中国科学: 信息科学 2022 年 第 52 卷 第 2 期: 189–204
SCIENTIA SINICA Informationis
《中国科学》杂志社
SCIENCE CHINA PRESS
6G 网络安全专题 · 论文

网络空间内生安全发展范式

邬江兴

国家数字交换系统工程技术研究中心, 郑州 450002

E-mail: ndscwjx@126.com

收稿日期: 2021–08–11; 修回日期: 2021–09–30; 接受日期: 2021–10–13; 网络出版日期: 2022–01–29

国家重点研发计划 (批准号: 2020YFB1806607) 和国家自然科学基金创新群体项目 (批准号: 61521003) 资助

摘要 本文试图从科学研究范式的高度诠释网络空间安全发展历程的思维视角和方法论, 指出相应发展范式变革的本质原因, 目的是围绕网络空间普遍存在的内生安全共性问题和基于这些共性问题引发的 “未知的未知” 安全威胁, 提出解决问题的新理论、新方法论以及相关的实践规范, 以期用内生安全发展新范式为网络空间安全领域以及新一代信息技术与相关产业贡献可复制的成功模板. 本文在简要介绍范式的概念和理论基础上, 以范式的世界观和方法论回顾了传统网络空间安全的主要发展历程以及难以克服的挑战, 归纳总结网络空间内生安全共性问题, 提出网络空间内生安全发展新范式, 介绍了新范式的理论基础、实践规范以及机制方法.

关键词 内生安全共性问题, 未知的未知安全威胁, 相对正确公理, 动态异构冗余构造, 内生安全发展范式

1 引言

美国著名科学哲学家托马斯 · 库恩 (Thomas Kuhn) [1] 提出了范式 (paradigm) 的概念和理论, 并在 1962 年首次出版的 “The Structure of Scientific Revolutions”, 即 “科学革命的结构” 一文中进行了系统阐述. 他从科学史的视角探讨常规科学和科学革命的本质, 第一次提出了范式理论以及不可通约性、学术共同体等概念, 提出了革命是世界观的转变之观点. 库恩 [1] 指出, 范式从本质上讲是一种理论体系、理论框架, 在该框架内的理论、法则、定律具有普适性, 是开展科学研究、建立科学体系、运用科学思想的坐标、参照系和基本方式. 他还指出, 在常规科学时期, 科学研究的发展是受范式限制的, 科学的活动就是在范式的指导下解难题或消除疑点的活动. 所以, 随着观察与实验的深入, 科学研究必须不断地揭示意料之外的新现象, 逐渐发现原有范式解决不了的难题. 这些难题就构成旧范式的反常. 随着反常的日益增多, 旧的科学范式越来越难以应付, 从而陷入危机之中. 在库恩看来, 这就意味着科学革命的时机到来了. 库恩在书中的重要贡献之一就在于把以往貌似堆积无序的科学进展历史 “建构” 出一个结构、一个关于 “范式” 的结构, 从而发现了 “科学革命的结构”.

引用格式: 邬江兴. 网络空间内生安全发展范式. 中国科学: 信息科学, 2022, 52: 189–204, doi: 10.1360/SSI-2021-0272
Wu J X. Development paradigms of cyberspace endogenous safety and security (in Chinese). Sci Sin Inform, 2022, 52: 189–204, doi: 10.1360/SSI-2021-0272

作者认为范式有 3 个基本特点: 一是, 范式在一定的范围内具有公认性; 二是, 范式是一种由基本定律、理论、应用及相关仪器装备等构成的整体; 三是, 范式能为科研与技术开发贡献可重现的成功模板.

按照作者的理解, 范式就是科学技术发展阶段的世界观和方法论, 是提出和解决问题的方法之方法. 世界观是指处在什么样的位置、用什么样的时间段的眼光去看待与分析事物, 它是人对事物的判断的反应, 是人们对世界的基本看法和观点. 方法论是一种以解决问题为目标的理论体系或系统, 通常涉及对问题阶段、任务、工具、方法技巧的论述. 方法论会对一系列具体的方法进行分析研究、系统总结并最终提出较为一般性的原则. 概括地说, 世界观主要说明世界 "是什么" 的问题, 方法论则主要说明 "怎么办" 的问题.

与库恩的看法有所不同, 作者认为范式间虽有思维方式、理论方法和技术路径方面的显著区别, 但也不应该是 "改朝换代" 式的取代关系, 相互间应该是共生并存的并具有一定的继承或迭代发展关系. 但有一点是毋容置疑的, 范式的变革往往在原有范式存在无法解决的难题时才会应运而生. 由此, 网络空间安全技术的演变历史就如同科学研究历史一样, 既存在演进发展过程又存在变革式发展阶段.

2007 年, 吉姆 · 格雷 (Jim Gray) [2] 在 "科学方法的革命" 演讲中, 提出将科学研究分为四类范式这种分类已成为一种共识. 其中, 科学研究第一范式的思维视角是观察与发现, 其方法论是试验或测量, 主要以记录和描述自然现象为特征, 代表性的事件有元素和基本粒子的发现、电磁现象、光电效应、宇宙观察等, 但这些研究显然受当时试验或实验条件限制影响, 很难完成对自然现象更精确的理解; 科学研究第二范式的思维视角是分析与归纳, 理论分析和演绎推论是其方法论, 代表性成果有牛顿的三大定律、达尔文的生物进化、麦克斯韦尔的电磁学、普朗克的量子理论、爱因斯坦的相对论等, 随着理论验证的难度和代价越来越高, 科学实验手段越发显得力不从心; 科学研究第三范式的思维视角是数值模拟/仿真, 方法论是在计算机上实现一个特定计算, 非常类似于一个物理实验, 换言之, 就是用计算机来做试验或实验, 但严重受限于算法创建和算力提升; 科学研究第四范式的思维视角是通过海量、异构、多元的数据资源发现新的科学规律, 揭示新的科学机理 (也称为数据驱动的科学), 其方法论是大数据分析, 主要特征是放弃对因果关系的渴求, 取而代之关注相关关系.

事实上, 不论何种发展范式其思维视角和方法论都是独特的, 其实践规范在一定范围乃至相当长时期内都具有普适意义, 可以相互借鉴, 并能够继承演进或迭代发展.

尽管网络安全界至今对以往乃至当前是否存在过 "发展范式" 的提法尚无公论, 但作者试图从貌似堆积无序、杂乱无章的网络安全发展历史中 "建构" 出一个结构, 一个关于 "范式" 的结构, 从而发现 "改变网络空间游戏规则的革命性结构". 本文在简要介绍范式的概念和理论基础上, 以范式的世界观和方法论回顾了传统网络空间安全的主要发展历程以及难以克服的挑战, 归纳总结网络空间内生安全共性问题, 并提出网络空间内生安全发展范式, 最后简要介绍新范式的发展动态.

2 传统网络空间安全世界观与方法论

不可否认, 网络空间安全技术客观上确实存在过 3 个可以用范式诠释的发展时期, 作者分别用网络空间安全发展第一范式、第二范式和第三范式来定义.

