禀安全对比如图 2 所示。先天能力是指组件内部固有的能力，如厂商原有设计的能力或通用设备可广泛安装第三方软件的能力。防火墙的阻断控制能力、保险柜的物理防护能力和定制化态势感知系统的安全监测能力均属此类。先天能力激活过程体现为在业务需要时对产品固有能力进行启用，如开启路由器的 NetFlow 导出能力使其同时成为探针，主机内部安装可信计算功能等，有利于降低成本。本文把人也泛化成组件，员工的潜力经培养后发挥出来，也属于先天能力激活的范畴。外嵌能力内化的例子则更为常见，信息化系统开发商可以外采第三方的安全审计功

能,作为自身系统的构成组件销售出厂,对于客户而言,该系统具有内建的安全能力,简化了客户的认知复杂性。

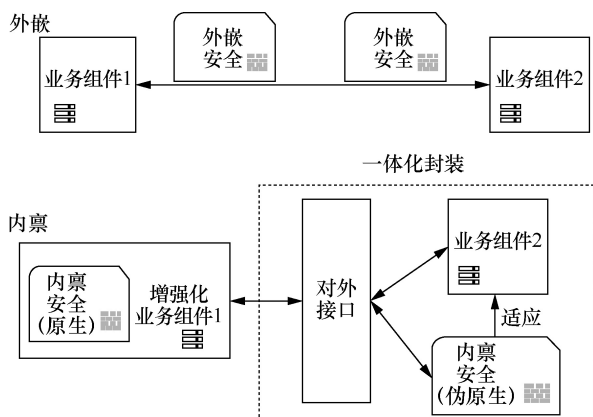


图2 外嵌安全与内禀安全对比

Figure 2 Comparison between embedded security and intrinsic assurance

形式化地,枚举网络空间中安全防护技术 $t_j, j=1,2,\dots,m$ 。以特定方式综合各类安全防护技术,可实现一种安全支撑能力,记作 $C_i = \Psi_i(t_1, t_2, \dots, t_m), i=1,2,\dots,n$ 。以特定方式综合各类安全支撑能力,可针对当前业务场景形成安全控制措施,记作 $S = \Phi(C_1, C_2, \dots, C_n)$ 。对于外嵌安全体系,安全支撑能力的建设通常追求通用性,独立于特定业务。内禀安全体系则主张安全支撑能力 C_i 隐藏在特定业务组件 B 中,使其形成增强业务组件 B' ;并逐渐发展出对该业务的适配性,自身演变为定制化的安全支撑能力 C_i^B ,记作 $B' = \Gamma(B, C_1^B, C_2^B, \dots, C_i^B, \dots, C_n^B), C_i^B = \Psi_i^B(t_1, t_2, \dots, t_m)$ 。

内禀安全理念的实现过程体现为用模块化的组件对各项具体能力加以承载,并实现组件间的协同联动,构成有机互动的内禀安全体系。这一体系可以类比人体淋巴系统。淋巴系统的各个器官既独立运作,又与其他肌体系统相适应。具有内禀安全能力的组件(下文简称内禀组件)不等于具有自我安全保障能力的组件,后者只是前者的一种特例,而安全能力所支撑的保障对象更多是针对上级组件,即包含了本组件的更宏观的组件。内禀组件的优势之一在于安全对业务的适应,有助于透明化感知安全态势、定制化配置安全策略、贴身化执行安全保护;优势之二在于资源复用和成本降低的潜力,通

过就地取材消除某些外部资源需求;优势之三在于通过将业务功能与安全功能进行合并封装,从上层视角看减少了组件数量,进而通过层层聚合封装简化了整体工程架构,降低了管理复杂度。随着这类组件在组织网络中的生长和链接,可逐渐形成互操作标准,实现统一的协同能力,可在不中断原有业务的前提下演化出协同联防、层层设防甚至全民皆“兵”的纵深防御体系,称作内禀安全体系。内禀安全体系虽然强调能力的下沉和分散,提倡内禀组件自行其是,但为了实现组件间协同并兼容遗留架构,集中化的安全管理也可加以应用,以作为对内禀安全体系的指挥控制中枢。

