用科学的网络安全观指导关键信息基础设施安全保护

李旸照[1,2]，沈昌祥[3]，田楠[4]

（1. 中国长江三峡集团有限公司，北京 100038；2. 浙江大学控制科学与工程学院，浙江 杭州 310027；
3. 中国工程院，北京 100088；4. 中国人民解放军 91977 部队，北京 100089）

摘　要：在当前竞争日益激烈的国际网络空间安全博弈中，关键信息基础设施安全形势严峻。从科学原理上看，网络安全风险的实质是人们对信息科学认知逻辑的局限性，建设“刀枪不入”的网络防御体系是不可能的；从经济效益上看，建设这种网络防御体系也不一定划算。网络安全工作的关键是安全目标的收敛，重点是确保完成计算任务的逻辑组合不被篡改和破坏，从而实现正确计算。围绕这个安全目标，从逻辑正确验证理论、计算体系结构和计算工程应用模式等方面进行科学技术创新，解决了逻辑缺陷不被攻击者利用的问题，形成攻防矛盾的统一体，为信息系统建立主动免疫能力。

关键词：关键信息基础设施；网络安全；可信计算；主动免疫

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.2096−3750.2019.00114

Guiding the security protection of critical information infrastructure with scientific network security concept

LI Yangzhao[1,2], SHEN Changxiang[3], TIAN Nan[4]

1. China Yangtze Three Gorges Group Co., Ltd., Beijing 100038, China
2. School of Control Science and Engineering, Zhejiang University, Hangzhou 310027, China
3. Chinese Academy of Engineering, Beijing 100088, China
4. Chinese People’s Liberation Army 91977 Force, Beijing 100089, China

Abstract: In the current increasingly competitive international cyberspace security game, critical information infrastructure is facing a severe security situation. From the view of scientific principle, the essence of network security risk is the limitation of people’s cognitive logic of information science. It is impossible to build a solid network defense system, and it is not necessarily cost-effective from the view of economic benefits. In network security work, the most important thing is the convergence of security objectives. The key is to ensure that the logical combination of computing tasks is not tampered with or destroyed, and to achieve correct calculation. Focusing on this security goal, scientific and technological innovations were made in such aspects as logical correct verification theory, computing architecture and application mode of computing engineering. The problem that logical defects were not exploited by attackers was solved, a unity of offensive and defensive contradictions was formed, and the active immunity capability for information systems was established.

Key words: critical information infrastructure, network security, trusted computing, active immunization

1　引言

习近平总书记指出：“没有网络安全就没有国家安全，没有信息化就没有现代化”。美国社会学家约翰·奈斯比特在《大趋势》一书中提到“目前我们的社会正在发生重大变化，其中最为微妙也最具有爆炸性的变化是从工业社会向信息社会的转变，一个新的文明正在我们生活中出现。”这被称为历史上重大变革的信息化社会，代表着人类的经济结构正在从“以物质与能量为重心”向“以信息

收稿日期：2019−08−30；修回日期：2019−09−12

与知识为重心”转变，而以互联网为主的信息技术革命则是社会信息化的主要推动力，当今世界已通过互联网变成了“地球村”。

网络和信息资源的互联互通，形成了覆盖全球的网络空间，成为与陆地、海洋、天空和太空同等重要的人类活动新领域。网络空间由互联网、通信网、计算机系统、自动化控制系统、数字设备及其承载的应用、服务和数据等组成，网络空间和实体空间之间，逐步形成了深刻的、复杂的相互嵌套结构，网络空间安全已成为事关全局的重大问题。

2　我国关键信息基础设施安全保护面临的3个重大风险

网络空间安全的核心在于关键信息基础设施的安全。关键信息基础设施承载了社会治理、人民生活最基础的公共服务，聚集了经济运行、劳动创造等最广泛的资源财富，彰显了国家建设、运营、维护和使用网络神圣不可侵犯的主权。随着云计算、物联网、大数据和人工智能等新一代信息技术的快速发展，我国关键信息基础设施面临的内/外部安全形势发生了很大变化，网络安全威胁呈现高烈度、未知性、多样化的趋势。

2.1　高烈度对抗的风险

习近平总书记强调：“中华民族伟大复兴，绝不是轻轻松松、敲锣打鼓就能实现的，在前进道路上，我们面临的风险考验只会越来越复杂，甚至会遇到难以想象的惊涛骇浪。”网络攻击方式多样、手段隐蔽、潜伏期长、造成的损失巨大，在时间和空间上都不受边界制约。从国内外一系列网络安全事件来看，对网络中关键信息基础设施的攻击已经成为国家级对抗中的首选武器，以互联网为代表的网络空间，已经成为各方势力角力和斗争的主阵地、主战场。