2.1 网络空间安全发展第一范式

网络空间安全发展第一范式, 作者称之为 "基于冗余配置与表决的功能安全发展范式". 其思维视角是如何解决网络空间终端、节点和网络系统软硬件物理或逻辑性失效问题; 其假设前提为, 无论是

物理还是逻辑失效都是随机性的, 不存在任何人为性质的蓄意干扰问题; 其理论基础是建立在统计学之上的可靠性与鲁棒控制理论 [3]; 方法论则是在关键路径、节点、网络架构等层面引入或导入重复处理的时间冗余、主备用或负载分担方式的空间冗余、基于表决/裁决的同构或异构冗余等; 其处理原则是基于冗余体制机制的可靠性设计方法, 重点是防范共模扰动带来的不利影响. 由于数字化、网络化、智能化技术的不断渗透, 单纯的随机性失效假设条件已无法成立, 不确定性或 “未知的未知” 的人为攻击成为功能安全发展范式的新挑战.

2.2 网络空间安全发展第二范式

网络空间安全发展第二范式, 作者称之为 “基于加密与认证授权的安全发展范式”. 其思维视角是用授权管理方式保护合法用户安全地使用软硬件设施或信息服务或数据资源 [4]; 其假设前提是加密和认证算法在数学上是可靠的, 算法所依托的宿主软硬件环境是可信任的; 其实践规范是基于密码编码和工程管理理论与方法对网络设施、信息服务、数据资源等实施授权使用; 其处理原则是相对被保护对象需要附加的加密认证代码或配套的专用设施; 其挑战性问题是加密/认证算法的宿主执行系统之漏洞后门等未知安全问题很难从根本上避免或杜绝.

2.3 网络空间安全发展第三范式

网络空间安全发展第三范式, 作者称之为 “基于检测与分析的网络安全发展范式”. 历史上曾出现过 3 个聚焦发展阶段.

阶段 1: 病毒木马查杀阶段. 主要目标: 寻找并查杀植入的恶意代码; 思维视角: 检测并清除网络空间终端、节点或系统软硬件中插入/植入的恶意代码; 假设前提: 蠕虫、病毒、木马等恶意代码存放及其运行特征是已知的; 方法论: 设法迭代检出恶意代码并删除、报警/隔离/人工介入、防止传播/扩散、建立病毒木马库、丰富恶意行为特征知识库等 [5]; 实施规范: 相对于目标软硬件代码或系统需要附加的检测或防护代码或设施.

阶段 2: 软硬件漏洞发现与修补阶段. 主要目标: 寻找恶意代码可植入的原因; 思维视角: 用补丁方式修补目标系统软硬件代码设计中存在的安全缺陷, 或引入不同层次的动态技术, 避免病毒木马的注入或降低漏洞的可利用性; 假设前提: 软硬件代码设计缺陷已知或清楚攻击面及攻击资源的可利用机制; 方法论: 建立并完善漏洞库、制订代码安全设计规范、开发设计脆弱性分析技术主动挖掘漏洞、降低攻击表面的可达性或攻击资源的可利用性等 [6]; 实施规范: 相对于目标软硬件代码或系统需要附加的检测或防护代码或设施.

阶段 3: 攻击行为特征感知与阻断阶段. 主要目标: 发现不规范的蓄意行为和特征; 思维视角: 通过攻击行为的特征感知, 阻断攻击链或降低攻击链的可靠性; 假设前提: 清楚攻击行为的所有特征, 了解目标对象所有合规特征, 即需要 “知己知彼”; 方法论: 运用内置探针、蜜罐、沙箱、运行日志等实时或非实时方法尽可能地收集疑似问题场景数据, 借助黑/白名单、大数据和人工智能等技术发现或抑制可能的攻击行为 [7,8]; 实施规范: 相对于目标软硬件代码或系统需要附加检测或防护代码或设施. 第三范式各阶段都存在的难题是, 软硬件系统内生且又无法彻查与杜绝的漏洞问题.

上述 3 种网络安全发展范式的共性难题是, 在缺乏先验知识的条件下, 如何应对网络空间基于未知漏洞后门、病毒木马等未知的内生安全威胁.

3 网络空间内生安全共性问题分析与归纳

首先, 要搞清楚什么是内生安全问题? 内生 (endogenous) 的词面意义是指, 一个系统或一个模型内存在互为依存或纠缠关系的因素 (或变量), 这种因素或者变量称为内生的或内源性的. 与内嵌 (embedded) 或内置 (built-in) 因素不同, 凡是不可分离的因素才能称为内生的. 内生安全问题本质是事物的矛盾性表现, 正如德国哲学家黑格尔所述: "一切事物都是自在的矛盾, 矛盾是一切运动和生命力的根源", 由此不难理解, 事物的两面或多面性决定内生安全问题存在的泛在性和必然性. 从一般意义上说, 任何自然的功能或人造的功能, 都存在伴生或衍生的显式的副作用或隐式的暗功能. 副作用也许能够区分其良性或非良性的属性, 但暗功能的性状及可能的影响则完全是未知的. 内生安全问题就是元功能或本征功能的内在性矛盾, 既有个性化特点也有共性化表现, 因此只可能设法去规避或抑制而不可能彻底消除. 此外, 按照矛盾论的表述, 内因只有通过外因起作用, 因而内生安全问题只有在外部因素影响或扰动下才有可能转变为内生安全威胁 [9]. 需要强调指出的是, 个性化问题不可能有统一解, 只有共性化问题才可能存在普适性解. 以下所列均为网络空间内生安全问题.

(1) 大数据内生安全问题: 分析结论的不可解释性.

(2) 人工智能内生安全问题: 分析结果的不可解释性、不可判识性、不可推理性.

(3) 区块链内生安全问题: 市场占有率 >51% 软硬件节点中存在共模性质的漏洞后门等.

(4) 5G 网络内生安全问题: 与 IT 及互联网深度融合引入传统 IT 基础设施的漏洞后门、病毒木马等.

(5) 可信计算内生安全问题: 可信根的可信性存在 "灵魂拷问" 问题.

(6) 动态/主动防御内生安全问题: 无法防护基于宿主环境内调度环节漏洞后门攻击.

(7) 传统可靠性理论的内生安全问题: 功能安全与网络安全已成为交织问题.

其次, 要弄清什么是内生安全共性问题? 按照共性 (generality/ubiquity) 的词面解释: 共性, 就是某个领域内普遍或泛在化存在的某种性质. 所谓内生安全共性问题应该是内在的而不是外在的、普遍的而不是特殊的、群体的而不是个体的. 那么, 网络空间是否存在内生安全共性问题呢? 对此业界有不同认识. 有观点认为, 网络空间因为没有泛在化的安全问题, 网络安全学科至今尚无统一的理论体系; 还有观点称, 网络安全是伴生性技术, 网络安全问题是随着信息和网络技术与各行业的结合而产生、衍化出来的; 另有观点认为, 网络安全具有明显的差异性和个性化特征, 根据需求不同、应用场景不同、服务面向不同, 有不同的描述和表达; 更为直白的观点是, 网络空间尽管存在内生安全问题, 但似乎不存在内生安全共性问题. 但是作者则认为, "网络空间不仅存在内生安全问题而且存在严重的内生安全共性问题!". 以下 6 个方面的认知足以支撑本论断的成立.

(1) 人类技术发展和认知水平的阶段性特征、复杂性与完备性矛盾导致软硬件代码设计缺陷 (脆弱性) 或漏洞问题不可能彻底避免.

(2) 全球化、多极化时代, 任何国家或企业都不可能建立起完全自给自足的全产业链, 只要技术链、供应链、制造链等存在不可控环节就不可能彻底杜绝后门问题.