3 内禀安全支撑能力框架

基于上述内禀安全理念,本节对内禀安全支撑能力进行了枚举和组织,形成了内禀安全支撑能力框架。虽然其中某些能力在实践中已经有了实际使用,但本节从内禀安全视角对这些能力进行阐释,可识别出新的战术价值。此外,本节通过调研现有技术成果,识别出框架中各项战术能力的典型支撑技术。

内禀安全支撑能力框架将安全支撑能力分为采集、认知、执行、协同和弹复5类。如果将内禀安全支撑能力比作人体的自我保护能力,这5类能力则分别对应人的感官、大脑、四肢、神经和皮肉脏腑。5类能力分别由相应的具体能力项构成,内禀安全支撑能力框架如图3所示,接下来将对各能力项进行解释。

(1) 内禀采集

采集是网络信息数据的获取、处理和存储的过程,是建立环境认知的基础。依采集位置不同,可分为远程主动探测、网络被动收集、主机状态读取和数据存储调取。采集能力适配了异构的探测目标和多样化探测手段。本文在采集这一概念基础上提出内禀采集能力,特指那些结合业务组件特性的采集能力,主要关注网络位置邻近性或业务需求定制性,可通过业务组件内置的软件代理或硬件模块加以实现。本节提出多种符合内禀安全理念的采集场景,它们是对现有采集方式的优选而非变革,已经有广泛而成熟的实现。

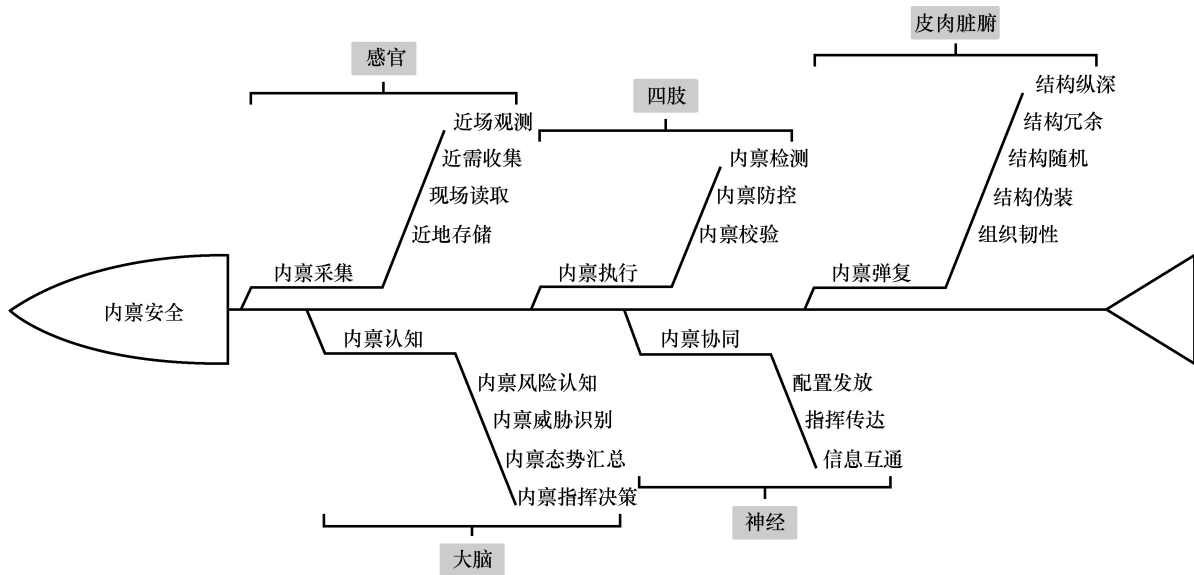


图3 内禀安全支撑能力框架
Figure 3 Intrinsic assurance support capability framework

1) 近场观测。信息获取组件接近观察目标,以获得探测性能、位置可达性、资料丰富性等方面的采集优势。① 近场主动探测:执行远程主动探测的探针接近探测目标进行部署,其基础技术为协议栈处理,如将针对企业网络资产可用性和脆弱性的探针从外网转移至内网部署从而深化可视性。② 近场被动收集:被动流量录制位置接近行为分析对象,以获得更为准确全面的行为观测资料,其基础技术包括主扫探针、流量镜像、流导出^[17]等。

