中国科学: 信息科学 2022 年 第 52 卷 第 10 期: 1929–1937
SCIENTIA SINICA Informationis
观点与争鸣
《中国科学》杂志社
SCIENCE CHINA PRESS

论网络空间内生安全问题及对策

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: 2022–06–17; 修回日期: 2022–08–07; 接受日期: 2022–08–26; 网络出版日期: 2022–10–10

国家自然科学基金创新群体项目 (批准号: 61521003) 资助

摘要 本文从内生安全问题概念及基本特征研究出发, 提出网络空间内生安全防御范式的思维视角、方法论和实践规范. 本文指出内生安全问题与其本征功能实体间是事物内部各个对立面之间互相依赖又互相排斥关系的矛盾性表达, 具有不可分割性, 只可能演进转化或和解而不可能彻底消除; 提出网络空间内生安全问题概念并列举了相关实例; 定义了网络空间内生安全共性问题并给出了基本特征, 强调当前网络安全防御范式不可能从根本上解决内生安全共性问题; 比较了网络空间内生安全发展范式与既有范式在思维视角、方法论和实践规范层面的区别.

关键词 内生安全问题, 网络空间内生安全问题, 网络空间内生安全共性问题, 网络空间内生安全防御范式

1 引言

本文试图从还原论的角度寻求网络空间安全威胁的主因, 研究提出内生安全问题、网络空间内生安全问题以及网络空间内生安全共性问题的基本特征, 强调指出当前网络空间安全防御范式无法应对网络空间内生安全共性问题挑战. 因而亟需思维视角、方法论和实践规范层面的变革式创新, 开拓“构造决定安全” 的内生安全防御新范式 [1], 发展新一代安全性可量化设计与验证度量的信息物理系统 (cyber-physical systems, CPS), 或具有广义功能安全 [2] (generalized functional safety, GFS) 属性的数字基础设施.

2 内生安全问题

2.1 内生安全问题定义

德国哲学大师黑格尔曾经说过 “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” [3]. 从一般哲学意义上讲: 自然界或人工系统中不存在逻辑意义上的 “当且仅当的功能”, 即不存在没有矛

引用格式: 邬江兴. 论网络空间内生安全问题及对策. 中国科学: 信息科学, 2022, 52: 1929–1937, doi: 10.1360/SSI-2022-0242
Wu J X. Cyberspace's endogenous safety and security problem and the countermeasures (in Chinese). Sci Sin Inform, 2022, 52: 1929–1937, doi: 10.1360/SSI-2022-0242

盾或缺陷的事物; 从可靠性理论出发: 没有一个人工设计与制造的物理或逻辑实体是 “完美无缺” 的, 在各种扰动因素作用下其全生命周期内总存在不同前提、不同程度的功能失效问题 [4]. 因此, 任何事物, 如果在本征功能外还存在不良 (或非期望) 的副作用、暗功能, 或者一个模型内存在由构造决定的互为依存又存在矛盾关系的现象, 称为内生安全问题 [1] (endogenous safety problem, ESP). 显然, 按照唯物辩证法的对立统一观点 [5], 内生安全问题本质上是事物内部多个对立面之间互相依赖又互相排斥关系的外部表现, 是事物自身不可分割的一部分 [5]. 由此不难推论, 内生安全问题的矛盾性质决定其不可能从根本上被消除, 矛盾只能不断演进转化或和解 (通常所谓的矛盾解决, 并非说矛盾与它的对立面不存在了, 而是说它们在和解中存在或者以一种折中关系呈现). 例如, 当硬布线逻辑的控制器被基于 CPU 的微控制器 MCU 替代后, 前者随机性失效率高的矛盾被转化为后者网络安全性低的主要矛盾, 这就是矛盾现象的演进转化. 需要强调指出的是, 矛盾的转化或和解一定是要付出额外代价的, 当主要矛盾被转化为次要矛盾时, 只要是利大于弊, 相关经济技术代价总是可接受的.

总之, 内生安全问题的哲学本质是目标对象的结构性矛盾所致, 事物的多面性决定了内生安全问题存在的必然性和普遍性. 至此, 人们可能会问世上是否存在非内生安全问题, 其实 “飞来横祸” 等未构成内在矛盾关系的事件就不属于内生安全问题的讨论范畴.