(3) 现阶段人类科技能力无论是在理论还是技术方面尚不具备彻查目标系统 (尤其是复杂系统) 软硬件代码中的漏洞后门等问题. 就普遍性而言, 若要穷尽或彻查目标系统软硬件代码问题, 在可以预见的将来, 仍然是难以克服的科学与技术挑战.

(4) 随着信息技术、网络技术与智能技术以及人为攻击因素不断渗透传统的功能安全领域, 网络安全问题使得针对单纯随机性事件的可靠性假设前提已经难以成立, 功能安全问题不可避免地演变为 Safety 和 Security 复合问题.

(5) 上述 4 个问题的存在使得信息领域或相关行业产品安全质量尚无有效的控制办法, 造成网络空间全产业链从源头起就存在难以消除的安全问题, 也为信息技术和相关产品无需提供安全性质量承诺或法律责任给出了人类社会自有商品交换以来十分荒谬的理由.

(6) 图灵机 (Turing) 只是回答了什么是可计算问题, 冯 · 诺依曼 (John von Neumann) 计算结构也只是解决了怎么计算的问题, 现阶段计算机科学与工程的进步尚不能区分什么是恶意或善意的计算问题.

由此可见, 网络空间因为广泛存在内生的且是共性的安全问题, 攻击者只要能找到合适的攻击面及可资利用的软硬件资源, 就可以建立起有效的攻击链, 外因就能通过内因构成广义不确定安全威胁 [9].

遗憾的是, 现有的网络安全技术无论是对防御目标还是对所谓 “安全守护神” 自身而言, 都无法回避或消除软硬件内生安全共性问题的影响, 即使加密认证等算法的安全性在数学意义上可能已经足够强大, 但其物理或逻辑实现载体的安全性仍然难以给出理论与工程上令人信服的证明. 大量事例表明, 基于加密认证和传统的主被动防御技术体系常常被内生安全共性问题 “旁路或短路”, 这使得现有的安全技术呈现出难以解决的逻辑悖论也就不足为奇了.

内生安全共性问题必然会引发网络安全科学与技术方面一系列的难题. 例如, 如何才能证明当今 “叠罗汉” 式的附加安全防护是安全可信的? 如何才能证明叠上去的每个罗汉其自身是安全可信的? 由于内生安全共性问题的存在, 所有安全技术怎样才能自证清白? 在万物智能互联时代能在工程技术层面彻底避免触发或隔离内生安全共性问题吗? 信息产业及相关领域必将长期面对没有任何商家敢保证 “自主可控产品” 不存在安全漏洞、没有任何安全检测机构敢为送检设备/装置/产品作无漏洞后门等安全担保的严峻挑战. 作者以为, 若要防御未知的未知威胁 [10] 必须转换思维视角, 提出新的方法论!

4 网络空间内生安全发展范式

4.1 网络空间内生安全发展范式期望目标

网络空间内生安全发展范式的期望目标是: 提出新的普适性理论, 建立新的实践规范, 开辟新的技术路径, 研制新型技术装备. 具体表现在 3 个方面.

一是解决网络空间普遍存在的内生安全共性问题, 破解第一、第二、第三范式难解之困.

二是创新基于 “亡羊补牢” 和加密认证的网络安全基础理论和实践规范, 转变单纯地依靠漏洞后门和攻击特征精确发现以及缩小攻击表面 (attack surface) 的技术发展路线 [11].

三是提出一种不依赖 (但不排斥) 漏洞后门发现和攻击特征分析等先验知识的内生安全理论与体系, 建立一套有效解决网络空间内生安全共性问题的实践规范, 以创新的广义鲁棒控制构造破解目前功能安全与网络安全性不能量化设计、无法验证度量的工程技术难题, 从根本上实现当前网络安全领域思维视角与方法论的转变, 破解如何有效防范未知的未知威胁、如何基于相对性构造原理抑制内生安全共性问题影响等亟待解决的重大科学问题.

4.2 破解内生安全共性问题的新视角与方法论

破解网络空间内生安全共性问题的新视角与方法论总结为以下 4 个方面.

(1) 确定思维新视角. 如何能在不依赖 (但不排斥) 攻击者先验知识或精确检测与分析结果的情况下, 有效阻断基于内生安全共性问题的 “未知的未知” 安全威胁.

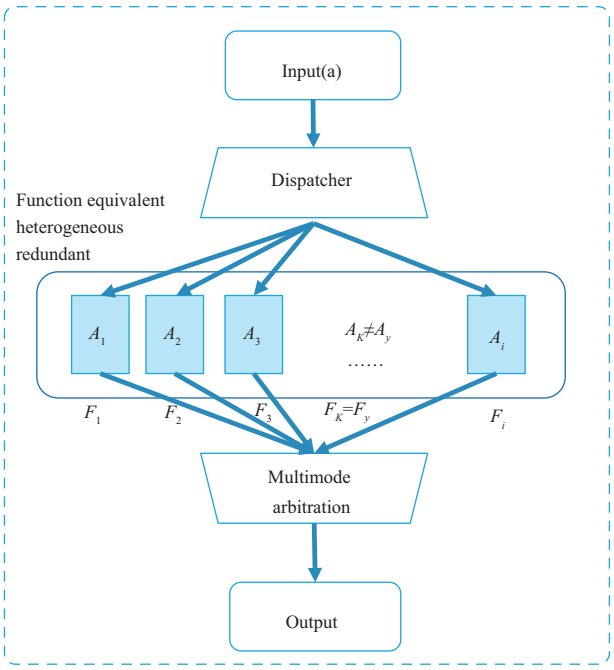

图 1　相对正确公理的逻辑表达

Figure 1　The logical expression of the relatively-correct axiom

(2) 创立新方法论. 用功能等价异构多元相对性判识构造, 将个体层面的 “未知的未知” 安全威胁变换为群体层面差模形态的 “已知的未知” 安全威胁, “已知的未知威胁” 是指能预测到可能会发生, 因而可以在一定程度上进行防范的 “未知威胁”.

(3) 实施规范与处理准则. 将 “已知的未知” 威胁变换为 “概率可控” 的可靠性事件, 将共模逃逸概率控制在设定的阈值内, 一体化地解决功能安全和网络安全问题.

(4) 限制试错或盲攻击. 从机理上消除试错或盲攻击所必须的背景不变前提条件.

4.3　猜想与问题

2013 年, 作者基于 “相对正确公理”(也称共识机制) 的再发现, 提出用相对性构造原理将 “未知的未知” 安全问题转变为 “已知的未知” 安全问题的猜想, 但碰到两个必须解决的科学难题.

一是, 相对性构造的有效性前提是, 构造内的物理或逻辑失效因素属于可用概率表达的随机性事件, 而基于内生安全共性问题的人为攻击则属于未知的未知问题, 无法用概率描述, 因而是两个数学性质完全不同的问题, 如何才能归一化处理;

二是, 由于相对性构造完全没有考虑基于目标对象内生安全共性缺陷的人为攻击问题, 因而在网络攻击可达且目标对象攻击资源可利用条件下, 其可靠性模型或相对性构造并不具备品质鲁棒性和稳定鲁棒性.

4.4　理论基石: 相对正确公理

众所周知, 在人类社会活动中常常依赖这样一种公知, 即 “人人都存在这样或那样的缺点, 但极少出现独立完成相同任务时, 多数人在同一个地点、同一时间, 犯完全一样错误的情形”. 作者将其称为 “相对正确公理”. 其相应的逻辑构造如图 1 所示.