2) 近需收集。信息获取组件接近于信息采集的需求来源和指挥中枢,如在安全运营中心(SOC, security operations center)中自建主动探测能力。在事件调查阶段,SOC可根据当前决策上下文随时发起远程主动探测,获取WHOIS、DNS、开源情报等信息;或自行发起对企业知识库系统的查询,以实现当前线索的按需富化。

3) 现场读取。信息获取组件与采集目标合一,通过发掘组件的自我状态感知机制实现现场读取能力,其执行频率可以是常态化的或按需的,执行时机可以是实时性的或回溯性的。具体技术实现机制包括程序流探测、主机参数收集、主机配置读取、主机资源测量、主机日志提取、主机流量录制和主机状态快照等。这种能力可用于网络空间资产管理、电子取证、应用安全测试、应

用性能测量等功能的实现。其基础技术包括捕获、流导出、快照、遥测、程序插桩等。

4) 近地存储。近地存储是指信息收集结果存放位置接近信息采集组件的存储策略。将信息收集结果的存储地点调度到信息获取组件内部,或该组件的邻居位置,可充分利用各节点富余存储能力,降低数据传输开销,增大资源使用效率。内容分发网络、P2P、边缘计算^[18]等现有技术架构都包含了近地存储这一设计思路。为支持其他组件在必要时获取相关数据,存储组件需针对自身所存储的数据开放查询获取接口。

(2) 内禀认知

认知能力在采集能力的基础上,承担各类态势分析和逻辑判断任务,如对潜在风险进行评估,对已知威胁进行匹配,对可疑行为进行识别,对整体态势进行梳理。认知能力的构建需要机器智能和人类智慧相辅相成,其基础技术包括人机交互、机器学习及知识库等。内禀认知能力是指与内部业务活动相邻近或与内禀采集能力相配套的认知能力,常表现为局部化的分析推理。其对立面则是集中化的“安全大脑”,这种认知架构拥有全局视野,但需要大量的数据传输,也难以建立通用而有效的分析逻辑,因此两种架构应结合运用。内禀认知包括如下几个子类。

1) 内禀风险认知。① 内禀风险评估:通过

内禀采集能力产生更完善的信息收集,对组织风险产生更全面完整的认知。② 内禀基线评价:利用业务透明性,研判当前风险强度与安全策略的一致性,发现过大的暴露面、过高的账户权限、过松的认证方式等,并构建出更为科学精准的安全控制策略。③ 内禀风险适应:通过对内禀采集能力提供的感知结果进行持续分析,快速感知环境变化,提示对当前安全控制策略进行变更。

2) 内禀威胁识别。① 由己辨彼:基于企业所属具体地域、行业的威胁形势及企业自身业务、资产特点,对外部社区所分享的宽泛威胁情报和广谱检测规则进行关联过滤,实现本地化的情报筛选聚焦和定制化的规则优先级排序,仅保留与当前业务相关的威胁检测逻辑,避免无关检测逻辑造成的算力消耗和告警泛洪,构建高效率、低噪声的威胁发现能力。② 因白鉴灰:通过对企业自身正常的网络流量、系统程序和业务行为进行归纳,总结出企业自身专有的白流量、白程序、白行为知识库,进而鉴于“自己”辨别“非己”,执行白名单威胁检测法,在避免误报误杀的前提下更全面地辨别出灰色流量、灰色软件和灰色操作。