2.2 内生安全问题基本特征

(1) 矛盾性. 事物除了本征功能外, 还存在衍生、派生、显式表达的矛盾性功能. 从全局意义上说, 内生安全问题如同一枚硬币的两面, 不可分割, 矛盾只能演进转化或和解, 但无法从矛盾所在事物本体中彻底消除.

(2) 潜在危害性. 通常, 显式表达的矛盾性功能尚可采取一些预先性的防范或规避措施, 但隐式表达的内生安全问题往往因其未知属性而更具威胁性.

(3) 多重表现性. 内生安全问题既有个性化表现, 也有共性化表达, 更有混合方式的呈现. 在不同场景下总存在主要矛盾与次要矛盾的区别. 个性化问题是否存在特殊解, 需要具体问题具体分析, 但共性问题往往具有普适性解的强烈需求.

(4) 外部作用性. 内生安全问题是内在结构性矛盾, 通常需要在外部触发因素成立情况下才可能导致内生安全问题产生实质性后果, 即服从哲学层面矛盾的内外因辩证关系: “内因是事物的变化根源, 外因是事物变化的条件, 外因通过内因而起作用” [5].

3 网络空间内生安全问题

3.1 网络空间内生安全问题定义

信息世界的网络空间 (cyberspace) 与现实世界的物理空间既有相同的哲学本质也有不同的问题空间与个性化的基本特征. 从网络空间现象观察, 一个确定功能的软硬件实体总存在着显式副作用或隐式暗功能 (包括蓄意设置的后门或不经意间误用的陷门等); 从网络空间工程实践规范可知, 无论采用何种设计方法都不可能获得一个没有伴生或衍生功能的 “纯粹功能”; 从网络空间功能安全角度观察, 既存在软硬件内生安全问题因随机性或不确定性扰动而导致的系统功能不可靠表现, 也存在内生安全问题被外部或人为蓄意利用导致的系统非期望功效. 我们将这些基于软硬件内生安全问题或结构性矛盾呈现的非期望功能表达, 称为网络空间内生安全 (cyberspace endogenous security & safety, CESS) 问题 [1] (以下简称 CESS 问题). 显然, CESS 问题与一般内生安全问题一样, 同样具有矛盾性、潜在危害性、多重表现性和外部作用性等基本特征, 但受网络空间泛在性、虚实世界关联性、技术与产业供应

链格局和人机物或人网物多元融合等特殊因素影响, CESS 问题的成因机理及表现形式更为复杂, 具有一些特殊性状. 尤其是, 基于信息物理系统软硬件漏洞后门等的内生安全共性问题几乎遍及数字世界的每一个角落.

3.2 漏洞后门等问题

漏洞后门以及相关问题是网络空间标志性的内生安全共性问题 (见本文第 4 节). 漏洞后门等问题的主要区别和共同性在于以下几方面.

(1) 主客观性. 漏洞为软硬件代码设计中的无意识行为, 与人性善恶无关, 后门则是人为刻意设计或蓄意植入的, 而陷门通常是使用者在不知情条件下误用了带有后门功能的软硬件所致的. 就人类目前的工程技术能力而言, 还很难彻查或穷尽复杂系统中的漏洞后门或陷门.

(2) 先天与后天性. 漏洞往往是目标对象本征功能代码设计阶段或版本修订迭代过程中的缺陷, 而后门既可在设计阶段蓄意融入目标对象本征功能, 也可在使用及售后服务阶段或环节刻意植入.

(3) 可利用性. 后门功能在攻击可达条件下具有确定的可利用性, 漏洞的可利用性则存在不确定性 [6], 但两者都依赖现有网络空间技术与生态环境及攻防博弈游戏规则. 此外, 漏洞后门的利用通常需要以注入攻击代码为前提, 实际效果与目标运行环境和攻击者经验强相关.

(4) 危害性. 与主客观生成动机无关, 漏洞后门皆可能给信息物理系统带来安全威胁或导致安全事故.

3.3 网络空间内生安全问题举例

网络空间安全问题包含的内容非常广泛, 为了更好地理解其概念和内涵, 本文列举了大数据、人工智能、区块链、零信任架构、数字加密与认证等当前 “热门” 技术存在的个性化或共性化或宿主依赖型的内生安全问题.