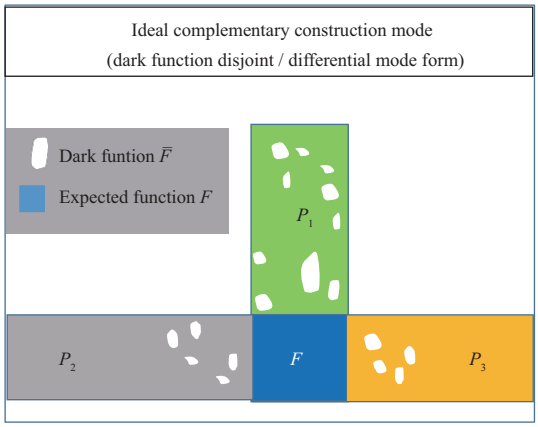

图 2　理想互补构造方式

Figure 2　An ideal complementary structure

图 1 中 $A_1 \sim A_i$ 表示可以独立完成任务 a 的人群, 它们之间在逻辑上可以看作是功能等价的异构冗余关系. 当任务 a 被同时分发给 $A_1 \sim A_i$ 时将会产生输出结果 $F_1 \sim F_i$, 一个大数表决器选择具有共识性质的任意 F_k 的输出. 其实, 这种共识构造及机制也是人类社会民主制度的基石. 不过, 该公理成立的首要前提是必须排除任何联合作弊的情形.

从哲学层面看, 不确定或未知等问题往往属于相对性的范畴, 通常源于感知空间或认知手段的局限性, 一般得到的是 “盲人摸象” 般的似是而非的结果.

4.5　相对正确公理的再发现

对该公理仔细研究之后作者有以下再发现.

一是个体层面的不确定性 (未知的未知) 问题可以由共识构造转化为群体层面差模或共模表现形态的 “已知的未知” 概率问题. 换言之, 我们能以 “只知其然, 不知其所以然” 的方式感知个体层面的未知事件 (尽管不清楚具体原因、基本性状和行为特征).

二是调整人数、类型、任务复杂度、完成时间、表决策略等可以控制共识层面差模概率的大小, 即控制未知问题的可能影响范围.

三是共识结果在小概率上存在错误的可能, 也就是说, 存在人们常说的 “真理往往掌握在少数人手里” 的情景, 因此尚不能简单地依赖多数表决结果下定论.

四是相对正确公理在人为试错或盲攻击条件下不具有稳定鲁棒性和品质鲁棒性, 也就是说如果存在私下串联或作弊的情形, 共识结果不存在可靠的置信度.

4.6　基于再发现的推理构造

根据上述发现我们不难推出一个理想的互补构造来实现未知的未知感知, 如图 2 所示.

这里, 只有 $P_1 \sim P_i$ 的功能 F 属于期望的功能交集, 其他不存在交集的副作用或暗功能称为差模暗功能. 实际上, 在工程技术层面几乎不可能实现这种理想的相对性互补构造. 为此作进一步的推理.

推理 1　$\forall i,\ i = 1, 2, \ldots, n$, $P_i = F \cup \bar{F}_i$, 其中 P_i 是目标功能 F 的第 i 个构造的功能集, $\bar{F}_i$ 是第 i 个构造的暗功能, 存在

$$P_1 \cap P_2 \cap \cdots \cap P_n \subseteq \forall_{i,j} P_i \cap P_j.$$

若存在 $\bar{F}_i \cap \bar{F}_j = \Phi$, 则 $P_1 \cap P_2 \cap \cdots \cap P_n = F$.

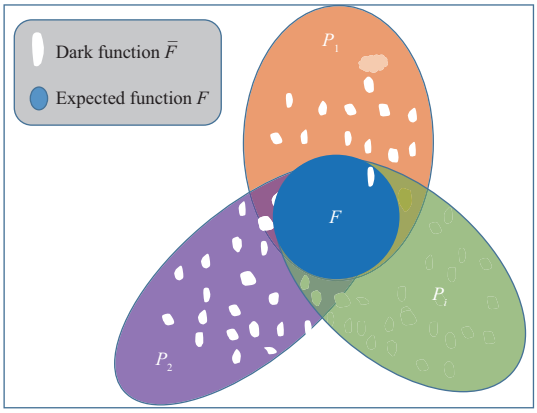

图 3　符合实践的可应用构造

Figure 3　The applicable structure with more practical specifications

实际中, 很难设计出满足 $\bar{F}_i \cap \bar{F}_J = \Phi$ 的功能集 P_i, P_j. 此时, 只要满足

$$(P_1 \cap P_2 \cap \cdots \cap P_n) \subset (P_1 \cap P_2 \cap \cdots \cap P_{n-1}) \subset \cdots \subset (P_1 \cap P_2 \cap P_3) \subset \left(P_1 \cap P_2\right), \tag{1}$$

则 $\lim_{n\to\infty} P_1 \cap P_2 \cap \ldots \cap P_n = F$.

证明　由于 $P_1 \cap P_2 \cap \cdots \cap P_n = F \cup (\bar{F}_1 \cap \bar{F}_2 \cap \cdots \cap \bar{F}_n)$, 则式 (1) 设计条件可表示为

$$(\bar{F}_1 \cap \bar{F}_2 \cdots \cap \bar{F}_n) \subset (\bar{F}_1 \cap \bar{F}_2 \cap \cdots \cap \bar{F}_{n-1}) \subset \cdots \subset (\bar{F}_1 \cap \bar{F}_2 \cap \bar{F}_3) \subset (\bar{F}_1 \cap \bar{F}_2). \tag{2}$$

假设暗功能集是有限集合 $\bar{F}$, 其元素个数为 M, 可知, $\bar{F}_1 \cap \bar{F}_2$ 的元素个数最大为 M. 根据式 (2), n 最大为 $M+1$ 时, $\bar{F}_1 \cap \bar{F}_2 \cap \cdots \cap \bar{F}_n$ 的元素个数将为 0. 即 $n \geqslant M+1$ 时, $P_1 \cap P_2 \cap \cdots \cap P_n = F \cup (\bar{F}_1 \cap \bar{F}_2 \cap \cdots \cap \bar{F}_n) = F$.

由上述内容可知以下两点.

(1) 要获得 F, 定理中给出的其中一个条件就是 $\bar{F}_i \cap \bar{F}_j = \Phi$, 即要能够设计出满足目标功能 F 且暗功能无交集的两个功能集 (或者称为执行体) P_i, P_j, 这样, 依靠 2:0 的多数裁决机制就能保证系统 Safety 和 Security 安全, 而现实中要满足这个条件, 是几乎不可能的.

(2) 此外, 由推理及式 (1) 可知, 工程设计中, 我们可以通过增加构造体的数量 i, 并增加新构造体与集合中已有构造体之间的异构度减少暗功能的交集, 从而可以在实际中逼近甚至获得 F.

我们可以得到一种更符合实践规范的应用构造, 如图 3 所示.