3) 内禀态势汇总。组件建立本层级的态势感知能力,如下级部门自行建立局部态势理解,向上级报送汇总指标而非原始数据,有助于在上级部门更高效地建立全方位大规模态势感知体系^[19]。常规的态势感知系统利用庞大的传输带宽将多种数据源采集结果送达集中式的“安全大脑,进而以大数据技术为基础消耗巨大的计算资源才能完成有用的分析例程。内禀态势汇总系统则参照边缘计算架构,将一些具有局部语义的感知计算逻辑下移到分支机构,在当地即可实现相当程度的感知理解能力并建立相应的应用程序。这种架构只需要将聚合提炼后的局部态势指标数据传输到上级机构进行全局汇总,有效节省了传输带宽,降低了上级机构的算力负担和管理复杂度,也让下级机构获得了更高的灵活性和自主性,最终让整体工程建设具有更好的可行性和实用性。

4) 内禀指挥决策。综合内禀风险认知、内禀威胁识别和内禀态势汇总能力,对网络安全态势进行全面理解和预测,从而建立行动决策,并交付外部的执行组件进行实施。

(3) 内禀执行

执行能力建立在认知能力的基础上,在检测和处置阶段执行具体的安全策略,包括对入侵检测逻辑的实时执行,对认证授权请求的依规审批,对预定处置规则的现场实施。执行能力与采集能力的区别在于,后者是对环境的探查,前者是对环境的改变,安全性的改善最终由执行能力加以落实。内禀执行能力是指在接近业务目标处近场部署的安全策略执行能力,或与内禀认知能力相配套的安全策略执行能力。

1) 内禀检测。执行由内禀认知能力产生的更为细致的入侵检测策略,从而产生更高质量的告警信息,其基础技术包括推理引擎、SDN^[20]等。

2) 内禀防控。执行由内禀认知能力产生的更贴近业务目标的入侵防护策略,在各个控制关口做出适当的通关、阻断、重定向等动作。相关基础技术包括运行时应用自防^[21]、代码指针完整性校验^[22]、数据执行保护^[23]等。

3) 内禀校验。业务组件内部通过各类完整性校验机制,及时发现和阻止不可信实体,其基础技术包括密码学、可信计算等。

(4) 内禀协同

内禀协同能力体现为体系化的协作机制,在内禀指挥决策能力的基础上进行通信调度,使分散的内禀能力组件实现信息共享和行动协调。内禀协同能力的基础包括统一标准建设、建立通信通道等。

1) 配置发放:实现配置策略从内禀认知能力组件到内禀执行组件的下发输送。

2) 指挥传达:实现指令传送,对内禀组件间的协调联动进行编排。

3) 信息互通:通过常态化的数据输送或临时性的数据调取,让内禀采集能力可以为其他组件所用,如作为内禀认知组件的决策依据。

(5) 内禀弹复

弹复力有时也被称作弹性、韧性、复原力等,在系统工程领域是指系统面对干扰的鲁棒性和应对灾变的修复力。在网络安全领域中,网络弹复力是指网络系统能够有效吸收网络攻击,从而使运行不受影响,或者能够在受到影响后快速恢复。网络弹复力来自网络自身拓扑结构及运行机理的特性,是网络的内在禀赋,因此内禀弹复的概念

可等同于弹复力。

1) 结构纵深：利用组织网络自身的特点，建立适合当前网络拓扑的多层安全控制关口，从而形成纵深防御体系。

2) 结构冗余：利用结构冗余增强系统的可用性。可行基础技术包括冷备、热备、分布式技术等。例如，DHR 系统表现出了结构冗余能力。

3) 结构随机：利用持续的结构自变化引入随机性，对入侵者进行干扰。MTD 和 DHR 都表现出此类能力。基础技术包括地址空间布局随机化^[24]、指令集随机化^[25]等。

4) 结构伪装：网络中内建蜜罐、蜜饵、蜜场等防御欺骗技术，对攻击者的火力进行吸收。

5) 组织韧性：对网络灾害进行有效响应恢复的组织能力。① 资源韧性：在应急状态下能够分配充足的响应资源。② 技术韧性：具备一定的技术能力，能够基于镜像备份对受灾系统进行恢复。③ 职能韧性：在部分职能部门不可用的情况下，剩余部门仍可完成组织的运转。