(1) 大数据技术能够根据算法和全数据集发现未知的规律或特征, 而蓄意污染数据样本、恶意触发算法设计缺陷也可能使人们误入歧途 [7], 结果的不可解释性是大数据技术个性化的内生安全问题, 而其处理系统的软硬件漏洞后门问题则是无法回避的共性化内生安全问题.

(2) 当前主流人工智能技术靠大数据、大算力、深度学习等算法获得前行动力, 而结果的不可解释性、不可预判性、不可推论性则是 AI 技术个性化内生安全问题 [8], 同时也存在宿主系统共性安全问题.

(3) 区块链技术开辟了无中心记账方式的新纪元, 其共识机制却不能避免市场占有率大于 51% 的相同软硬件产品中的同一漏洞后门问题 [9], 这是区块链 1.0 技术因为宿主依赖而导致的内生安全问题.

(4) 基于分布式逐级认证体制的零信任安全架构, 形式上具有很强的开放性和安全性, 但相关认证节点或实现系统中若存在可被利用的软硬件漏洞 [9], 则也存在宿主依赖型的内生安全问题.

(5) 计算机体系结构中的分支预测 (branch prediction) 是一种解决 CPU 处理分支指令 (if-then-else) 导致流水线失败的数据处理优化方法. 然而, 幽灵漏洞 (specter) 正是这种降低内存延迟、加快执行速度的 “预测执行” 之副作用或暗功能, 可能造成受害进程保存的敏感数据或信息泄露事件 [10], 属于典型的网络空间内生安全个性化问题.

(6) 云计算/数据中心技术改变了信息服务提供方式, 提升了资源利用效率, 但是敏感数据泄漏、数据完整性、服务功能中断以及服务性能劣化等网络攻击问题 [11,12] 使人们极度担心 “鸡蛋都放在一个篮子里” 的安全性. 这属于典型的宿主依赖型网络空间内生安全问题.

(7) 即使数字加密或认证算法在数学意义上可能已经足够强大, 但是执行加密认证算法的软硬件

系统中若存在漏洞后门并可被利用 [13,14], 那将导致灾难性后果. 因此, 加密认证也属于典型的宿主依赖型内生安全问题.

(8) 既有的网络安全技术系统无一不是由软硬件构成的, 在为目标对象提供期望的安全防御功能的同时, 难以避免由于自身原因给目标系统引入新的安全漏洞, 这是网络空间内生安全共性问题所致的.

(9) 基于云计算/边缘计算等技术的 5G 服务平台或网络, 因为软硬件设计存在未知的缺陷可能招致网络攻击造成信息泄露或数据资源被控或 "宕机" 问题等 [15].

(10) 图灵机只是回答了什么是理论层面的可计算问题, 冯 · 诺依曼 (John von Neumann) 计算结构只是解决了什么条件下可计算问题能够以工程化方式实现, 但计算机从机理上就无法区分什么是善意或恶意的计算.

以上例子都属于网络空间 "内生不安全或内在矛盾性技术" 的范畴, 尽管有些具有典型的个性化特征 (例如, 大数据、人工智能等), 但如前文所述, 网络空间中所有技术架构或算法的实现都要以各种软硬件为基础, 因而不可避免地存在个性化、共性化以及宿主依赖型 CESS 问题的多重或混合呈现形态.

4 网络空间内生安全共性问题

4.1 共性问题定义

正如网络空间内生安全问题定义那样, 网络世界 (cyber) 本质上是由综合了计算、网络、传感和物理环境的 CPS 系统构成的, 而信息物理系统的 "基础建筑材料" 则是由各种软件、硬件代码组成的 [16]. 按照矛盾论的说法, 网络空间任何事物都存在矛盾, 人为设计和制造的软硬件中存在缺陷或漏洞问题也概莫能外. 从哲学层面上说, 共性 (generality, ubiquity) 特征, 就是某个领域或行业内普遍或泛在化存在的某些特性, 它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. 于是, 我们将软硬件漏洞后门及相关问题统称为 "网络空间内生安全共性问题" [9] (common problem of CESS).

4.2 共性问题成因与机理

(1) 认知能力桎梏. 由于人类科技发展和认知水平的阶段性特征导致软硬件代码设计脆弱性或漏洞问题不以人们意志转移, 其内在矛盾性也不可能彻底避免. 例如, 分支预测技术发明者, 肯定想不到几十年后这一方法会成为 "幽灵、熔断" 漏洞的本因问题 [10].