在这个构造中, 凡是不存在交集的暗功能称为差模暗功能, 在机理上就无法被利用; 存在 $P_i \cap P_j$ 暗功能交集的称为共模暗功能, 在外界广义扰动因素影响下有可能发生共模逃逸. 于是, 即使在暗功能及其特征完全未知情况下, 借助基于裁决的反馈控制机制, 策略性地改变异构执行体间的功能交集, 在本征或元功能不变 (即使命确保) 的情况下, 对攻击者而言, 当前构造环境具有视在的不确定性, 试图通过异构不稳定攻击表面形成协同一致的攻击逃逸存在指数级难度的挑战. 我们将这种构造命名为 “动态异构冗余” 构造 (dynamic heterogeneity redundancy, DHR) [12], 如图 4 所示.

4.7　DHR 构造主要特性

DHR, 这种基于迭代裁决的多维动态重构反馈运行环境, 使得任何独立的人为试错或盲攻击事件都会被异构容错机制所屏蔽, 反馈控制环路会引发异构冗余环境内呈现出功能等价条件下的 “测不准

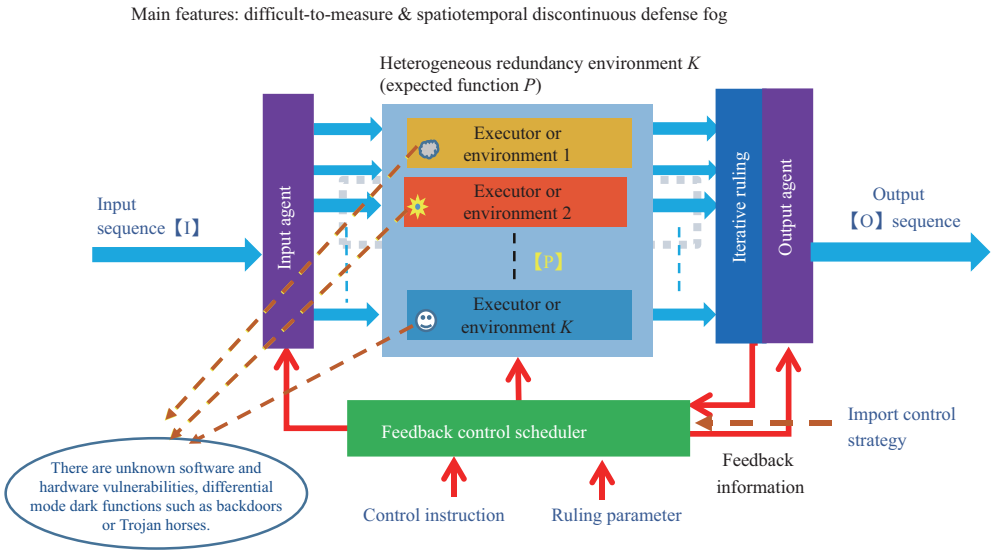

图 4　DHR 构造示意图

Figure 4　The DHR architecture

效应" [13], 也就是说能从机理上破坏试错攻击 "背景条件不变" 的假设前提, 逼迫攻击者必须具备 "非配合条件下, 动态异构冗余环境内协同一致攻击" 的能力. 换言之, DHR 构造固有的随机、多样、冗余特性, 能够产生类似量子物理的测不准效应和生物世界的拟态现象, 使得我们可以在不依赖 (但不排斥) 外部先验知识和附加防御措施的情况下, 仅依靠异构配置、策略裁决、反馈控制和多维动态重构等机制, 就能够同时应对 "基于暗功能的人为攻击" 和软硬件随机性失效引发的故障, 即可提供 Safety 和 Security 一体化的广义鲁棒控制功能.

4.8　内生安全发展愿景

内生安全的发展愿景包括:

(1) 能够在缺乏关于攻击者先验知识的情况下, 有效应对目标对象漏洞后门/木马病毒等引发的确定性风险或不确定性威胁;

(2) 防御有效性由目标对象内生安全构造与机制决定, 不依赖 (但不排斥) 任何基于检测分析的先验知识和外挂/内置式防御手段;

(3) 不以防御对象软硬构件之 "安全可信" 为前提, 适应开放式产业链和全球化生态环境;

(4) 能自然接纳或融合已有的网络安全防护技术, 按照异构化配置可获得指数量级防御增益;

(5) 构造内的功能和网络安全性可量化设计与验证度量, 能够对抗任何基于试错的暴力破解;

(6) 能为 IT (information technology), ICT (information communication technology), ICS (industrial control system), CPS (cyber-physical systems) 等领域提供 "高可靠、高可信、高可用" 三位一体的内生安全功能.

4.9　内生安全的约束条件

内生安全的约束条件包括:

(1) 仅对目标对象 DHR 构造内由于内生安全共性问题产生的安全威胁有效;

(2) 遵循要地设防/隘口部署的安全防御原则;

(3) 防御的有效性很大程度上依赖跨异构软硬件平台的软件代码移植技术的成熟度;

(4) 需要融合使用包括密码/认证等机制在内的其他安全技术应对 “来自正门的攻击”;

(5) 在初始成本、空间受限和功耗敏感的应用领域存在一定程度的工程实现挑战.

总之, 内生安全发展范式之 DHR 构造方法可以有效应对来自外部的基于构造内任何内生安全共性问题的 “歪门邪道” 式的攻击, 从理论和实践上可以终结当前基于软硬件代码设计缺陷或漏洞的攻击理论和方法. 因此, 变革当前网络安全发展范式, 可在很大程度上扭转网络空间易攻难守的战略格局, 改变现有的游戏规则. 此外, 与以往的网络安全发展范式不同, 新范式不仅是安全发展方式上的转变, 更重要的是为 IT, ICT, ICS, CPS 等领域赋予了三位一体的 “高可靠、高可信、高可用” 广义鲁棒控制功能.

4.10 基于 DHR 原理的实践规范

DHR 构造的宗旨是使防御对象软硬件系统在使命确保条件下具有一体化的内生安全功能, 可以提供一种比经典非相似余度构造 (dissimilar redundant structure, DRS) 更优异的广义鲁棒控制架构 [12]. 基于 DHR 原理的实践规范包括如下几方面.

(1) 围绕一个前提: 在不依赖 (但不排斥) 先验知识和附加或外挂安全措施条件下, 管控利用构造内可能存在的内生安全共性问题而引发的已知或未知的安全威胁.

(2) 借鉴一个公理/二种理论: 相对正确公理、可靠性理论与编码信道理论 [7];

(3) 基于一个再发现: 共识构造内个体层面的 “未知的未知” 问题能够转换为群体层面以 “已知的未知” 形式表达的差模或共模问题; 大数表决策略不具有稳定鲁棒性;

(4) 提出一种新理论: 能一体化地应对网络空间广义不确定扰动对构造内功能安全与网络安全的影响;

(5) 创造一种新构造: 动态异构冗余构造 DHR, 在其之上可建立或提供各种安全性有保障的服务功能, 并可自然地接纳既有或未来的各种安全技术所带来的环境异构性, 使之获得指数量级的防御增益 [12];

(6) 产生一种相似效应: 类似量子物理的测不准效应, 能从机理上使人为试错或盲攻击失去效能;

(7) 导入一类拟态机制: 构造环境内的动态可重构机制能够产生出类似生物界的拟态现象, 可显著地增强目标对象的防御迷雾;

(8) 获得一种可量化性能: 构造的内生安全机制与广义鲁棒控制功能导致的 “高可靠、高可信、高可用” 性可量化设计、可验证度量;

(9) 取得一种性价比优势: 相关软硬件系统在全生命周期内具有显著的比较优势.