4 典型业务场景

上述内禀安全支撑能力可以应用在多种实际业务场景中，对原有业务进行增强。本节对内禀安全理念的典型应用场景进行介绍。

(1) 网络测绘

网络测绘是网络安全的基石，通过对网络空间的大规模信息探测、信息融合和信息绘制，可实现对网络态势的有效感知^[26]。最常见的网络测绘是对 IPv4 地址空间的扫描，但除此之外，还存在其他的探测目标，如移动通信网、车联网、工业互联网等。甚至在单台主机之内，也存在大量的逻辑实体，值得进行监控和跟踪。进程、文件、应用、中间件乃至硬件，它们的属性信息和运行状态，对溯源取证活动而言是十分重要的数据。更加广义的网络测绘工作，还包括捕捉内容空间

中的文本、图片、音视频文件，采集社交账号、应用程序、终端、网元的行为。网络测绘的多样性，不仅在于它跨越了多种类型的网信空间，也体现在多个层次的网络断面。在不同断面上感知到的异构实体相互关联碰撞，将产生宝贵的信息情报。基于内禀安全理念，可以将这些视角、空间和层次统一起来，建立能够覆盖多重场景的测绘能力体系。从探针部署的位置看，大量的网络信息无法从外部探知，只能从网络内部汲取，甚至需要进入网元内部就地开采。从测绘目标来看，除了常见的服务测绘，还存在资产测绘、网络测绘、单机测绘和行为测绘等场景，这些场景对应的采集模块存在功能实现上的异构。内禀理念强调将内部采集能力加以发掘，将异构功能差异封装内化，以统一化架构，跨越多网域、多网段建立采集部署，融合多种采集方式，从而将外部测绘发展到内外协同测绘，将服务测绘过渡到全方位测绘。大规模的网络测绘需要数量众多的采集节点协作完成。通过内禀协同能力对各采集节点实施管理，下发配置和指令，互通信息有无。通过近场探测和现场读取能力可以使得测绘视野深入组织内网。通过结构冗余能力增强测绘系统的可用性。

2) 事件运营。事件运营一般是指企业为了防范网络攻击事件而采取一系列行动，包括防护、检测和响应，可以划分为事前、事中、事后三部分工作。在网络事件发生之前，建设具有内禀弹复能力的网络架构，基于近场观测能力摸清网络资产家底，通过内禀认知能力感知网络安全态势，制定防御策略，通过内禀协同能力实现策略全网下发生效。在网络运营过程中，对网络威胁执行持续的分析和阻断。当事件发生之后，内禀决策指挥能力通过指挥传达能力协调各组件的事件响应活动，并基于组织韧性完成网络恢复，基于内禀安全的事件运营如图 4 所示。

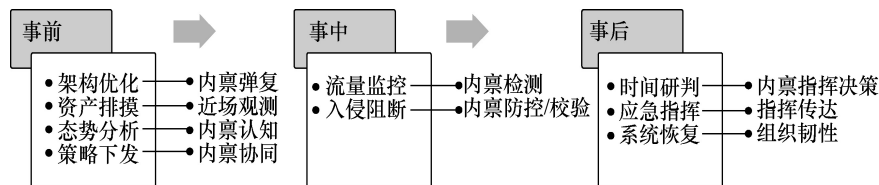


图 4 基于内禀安全的事件运营
Figure 4 Event operations based on intrinsic assurance

3) 攻击溯源。攻击溯源发生在事中及事后阶段,这时需要对攻击的源头进行追踪,对攻击者进行画像。在事件响应阶段,攻击溯源依赖于在各个网络位置搜集线索和情报,不断根据当前掌握的信息制定下一步信息搜集计划。现场读取能力和近需收集能力分别为主机取证和数据富化功能提供了一种标准化实现,经信息共享互通能力传送给指挥者后,内禀指挥决策能力可制定下一步方案。