(2) 生态环境依赖. 经济全球化是人类社会生产模式里程碑式的进步 (尽管目前正面临来自国际政治格局的严峻挑战). 然而, 基于专业化分工形成的生产与经贸关系、"你中有我、我中有你" 的技术链、供应链、服务链等全产业链格局, 存在严重的路径依赖问题, 使得软硬件产品在设计、制造、加工、营销和售后服务等环节中 "隐匿漏洞、植入后门、陷门泛滥" 成为无法杜绝的 "结构性" 矛盾问题 [17].

(3) 工程能力限制. 就当今人类工程技术能力而言, 即使是对几百万乃至几亿行代码的软件系统, 或者是几千万乃至上百亿只晶体管构成的硬件芯片只进行设计功能完备性检查都要花费极大的人力、物力和时间代价, 如果想彻查 "幽灵般" 的漏洞后门等暗功能, 不用说现有的科技水平是否能够设计出规模庞大、极其复杂且没有任何缺陷的测试规范和相应的工具软件, 仅就克服 "状态爆炸" 这一棘手问题, 在可预见的将来, 仍然是难以逾越的工程技术壁垒.

(4) 人类逐利本性. 只要网络空间 CPS 系统及相关产品在开发、设计、生产、制造、营销、售后等环节中存在软硬件代码设计漏洞或植入后门或无意间引入陷门 (芯片 IP 核或开源代码中的后门) 等问题, 利益攸关方就可借此途径不择手段追逐各种显式或隐式好处, 只要是有利可图, 网络空间的攻击行动就不可能自动停止.

(5) 不受约束行动. 任何一个 CPS 系统只要存在一个高危漏洞或被植入或引入一个后门 (陷门), 网络攻击者就可以不受地域、时间、法律、行为准则、道德规范等约束, 造成目标对象服务不可信甚至功能失效, 也包括侵犯用户信息或数据的完整性、机密性与可用性.

不言而喻, 在软硬件的算法或协议等设计、开发、加工、制造、销售、应用、售后服务等全产业链诸多环节中, 存在的漏洞后门及网络攻击必然会成为网络空间内生安全共性问题. 尤其是同质化的信息物理系统或数字基础设施之内生安全共性问题威害更广泛, 破坏性更严重, 是数字经济与社会建设中最大的 "公害问题". 不幸的是, 迄今为止, 人类对基于网络空间内生安全共性问题的未知攻击几乎无计可施. 更为糟糕的是, 长期以来信息物理系统及相关行业软硬件产品的网络空间内生安全性都无法给出可量化设计、可验证度量的技术指标 [17], 包括声称 "网络空间安全守护神" 的所有网络防御或安全产品. 这不仅颠覆了人们对现代商品经济产品质量保证体系的认知, 而且使得信息物理系统 CESS 问题大有发展为网络空间 "永恒之痛" 的趋势.

4.3 共性问题基本特征

(1) 不可避免性. 一般意义上, 只要是由软硬件构成的 CPS 系统或控制装置等都不可避免地存在已知或未知的内生安全共性问题.

(2) 条件可用性. 内生安全共性问题不是在所有条件下都能成为网络攻击的可利用资源, 也不是所有情况下都能导致安全事故. 内因需通过外因起作用, 例如, 当网络攻击不可达或漏洞后门无法注入攻击代码时, 内生安全共性问题通常不会自动成为网络安全事件 [18].

(3) 矛盾转移性. 任何在目标系统上外挂或嵌入或内置各种基于软硬件的安全防护措施, 由于自身无法保证不存在内生安全共性问题, 在转化一个矛盾时很难避免产生其他或关联的内生安全共性问题. 换言之, 只要附加安全措施是在同一目标对象中不断堆叠或迭代, 内生安全共性矛盾就会以不同形式演进转化.

(4) 问题交织性. 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功能安全领域, 网络空间内生安全共性问题使得基于随机性或 "已知的未知" 扰动之弹性控制理论前提难以成立, 功能安全问题不可避免地演进为 Security-Safety 交织或复合叠加问题, 即广义鲁棒控制问题 (generalized robust control problem, GRCP) 或者广义功能安全问题 [3] (security & safety intertwine problem, SSIP). 显然, 网络安全与功能安全的交织问题, 使得 CPS 系统及相关软硬件产品必须具有一体化的广义鲁棒控制或网络弹性/韧性 [2] (cyber resilience/toughness) 功能.