4.11 DHR 构造的内生安全机制

如图 5 和 6 所示, 基于内生安全共性问题的广义不确定扰动能被 DHR 构造的内生安全机制变换为构造内的 “差模或共模” 扰动问题, 理论上所有差模扰动都能被动态屏蔽 (或纠错), 这使得攻击者无法识别目标、攻击效果难以评估、攻击经验无法继承、攻击场景难以复现. 调节冗余度、调节异构度、调节比对长度、调节闭环响应时间、更换裁决策略、改变反馈函数可以量化控制共模逃逸概率和持续时长. 因此, 基于 DHR 架构的内生安全 (广义鲁棒控制) 技术能将 “未知的未知安全威胁” 变换为 “已知的未知安全问题”, 理论上可以 100% 地抑制 DHR 构造内以差模形态呈现的广义不确定扰动, 并能将构造内共模形态的广义不确定扰动的逃逸概率控制在设定阈值内, 这就为网络空间安全防御的有效性提供了可量化设计、可验证度量的新发展范式.

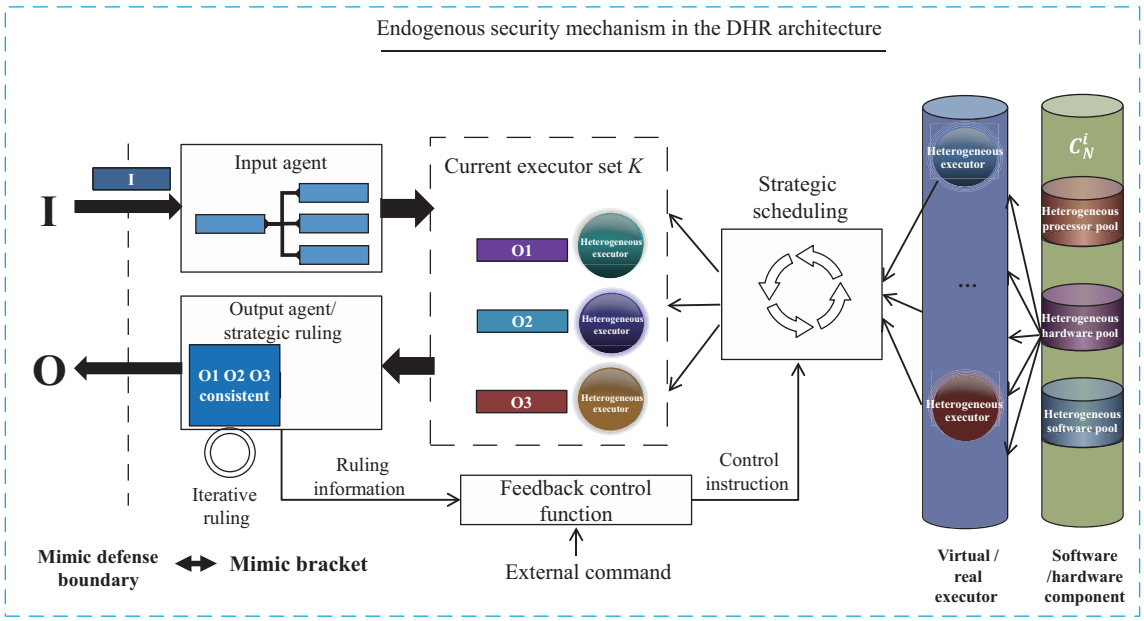

图 5 DHR 正常运行机制

Figure 5 Normal operation mechanism of DHR

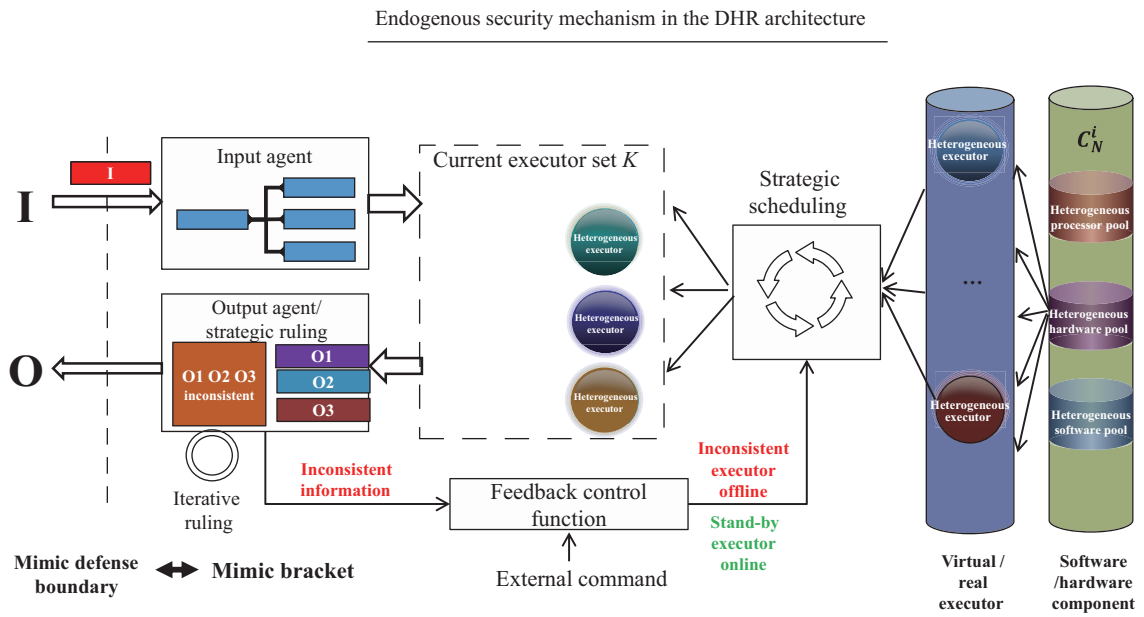

图 6 发现差模事件运行机制

Figure 6 Operation mechanism for discovering differential-mode events

如同可靠性测试那样, 检验内生安全功能/性能的最有效方式就是通过第三方白盒或破坏性注入方式, 测试/验证目标对象安全性是否能达到给定的设计阈值.

5 网络空间内生安全发展范式的动态

5.1 理论体系持续迭代

当前内生安全理论主要包含:

(1) 网络空间内生安全共性问题分析与归纳;

(2) 相对正确公理与基于编码信道的广义鲁棒控制理论;

(3) 不确定性与随机性事件归一化处理方法;

(4) 不依赖先验知识的一体化功能安全与网络安全架构;

(5) 内生安全架构安全性的设计、评估与测量方法;

内生安全发展范式的主要实践规范包含:

(1) 安全性可量化设计、可验证度量的技术体系;

(2) 基于动态异构冗余架构的技术实现;

(3) 工程实践准则与产品技术标准.

2017 年起, 科学出版社和德国 Springer 出版社先后发行《网络空间拟态防御导论》、《网络空间拟态防御原理: 广义鲁棒控制与内生安全》、《Cyberspace Mimic Defense: Generalized Robust Control and Endogenous Security》[14]、《网络空间内生安全: 拟态防御与广义鲁棒控制》4 套理论专著. 相关团队在内生安全领域已申请国际/国内专利超过 300 项, 8 项核心专利已获授权.