4) 态势感知。态势是指态势感知活动所形成的信息态产物。本文将态势分类为网络资产情势、网络威胁形势和网络保障阵势三方面信息。目前国内许多企业和政府机构开始部署态势感知信息系统,期望以体系化、工程化的方式实现态势感知目标。美国国土安全部开发了持续监控与缓解(CDM, continuous diagnosis & mitigation)态势感知系统,协助各个联邦部局实施网络资产情势透视、漏洞评估与处置指导等^[19]。CDM 具备内禀态势汇总架构,各部局机构都能独立建立本机构的风险感知能力,同时将必要的态势信息上交国土安全部的安全运营中心,实现联邦层面的系统性风险研判。作者团队参与建设的“天势”大规模态势感知系统在工程实战中践行了内禀安全理念。该系统将自身的安全情势也列入感知目标,充分复用了自身的内禀采集、内禀认知和内禀执行能力,从而降低了对外部保障措施的依赖。

5) 情报交换。这里将组件概念应用于行业、地区等概念。美国在金融、电力等关键行业建立本行业的情报交换与分析中心(ISAC)组织,致力于行业内的威胁情报共享。由于同行业面临的高级持续性威胁有很强的相似性,ISAC 有效促进了威胁情报交换的积极性和效果,而其他一些未能考虑行业特点、业务特性的情报交换项目则很难达到预期效果,也没能调动企业的参与度。如果把某行业看成一个整体,那么在外部看来,ISAC 使该整体具有了内禀协同能力,这是内禀安全思想在真实社会生态中的体现。

6) 安全服务。该场景将组件概念应用于企业、团队和员工这种管理域概念。企业通过为员工提供安全意识培训,可以降低网络钓鱼风险。

企业通过调集内部资源和人力,建设安全运营中心,执行威胁狩猎等主动防御行动,可有效增强安全保障效果,是内禀采集、内禀认知、内禀执行能力在真实安全运营场景中的体现。以上措施属于先天能力激活类的内禀安全实现路径。此外,某些企业外购托管化安全检测响应服务或托管化安全服务,并将其与企业自身安全能力和业务流程充分磨合,使外包人员和外部系统成为企业安全体系的一部分,这属于外嵌能力内化式的内禀安全实现,在市场上受到了越来越多的认可。

上述前4个案例分别涉及一个技术架构,从中可看出,网络安全功能与其所保障的信息系统已经彼此相嵌、互为内禀,二者成为“一体之两翼、驱动之双轮”,安全保障效果有望得到增强。后两个案例涉及管理架构,将安全职能融入业务组织中,使安全团队的工作更有针对性和实际效果。

5 可行性讨论

本节进一步探讨内禀安全理念在落地实践时的可行性和关键实施要点。组织机构可以采用工程项目方式规模化建设内禀安全体系,也可以选择对单个在线业务组件开发内禀安全能力作为试点,并陆续推广到网络内其他组件,从而逐渐演化出内禀安全体系。出于对成本因素的现实考量,建设者应遵循按需布防原则。按需布防以摸清家底、厘清威胁为前提,从全网角度统筹防御资源,选择性开发激活安全内禀,对于重要资产和关键路径按需实施重点防御,同时可以实施隔离管控,分解安全管理的复杂性。

相比内生安全框架,内禀安全的适应场景更广。内生安全框架立足工程建设场景,强调安全建设和信息化要同步规划、同步建设、同步运行,以实现信息网络的安全性。安全产品一般并不直接嵌入信息化业务组件内部,而是让安全组件与业务组件协同布局,可以实现架构级融合。内禀安全则将安全建设与信息化建设进行更紧密的结合,包括安全与业务功能的组件内融合。内禀安全的外延更加广阔,在粒度上不仅涉及企业网络的工程架构,而是小到电子组件大到地区性网络等不同层次都有所适用;在时间维度上与工程建

设周期过程无关, 并不必然依赖采购、立项和研发活动, 不仅可以通过对现有网络设施进行技术改造加以实现, 还可以通过管理策略的调整加以实现。网络运营者在大多数场景下需要沿用已有的信息化网络, 而非频繁建立新的信息工程项目。有时出于暂时性的经费短缺不具备这种条件, 只能采取微改进升级; 有时不愿打断原有业务, 只能无扰地部署安全设施。在工控等领域, 业务系统的重大改造与业务连续性可能会存在矛盾, 使得来自工程项目的安全能力无法部署。因此, 内禀安全理念强调甲方利益, 注重兼容用户的遗留系统, 包容异构的供应链产品, 支持渐进型改进, 降低启动成本, 保持业务连续。