5 创新网络空间内生安全防御范式

需要强调指出, CESS 问题与基于动态异构冗余构造 [1] (dynamic heterogeneous redundancy, DHR[1)]), 的网络空间内生安全防御 (又称拟态构造防御 (mimicry structure defense, MSD)) 不是同一层面的讨论对象. 前者研究分析什么是网络空间内生安全共性问题以及成因机理和基本特征; 后者

1) DHR 是指建立在 "相对正确公理" 逻辑表达与闭环鲁棒控制基础上, 基于策略裁决的迭代式多维动态重构结构, 由功能等价的异构执行体、输入/输出代理、采用迭代机制的策略裁决和反馈控制与调度器等构成, DHR 构造的抽象模型参见文献 [1].

研究如何运用创新的 DHR 构造, 从工程技术与系统层面, “免疫” 构造环境内基于 CESS 问题的网络攻击影响, 以及一体化地解决功能安全与网络安全交集区特有的 SSIP 问题 (也可称之为一体化安全问题域, 参见文献 [2] 的 Figure 1).

5.1 当前网络安全防御范式问题

由于 CESS 问题特别是内生安全共性问题已成为网络时代数字经济社会的最大 “公害”, 而当前主流的网络安全防御范式则显得力不从心.

(1) 思维视角陈旧. 建立在威胁感知、特征提取等先验知识积累基础上的 “亡羊补牢” 式被动防御 (也包括蜜罐、沙箱、移动目标防御等非积极的主动防御), 尽管可以对已知甚至 “已知的未知” 安全威胁 (对可能发生的风险已知, 但对风险发生的时机和可能产生的危害程度未知) 提供有效安全防护, 但是针对信息物理系统内生安全共性问题的 “未知的未知攻击” [17] (可能发生什么攻击未知, 因而也不了解攻击发生的时机和影响程度), 当前思维视角下的 “知其然也知其所以然” 的技术路线就不可能对未知性质的威胁提供可靠的防御 [9].

(2) 方法论的禁锢. 基于先验知识库的 “打补丁” 或 “附加防御” 方法论, 确实可以通过持续的演进迭代有条件地降低已知漏洞后门、病毒木马等问题的危害, 但仍然无法排除 “补丁” 或附加防御措施自身可能给目标对象物理或逻辑空间造成新的内生安全共性问题. 这将导致修补一个漏洞问题时可能在同一空间内产生另一个漏洞的无尽困境.

(3) 安全性无法量化. 因为附加或外挂式防御工程规范建立在已知或 “已知的未知” 威胁基础上, 其有效性与安全问题的成因和威胁机制的精准掌控程度强相关 (要求知其然也知其所以然), 所以从理论和实践层面都不可能对 “未知的未知” 安全威胁 [17] 形成任何有效防御, 更谈不上给出明确意义的可量化设计与验证度量的安全性指标了.

由此, 也引发一系列科学难题. 诸如, 如何才能证明这种 “打补丁/叠罗汉” 式的附加安全防护是安全可信的? 如何才能证明 “这些补丁” 其自身是安全可信的? 由于内生安全共性问题的存在, 既有的安全技术怎样才能自证清白? 等等 [9]. 理论和实践表明, 有些内生安全矛盾虽然不能消除但可能和解. 例如, 实施严格的网络物理隔离, 使内网安全漏洞无法被外网攻击触发 [19]. 不过, 诸如 “封门补漏” “主动探测” “加密认证” 等主流的附加型安全防御措施, 无论采用 “外挂” “内置” “嵌入” 或其他何种技术衔接或植入方式, 总是将内生安全矛盾在同一目标对象、同一时空维度、统一资源环境内作 “面多了加水, 水多了添面” 不变性质和时空位置的循环转化, 或者非结构化地利用随机性、多样性和动态性等安全元素实施系统开销很大的 “移动目标防御 (moving targets defense, MTD)” [20]. 即便如此, 这样的技术安排既无法从根本上应对 “未知的未知” 安全威胁, 也不能避免持续添加的系统防御开销导致全生命周期技术经济性的不断劣化.