5.2 技术体系初步构建

在国家重点研发计划 “网络空间安全” 重点专项项目资助下, 目前网络空间内生安全的发展围绕网络通信领域形成了从硬件到软件、从构件到系统、从技术到应用的全链条布局, 为学科方向的创新发展奠定了坚实基础, 也形成了包括支撑技术、共性基础技术、网络信息基础设施、工业控制与大数据、芯片、网络服务应用等领域的系列应用技术, 如图 7 所示.

5.3 标准体系开始建立

2017 年以来, 在国家项目的支持下, 国内多家合作单位启动拟态路由器、拟态域名服务器、拟态 web 服务器、拟态防火墙、拟态交换机的研制和标准化工作, 陆续向中国通信标准化协会提交了系列拟态设备的标准建议, 包括《拟态构造域名服务器技术要求》、《拟态构造域名服务器检测规范》、《拟态构造路由器技术要求》、《拟态构造路由器检测规范》、《拟态构造 web 服务器技术要求》、《拟态构造 web 服务器检测规范》、《拟态构造交换机技术要求》, 且均在通信标准化协会立项通过. 目前, 中国通信标准行业协会已立项 16 项拟态构造设备技术标准, 即将形成行业标准.

5.4 开发成功相关技术系统

目前, 国内已经完成了内生安全基线 1.0 的技术发展, 正在开展基线 2.0 的相关工作.

基线 1.0 的主要特性是基于可信性不能确保的货架 (COTS) 级商用组件/部件来构建内生安全系统, 目前已为 IT, IC, CPS, ICS 等多个领域的产品技术开发贡献了可重现的成功模板, 已推出 10 余类 30 多种世界首台套的产品或样机, 如图 8 所示.

基线 2.0 的目标是通过突破内生安全拟态防御基础原生技术、测试技术、拟态构造技术机制, 构建工具链和开发环境, 打造网络空间内生安全产业生态环境, 打造垂直行业领域通用技术平台, 使内生安全功能成为新一代信息设施或控制装置的基本功能.

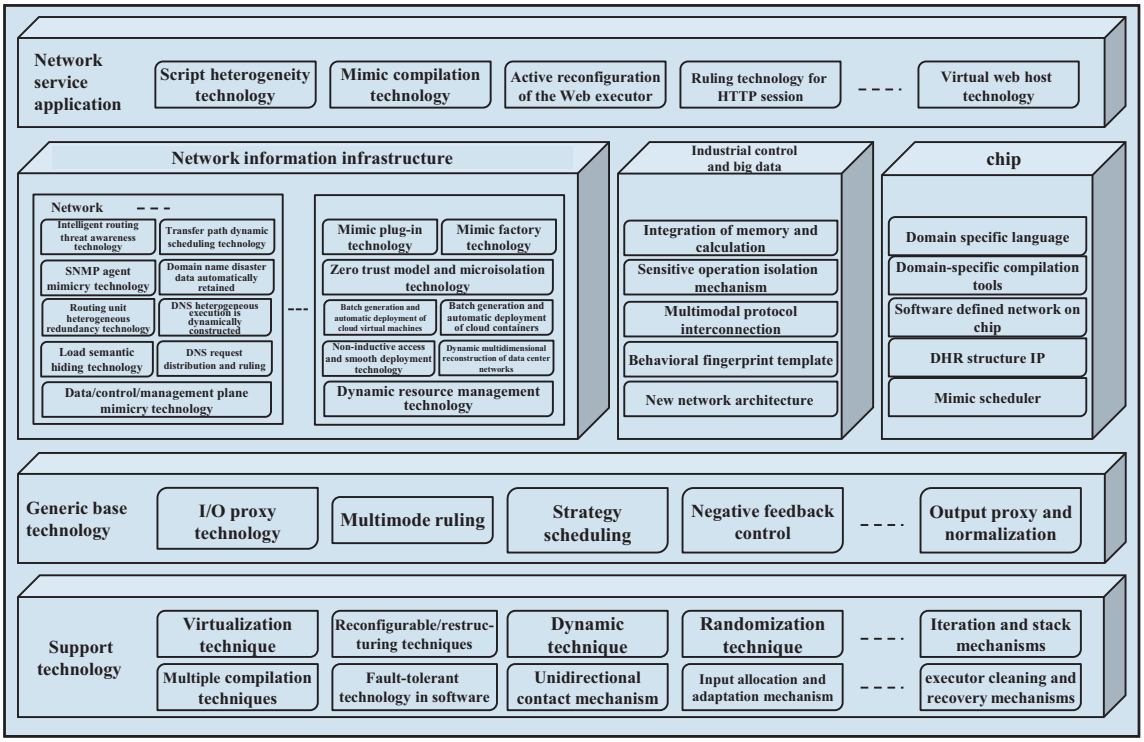

图 7　内生安全技术体系

Figure 7　Technological system of endogenous safety and security

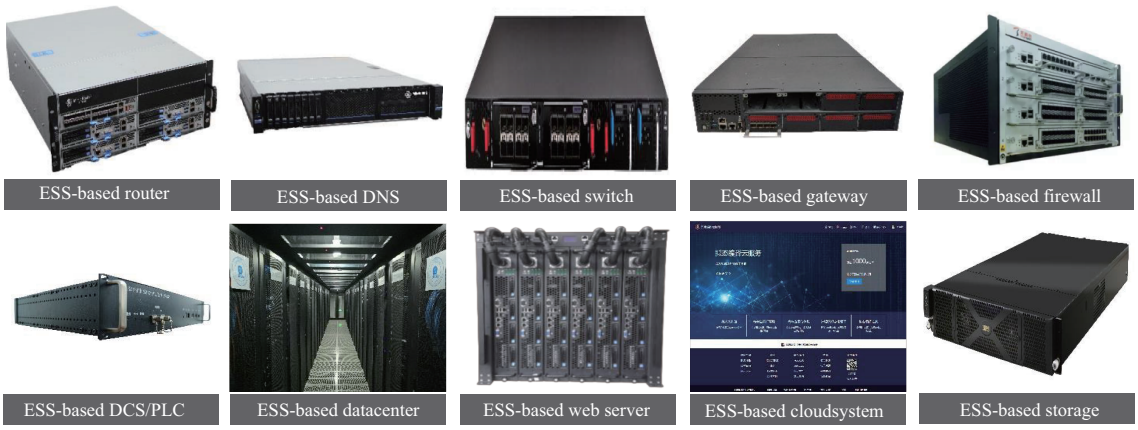

图 8　基线 1.0 产品和样机

Figure 8　Baseline 1.0 products and sample machines

5.5　体系化试点应用和部署情况

2018 年 1 月起, 基于 DHR 构造的系列内生安全产品, 包括拟态路由器、拟态域名服务器、拟态防火墙、拟态 web 服务器、拟态网关、拟态交换机等先后在国内某些电信运营商、大型数据中心、国家重点行业领域及专网中进行了体系化试点应用 (如图 9 所示), 并取得突出的试点应用效益. 应用情况表明, 基于 DHR 构造的系列内生安全产品在技术成熟度、技术普适性和技术经济性方面都达到了