内禀安全理念所主张的安全对业务的适应性并不意味着双向耦合关系。对于在线业务的安全加固工作, 应提倡安全功能对业务功能的低干扰, 尽量避免让安全建设过度制约业务系统运行。在算力利用方面, 安全计算应利用业务组件的富余算力, 可降低硬件成本和功耗, 但应避免降低业务性能。通过内禀协同能力, 合理调度安全功能的执行位置, 有助于规避性能层面的冲突。软件工程理论中存在模块化设计、面向对象设计等思想, 有助于实现功能解耦。

内禀安全理念从最初概念层面出发, 逐步向实战层面发展, 但目前还存在一些有待深入研究和改进的课题。①“伪原生”内禀安全由于内涵广阔, 概念门槛低, 容易沦为标签, 类似于“零信任”被扩大化。未来将对此进行思考, 并建立内禀安全能力成熟度模型以量化特定落地实现的效果。②原生内禀安全能力的实现对环境有较高要求, 如SDN平台支持、算力富余等条件, 需要探索如何扩展场景适用性。③内禀协同等能力的实现面临较复杂的工程挑战, 还需要从架构、技术等角度进行深入研究, 发展出更详细的实践指导。④内禀安全能力框架尚不能做到互斥且完备, 无法涵盖所有相关场景, 这将在后续工作中加以丰富和完善。

6 结束语

网络安全行业生态中存在多种不同的视角和层次, 产生了业务场景的差异。本文阐明安全攻

防的四方视角及四层手段, 进而立足战术层面提出内禀安全理念。内禀安全理念在研究现有安全内化理论共性基础上形成, 对应更广阔的外延和更广泛的场景。本文总结归纳符合内禀安全理念的优秀实践, 形成了内禀安全支撑能力框架, 并列举了一些应用场景。目前, 笔者对内禀安全的理论设想已经有了初步的落地实践, 但仍处在初级阶段, 还需要结合更多实战案例进一步完善、细化和发展。

参考文献:

- [1] 2020年我国互联网网络安全态势综述[R]. 国家互联网应急中心, 2021.
2020 CNCERT cybersecurity analysis[R]. CNCERT, 2021.
- [2] BECK E A. How zero-trust network security can enable recovery from cyberattacks[J]. ISACA Journal, 2014, 6:14-18.
- [3] 张焕国, 罗捷, 金刚, 等. 可信计算研究进展[J]. 武汉大学学报: 理学版, 2006, 52(5): 513-518.
ZHANG H G, LUO J, JIN G, et al. Development of trusted computing research[J]. Journal of Wuhan University: Science Edition, 2006, 52(5):513-518.
- [4] 沈昌祥, 张焕国, 王怀民, 等. 可信计算的研究与发展[J]. 中国科学: 信息科学, 2010, 40(2): 139-166.
SHEN C X, ZHANG H G, WANG H M, et al. Research and development of trusted computing[J]. Chinese Science: Information Science, 2010, 40(2):139-166.
- [5] CHIANG C, GOTTLIEB Y M, SUGRIM S J, et al. ACyDS: An adaptive cyber deception system[C]//Military Communications Conference. IEEE, 2016: 800-805.
- [6] 郭江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4): 1-10.
WU J X. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4):1-10.
- [7] 郭江兴. 网络空间拟态安全防护[J]. 保密科学技术, 2014, (10): 4-9.
WU J X. Cyberspace mimic security defense[J]. Confidential Science and Technology, 2014, (10):4-9.
- [8] 齐向东. 面向新基建, 用内生安全框架支撑网络安全体系建设[J]. 中国科技产业, 2020(8):4.
QI X D. For new infrastructure construction, support the construction of network security system with endogenous security framework[J]. China Science and Technology Industry, 2020 (8): 4.
- [9] DOUGHERTY C, SAYRE K, SEACORD R C, et al. Secure design patterns[R]. Togashi, Kazuya: JPCERT/CC, 2009.
- [10] Lipner S. The trustworthy computing security development lifecycle[C]//20th Annual Computer Security Applications Conference. IEEE, 2004: 2-13.
- [11] SIMOIU C. Secure by default: a behavioral approach to cyber security[D]. Stanford University, 2020.
- [12] HAIDER A, MATTEO C. On intrinsic safety of soft robots[J]. Frontiers in Robotics and AI, 2017, 4.