5.2 内生安全防御新范式

(1) 思维视角的转换. 如何能在不依赖 (但不排斥) 攻击者先验知识或精确感知与行为分析的前提下, 有效抑制基于内生安全共性问题的 “已知的未知” 随机性扰动及 “未知的未知” 不确定网络攻击, 这是新范式研究的出发点与立足点. 著名科学家钱学森院士在系统工程论中指出: “从复杂问题的总体入手, 认为总体大于各部分之和, 各部分虽较劣但总体可以优化.” [21] 当目标对象单体可靠性提升遭遇 “天花板” 问题时, 假设任何随机性扰动不会同时导致多数冗余体共模缺陷产生相同失效的前提成立, 则运用功能等价同构冗余构造的确能够大幅度地提升系统可靠性水平 [1]. 尽管如此, 同构冗余的信息物理系统在面对网络攻击挑战时其原有的假设前提则无法成立, 因为网络威胁不具有随机性

规律, 借助共模缺陷可以达成任何期望的攻击目的, 这是传统功能安全或高可靠系统不具有网络安全能力的核心问题所在. 异构冗余构造虽然存在实现技术代价较高, 应用领域受限的问题, 但是因为不存在相同设计或制造可能存在的已知或未知缺陷, 因而理论上不会发生共模失效. 恰当地运用这种既能对付差模摄动又能避免共模扰动的双重构造效应, 在应对网络空间人为攻击或蓄意扰动 (不包括试错攻击) 时, 使得攻击者很难在同一时间、同一输入激励条件下, 基于 "异构冗余空间" 内的不同攻击资源和不同攻击路径形成协同一致的攻击逃逸效果 [1]. 事实上, "入侵容忍技术" 正是将经典的非相似余度构造 (dissimilar redundancy structure, DRS) [1] 作为 "拦截漏网之鱼的最后一道屏障". 功能安全和网络安全的技术实践表明: 异构冗余构造不仅在功能安全领域是转化随机干扰和不确定扰动为差模形态表达的必要条件, 在网络安全领域也是转化人为攻击和不确定安全威胁为差模形态表达的必要条件. 为此, 我们将这种基于异构冗余构造形成的不依赖攻击者先验知识的差模感知体制与相关处理机制, 称为内生安全功能 [1] (endogenous security & safety function, ESSF).

(2) 创立新方法论. 运用功能等价异构冗余构造 (DHR) 及相关策略裁决与反馈迭代机制, 可以将个体层面的不确定扰动和未知网络攻击问题变换为群体层面以差模形式表达的 "已知的未知" 概率问题, 尽管在此情况下我们还不能实时地确定差模呈现结果的内在原因或机理 (通过后台或脱机处理技术实际不难分析之). 换句话说, 在异构冗余空间内我们只需实时发现差模问题场景, 即可开展场景迭代变换防御, 其有效性与差模问题的随机性或不确定性弱相关甚至不相关. 理论和实践可以证明, 当 DRS 变革为基于策略裁决的动态异构冗余构造 (DHR) 时, 确实能在缺乏先验知识条件下感知个体层面差模形态的 "已知的未知" 扰动或 "未知的未知" 攻击 [22, 23], 并通过各种纠错屏蔽或清洗重构或策略裁决或反馈迭代等技术应用. 将当前问题场景或主要矛盾作时空维度的迁移或变换, 可有效应对包括试错攻击或盲攻击在内的协同性质共模逃逸. 毫无疑问, 内生安全的 DHR 构造是新范式方法论的核心内涵.

(3) 更新实践规范. 因为无论是 "已知的未知" 或 "未知的未知" 差模扰动影响, 还是人为或非人为因素导致的差模作用, DHR 结构都能给出 "可量化设计与验证度量" 的安全性指标, 这是不同与以往 "尽力而为" 传统实践规范的核心所在 [1]. 理论上, 如果能保证 DHR 架构内各运行场景间 "绝对异构" 的话, 可以百分之百地抑制差模事件, 并使共模逃逸概率趋于零. 但是, 世界上不存在绝对化的事物, 因此 "绝对异构" 也不可能成为工程技术实践追求的目标 [9]. 作为一种合理折中, 只要相关部件能够满足设定的安全性要求, 清洗恢复、智能重构、基于裁决的动态反馈控制等时空转换或迁移技术, 可以获得 "兵来将挡水来土掩" 的自适应智能迭代效果. 需要特别指出的是, DHR 构造环境内策略性的部署不同厂家开发、采用不同防御机理的附加型网络安全产品, 可以显著降低异构冗余实现复杂度、提高产品的技术经济性、获得指数量级安全性与可靠性增益 [1], 且无需对相关软硬件本身的安全性或可信度提出过于苛刻的要求, 这一自然的、非排他的融合性质是 DHR 构造所特有的 [17]. 显而易见, 新的实践规范正是以 DHR 作为各种 CPS 系统的 "钢筋混泥土骨架", 以相关本征功能技术和现有或未来的网络安全技术作为 "混泥土配料", 构成具有 "钢筋混泥土质地" 的信息物理系统 [1].