图 9　体系化部署与应用

Figure 9　Systematic deployment and application

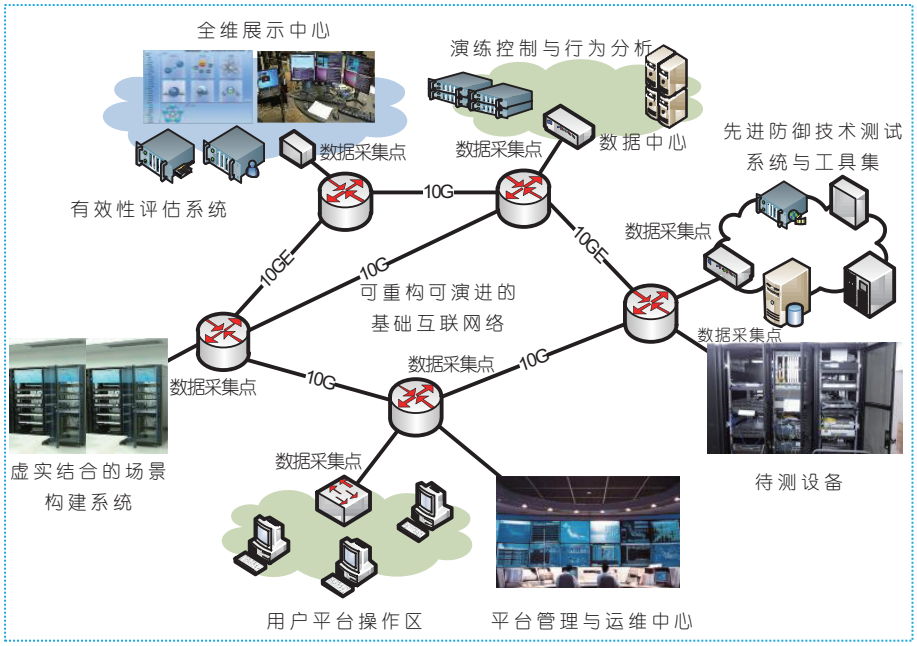

图 10　综合试验场景

Figure 10　Comprehensive test scenarios

可推广应用的程度.

5.6　构建综合试验场景

结合国家网络空间安全重点专项任务, 紫金山实验室创建了国际上首个永久在线、面向全球开放的网络内生安全试验场[1)] (如图 10 所示), 开创网络安全技术与产品评测新模式, 即 “网络信息产品是否安全由全球黑客说了算”. 基于该试验场, 自 2018 年以来, 网络空间内生安全研究团队连续三年组织开展 “强网” 拟态防御国际精英挑战赛, 在全球首创了白盒注入的攻击网安竞赛新模式. 该项赛事

1) https://nest.ichunqiu.com.

从实践上证明了安全性可以量化评估, 全球化环境下网络空间内生安全共性问题技术有解, 为全球网络空间 “互联互通、共享共治” 提供了中国智慧和中国方案.

6 结束语

内生安全理论及实践规范能够破解 IT, ICT, ICS, CPS 等领域网络内生安全共性问题不能管控的世界性难题, 使得 “从源头量化管控相关领域产品安全缺陷” 成为可能, 漏洞后门资源将失去战略性作用, 隐匿漏洞、设置后门不再具有威慑性意义, 注入病毒木马等的攻击方法将失去达摩克里斯之剑的作用. 有望彻底扭转当前网络安全等级保护制度 [15] “有合规性管理, 缺乏可量化指标”、“即使供应链自主可控也很难达成安全可信目的” 之困局, 可满足相关领域从软硬器件到系统到网络到各个层面内生安全功能赋能或部署之需求.

网络空间内生安全发展范式可以从理论和方法论角度证明 “开放性与安全性、先进性与可靠性、自主可控与安全可信、功能安全与网络安全” 的矛盾, 能够在内生安全理论与方法范畴内得到高度的统一.

参考文献

1 Kuhn T S. The Structure of Scientific Revolutions. Chicago: University of Chicago Press, 1962
2 Grey J. Jim Gray on eScience: A Transformed Scientific Method. Mountain View: Microsoft Research, 2009
3 Song B W. System Reliability Design and Analysis. Xi'an: Northwestern Polytechnical University Press, 2008 [宋保维. 系统可靠性设计与分析. 西安: 西北工业大学出版社, 2008]
4 Li H Q, Li J. Computer Network Security and Encryption Technology. Beijing: Science Press, 2001 [李海泉, 李健. 计算机网络安全与加密技术. 北京: 科学出版社, 2001]
5 Zhang Y S, Mi A R. Computer Viruses and Trojans. Beijing: Beijing Kehai Electronic Press, 2003 [张友生, 米安然. 计算机病毒与木马程序剖析. 北京: 北京科海电子出版社, 2003]
6 Manzuik S, Pfeil K, Gold A. Network Security Assessment: From Vulnerability to Patch. Rockland: Syngress Publishing, Inc., 2006
7 Feng D G, Xu J. Network Security Principle and Technolog. 2nd ed. Beijing: Science Press, 2010 [冯登国, 徐静. 网络安全原理与技术. 第二版. 北京: 科学出版社, 2010]
8 Wu H. Network Security: Attack and Defense. Beijing: China Machine Press, 2009 [吴灏. 网络攻防技术. 北京: 机械工业出版社, 2009]
9 Wu J X. Cyberspace Endogenous Safety and Security: Mimic Defense and General Robust Control. Beijing: Science Press, 2020 [邬江兴. 网络空间内生安全: 拟态防御与广义鲁棒控制. 北京: 科学出版社, 2020]
10 Wu J X. An Introduction to Cyberspace Mimic Defense. Beijing: Science Press, 2017 [邬江兴. 网络空间拟态防御导论. 北京: 科学出版社, 2017]
11 Jajodia S, Ghosh A K, Swarup V, et al. Moving Target Defense. New York: Springer, 2011
12 Wu J X. Principles of Cyberspace Mimic Defense: General Robust Control and Endogenous Safety & Security. Beijing: Science Press, 2018 [邬江兴. 网络空间拟态防御原理: 广义鲁棒控制与内生安全. 科学出版社, 2018]
13 Liu L S, Yu M L, Yan Z. A Concise Course on Advanced Quantum Mechanics. Beijing: Science Press, 2009
14 Wu J X. Cyberspace Mimic Defense: Generalized Robust Control and Endogenous Security. Berling: Springer, 2020
15 Li J. Evaluation Practice of Information System Security Level Protection. Harbin: Harbin Engineering University Press, 2016 [李嘉. 信息系统安全等级保护测评实践. 哈尔滨: 哈尔滨工程大学出版社, 2016]

Development paradigms of cyberspace endogenous safety and security

Jiangxing WU

National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002*, China*
E-mail: ndscwjx@126.com

Abstract This paper tries to systematically explain the thinking perspectives and methodologies for cyberspace security developments from the perspective of scientific research paradigm, and points out the intrinsic reasons for the corresponding development paradigm evolution. Aiming at the cyberspace endogenous security common problems and the "unknown-unknown" security threats based on these common problems, this study proposes a new theory, a new methodology, and related practice norms to solve these problems. These aim to contribute to a replicable, successful model for the cyberspace endogenous safety and security area and a new generation of information technologies and related industries using the new development paradigm. Based on a brief introduction of the concept and theory of the paradigm, this paper reviews the main development periods of cyberspace endogenous safety and security and insurmountable challenges in terms of the paradigm world outlook and methodology, summarizes cyberspace endogenous security ubiquitous problems, proposes a new development paradigm for cyberspace endogenous safety and security, and elaborates on the theoretical basis, practical norms, mechanism, and methods of the new paradigm.

Keywords endogenous security common problem, unknown-unknown security threats, relatively-correct axiom, dynamic heterogeneous redundancy architecture (DHR), endogenous safety and security development paradigm