- [13] KALOROU MAKIS P E, SMITH M J. Toward a knowledge graph of cybersecurity countermeasures[R]. 2021.
- [14] Mitre. ENGAGE[EB].
- [15] BARRETT M P. Framework for improving critical infrastructure cybersecurity[R]. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2018.
- [16] Joint Task Force Transformation Initiative Interagency Working Group. NIST special publication 800-53 revision 4-security and privacy controls for federal information systems and organizations[R]. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2013.
- [17] 李兴国, 费玲玲. 基于 Netflow 的流量分析技术研究[J]. 微计算机信息, 2008, 24(15): 198-200.
- LI X G, FEI L L. The research of netflow-based flow analyzing technology[J]. Microcomputer Information, 2008, 24(15): 198-200.
- [18] 施巍松, 张星洲, 王一帆, 等. 边缘计算: 现状与展望[J]. 计算机研究与发展, 2019, 56(1): 69-89.
- SHI W S, ZHANG X Z, WANG Y F, et al. Edge computing: state-of-the-art and future directions[J]. Journal of Computer Research and Development, 2019, 56(1): 69-89.
- [19] KAIBIAN J. Enhancing security in telemetry post-processing environments with continuous diagnostics and mitigation (CDM)[C]//France: EDP Sciences, 2014.
- [20] KIRKPATRICK K. Software-defined networking[J]. Communications of the ACM, 2013, 56(9): 16-19.
- [21] CISAR P, CISAR S M. The framework of runtime application self-protection technology[C]. 2016 IEEE 17th International Symposium on Computational Intelligence and Informatics (CINTI). IEEE, 2016: 81-86.
- [22] EVANS I, FINGERET S, GONZALEZ J, et al. Missing the point(er): on the effectiveness of code pointer integrity[C]//IEEE Symposium on Security and Privacy. IEEE, 2015.
- [23] GAO Y, ZHOU A, LIU L. Data-execution prevention technology in windows system[J]. Information Security & Communications Privacy, 2013.
- [24] GRAS B, RAZAVI K, BOSMAN E, et al. ASLR on the line: practical cache attacks on the MMU[C]. NDSS. 2017, 17: 26.
- [25] SINHA K, KEMERLIS V P, SETHUMADHAVAN S. Reviving instruction set randomization[C]. 2017 IEEE International Symposium on Hardware Oriented Security and Trust (HOST). IEEE, 2017: 21-28.
- [26] 赵帆, 罗向阳, 刘粉林. 网络空间测绘技术研究[J]. 网络与信息安全学报, 2016, 2(9):1-11.
- SHEN C X, ZHANG H G, WANG H M, et al. Research on cyberspace surveying and mapping technology[J]. Chinese Journal of Network and Information Security, 2016, 2(9): 1-11.

[作者简介]



陈训逊 (1972-), 男, 黑龙江哈尔滨人, 博士, 国家计算机网络应急技术处理协调中心正高级工程师, 主要研究方向为网络空间安全、计算机网络与信息安全。



李明哲 (1988-), 男, 山东临沂人, 博士, 国家计算机网络应急技术处理协调中心工程师, 主要研究方向为网络信息安全。



吕宁 (1988-), 女, 山东淄博人, 硕士, 长安通信科技有限责任公司工程师, 主要研究方向为网络安全。



黄亮 (1982-), 男, 湖南邵阳人, 博士, 国家计算机网络应急技术处理协调中心正高级工程师, 主要研究方向为网络信息安全。