(4) 拒止试错攻击. 在可靠性或传统功能安全的前提条件中, 一般无需 "对任何潜在的破坏都要关注对抗性" 的网络弹性 [24], 而在现代 CPS 系统中这恰恰是不可或缺的功能. 不幸的是, 传统功能安全的有利工具 DRS, 因为缺乏时间鲁棒性和品质鲁棒性, 不可能承受持续不断的试错攻击. 与之相反, DHR 构造却能从机理上颠覆试错攻击所必须的背景不变前提, 使任何试错算法 (包括 APT 攻击等) 在理论上无法收敛 [17]. 这是 DHR 构造所特有的属性.

需要特别强调的是, DHR 构造的安全区域仅限于输入代理、策略裁决和反馈控制部件环绕构成的边界内, 在此区域可有效管控架构内存在的内生安全共性问题, 但不能应对架构外的安全问题, 其攻

击表面就是它的安全边界 [1]. 例如, DHR 可以管控加密算法宿主系统中存在的漏洞后门或病毒木马等问题, 但无法解决加密算法自身设计问题; DHR 可以管控 TCP/IP 协议处理过程中的内生安全问题, 但无法克服 TCP/IP 协议自身的设计缺陷.

6 结束语

本文研究了内生安全问题的一般概念和基本特征, 得出网络空间主要安全威胁源于内生安全共性问题的结论; 研究表明该问题基本特征及其矛盾性质决定了无论采取什么样的演进转化或和解措施, 都无法突破当前网络安全防御范式自身构筑的桎梏; 研究发现功能等价条件下的动态异构冗余构造 DHR, 可以在 “只知其然不知所以然” 的状态下, 将独立个体的不确定安全问题变换为群体层面以差模形态表达的概率事件, 从而为 CPS 系统安全性不能量化设计与验证度量的世界性难题找到了解决方案; 研究指出 DHR 基于策略裁决的反馈控制构造, 不但能自然地接纳各类传统网络安全技术实施异构环境的策略性配置, 而且据此可获得指数量级的安全增益, 并能从机理上化解网络安全领域最为棘手的人为或智能 “试错” 攻击问题; 研究还发现 DHR 构造可以一体化地解决 CPS 系统中功能安全和网络安全交织区中的内生安全共性问题, 可为信息物理系统或网络空间软硬件产品赋能广义功能安全的属性; 研究指出但凡演进转化或和解共性安全矛盾就不可能不付出代价, 只是相对主要矛盾的解决, 技术经济代价就是次要矛盾了. 最后, 本文从思维视角、方法论和实践规范层面概略描绘了网络空间内生安全防御范式与既有范式间的主要区别.

读者对文中未能详尽说明的内容, 请关联参考文献所列材料.

参考文献

1 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]

2 Wu J X. Problems and solutions regarding generalized functional safety in cyberspace. Secur Saf, 2022, 1: 2022001

3 Hegel G, Wallace W. The Logic of Hegel. Oxford: Oxford University Press

4 Birolini A. Quality and Reliability of Technical Systems. Berlin: Springer, 1994

5 Xiao Q, Li X L, Wang Y X. Principles of Dialectical Materialism. 1st ed. Beijing: People's Publishing House, 1981 [肖前, 李秀林, 汪永祥. 辩证唯物主义原理. 第一版. 北京: 人民出版社, 1981]

6 Lei K N, Zhang Y Q, Wu C S, et al. A system for scoring the exploitability of vulnerability based types. Comput Res Dev, 2017, 54: 2296–2309 [雷柯楠, 张玉清, 吴晨思, 等. 基于漏洞类型的漏洞可利用性量化评估系统. 计算机研究与发展, 2017, 54: 2296–2309]

7 Goodfellow I, Pouget-Abadie J, Mirza M, et al. Generative Adversarial Nets. In: Neural Information Processing Systems. Cambridge: MIT Press, 2014

8 Yampolskiy R V, Spellchecker M S. Artificial intelligence safety and cybersecurity: a timeline of AI failures. 2016. ArXiv:1610.07997

9 Wu J X. Development paradigms of cyberspace endogenous safety and security. Sci Sin Inform, 2022, 52: 189–204 [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]

10 Kocher P, Horn J, Fogh A, et al. Spectre attacks: exploiting speculative execution. In: Proceedings of IEEE Symposium on Security and Privacy (SP), 2019

11 Takabi H, Joshi J B D, Ahn G J. Security and privacy challenges in cloud computing environments. IEEE Secur Privacy Mag, 2010, 8: 24–31

12 Yu N H, Hao Z, Xu J J, et al. Research progress of cloud security. Acta Electron Sin, 2013, 41: 371–381 [俞能海, 郝卓, 徐甲甲, 等. 云安全研究进展综述. 电子学报, 2013, 41: 371–381]

13 Wang X, Yu H. How to break MD5 and other hash functions. In: Proceedings of the 24th Annual International Conference on Theory and Applications of Cryptographic Techniques, 2005

14 Wang X, Yin Y L, Yu H. Finding collisions in the full SHA-1. In: Advances in Cryptology—CRYPTO 2005. Berlin: Springer, 2005
15 Ahmad I, Kumar T, Liyanage M, et al. Overview of 5G security challenges and solutions. IEEE Comm Stand Mag, 2018, 2: 36–43
16 Lee E A. Cyber physical systems: design challenges. In: Proceedings of the 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing (ISORC), 2008
17 Wu J. Cyberspace Mimic Defense. Cham: Springer International Publishing, 2020
18 Dong Y, Yang X, Deng Z, et al. Black-box detection of backdoor attacks with limited information and data. In: Proceedings of the IEEE/CVF International Conference on Computer Vision, 2021. 16482–16491
19 Wang Y J, Yang J H, Guo G T, et al. Analysis and prospect of physical isolation technology for network security. Inf Secur Commun Priv, 2016, 2: 117–122 [王永建, 杨建华, 郭广涛, 等. 网络安全物理隔离技术分析及展望. 信息安全与通信保密, 2016, 2: 117–122]
20 Jajodia S, Ghosh A K, Swarup V, et al. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. New York: Springer, 2011. 54
21 Zheng X H, Qu X D. Development process of Qian Xuesen's thought on systems engineering. Sci Tech Rev, 2018, 36: 6–9
22 Ren Q, Wu J, He L. Performance modeling based on GSPN for cyberspace mimic DNS. Chin J Electron, 2020, 29: 738–749
23 Ren Q, Guo Z, Wu J, et al. SDN-ESRC: a secure and resilient control plane for software-defined networks. IEEE Trans Netw Serv Manage, 2022. doi: 10.1109/TNSM.2022.3163198
24 Ross R S, Pillitteri V Y, Graubart R, et al. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. Gaithersburg: National Institute of Standards and Technology, 2019

Cyberspace's endogenous safety and security problem and the countermeasures

Jiangxing Wu

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

Abstract In this article, we present the general concept and characteristics of the endogenous safety issue in cyberspace along with the thinking perspective, methodology, and practice norms of the endogenous security & safety defense paradigm. Studies have shown that the endogenous safety problem and its intrinsic functional entities are contradictory expressions of the interdependent and mutually exclusive relationships between the opposites within things, which are indivisible and can only be transformed or reconciled but not eliminated. Next, the cyberspace endogenous security & safety problem concept and the related instances are put forward. The common problems of endogenous security & safety in cyberspace are defined with the basic characteristics and related instances are listed, which emphasize that the current cyberspace security defense paradigm cannot fundamentally solve the endogenous security & safety common problems. The paper compares the differences between the cyberspace endogenous security defense paradigm and the existing paradigm in terms of thinking perspective, methodology, and practice norms.

Keywords endogenous safety problem, cyberspace endogenous security & safety problem, cyberspace endogenous security & safety common problem, cyberspace endogenous security & safety defense paradigm