2.2　无险可守的风险

特种木马和网络攻击手段具有极度危险性，物理隔离已经无法确保抵御网络攻击。随着技术的进步和发展，网络攻击将成为关键信息基础设施稳定运行的主要风险之一。2010年“震网”病毒致使伊朗布什尔核电站20%的离心机报废；2012年“火焰”病毒致使中东石油工业网络瘫痪；2013年“棱镜门”事件致使多国政府、科研机构和企业的信息网络被入侵；2015年“乌克兰电网”事件中，“Black Energy”病毒造成乌克兰大规模停电；2017年“勒索病毒”事件中，“永恒之蓝”网络武器导致全球150多个国家的超过30万台计算机（含服务器）和自动化控制设备感染病毒。这些特种木马和特种网络攻击手段是针对物理隔离网和工业控制系统定制的，攻击者通常熟悉被攻击的系统和网络结构，采取先进的攻击技术，病毒扩散和破坏手段非常隐蔽，现有的防病毒软件无法查杀。

2.3　长期的风险

现阶段我国关键信息基础设施大量采用国外的产品和技术，该现状在短时间内还无法改变。部分国外的设备在测试中发现了高危漏洞甚至人为后门，攻击者容易获取管理密码，从而取得全部权限。同时，随着自动化、智能化领域的发展，网络互联互通进一步增强，关键信息基础设施网络安全防控难度进一步增加。纵向认证和横向隔离装置是电力生产工业控制系统的最后一道防线，但通过多项国际案例来看，隔离和认证装置并不是绝对可靠的。由于设备老旧或安装维护不当、参数阈值设置不合理、程序存在逻辑漏洞和远程后门以及设备厂商自身管理缺陷等问题，网络攻击者可能会通过互联网渗透进入控制区；此外，U盘或移动便携机“摆渡”、同一台计算机双网卡、生产控制区使用无线网络等多个途径也会导致病毒间接入侵控制区，进而破坏核心生产控制系统。

3　要树立科学的网络安全观，有效应对网络安全风险

在当前竞争日益激烈的国际网络空间安全博弈中，要树立科学的网络安全观，有效应对关键信息基础设施所面临的安全风险。

3.1　网络安全风险的实质

从科学原理上看，网络安全风险的实质是人们对信息科学认知逻辑的局限性，由于不能穷尽所有逻辑组合，只能局限于完成计算任务去设计信息系统，必定存在逻辑不全的缺陷，从而形成了难以应对人为利用缺陷进行攻击的网络安全问题，这也是永恒的主题。

网络空间安全的极度脆弱性主要源于3个方面：1) 计算科学问题。图灵计算模型解决了一阶逻辑不自洽性和不完备性等问题，缺乏对不正确的逻辑输入进行安全校验和纠正的攻防理念；2) 体系结构问题。冯·诺依曼架构将计算机分为运算器、控制器、存储器、输入设备和输出设备，缺乏对与计算部件同等重要的防护部件的设计；3) 应用模式问题。在重大工程项目中，普遍缺乏针对性的网络安全服务，若出现

安全问题难以在早期发现和消除影响。这导致了信息系统从“出生”就没有应对网络攻击、抵抗病毒的“免疫能力”，也缺乏外界的“安全赋能”。

网络空间安全的极度脆弱性从表象来看主要源于 3 个方面：1) 技术问题。信息资产和系统是静态、已知的，攻击方研发的漏洞和武器是动态、未知的，静态防御难以应对动态攻击。2) 管理问题。随着网络安全产业的兴起，大量通用设备和系统 0DAY 漏洞的频发，导致网络安全最终取决于底层设备、系统和供应链，补丁的准确性、有效性和及时性都不能满足安全需求，通过已知补丁无法抵御未知威胁。3) 攻守不平衡问题。网络进攻是“攻”一个点，防守是“守”一个面，行业内分析研判网络安全攻防效费比达 1:400。网络安全工作逐步转换为与 0DAY 漏洞的博弈，但日常网络安全受限于技术也难以通过 0DAY 漏洞来检查工作，导致攻击预警的确定性太低，从确定攻击到处置攻击的时间过长。

3.2　应对网络安全风险的关键在于安全目标的收敛

在上述形势下，建设“刀枪不入”的网络防御体系是不可能的；从经济效益上看，建设这种网络防御体系也不一定划算。随着信息化事业的发展，网络安全风险普遍存在于产生、存储、传播信息和数据的计算工具上，体现在网络与信息系统的物理安全、运行安全、信息安全和系统安全上。杀病毒、防火墙和入侵检测等传统“老三样”以相对已知、静态的特征匹配检测技术为基础，已经难以应对高频变化、动态生成和无孔不入的网络安全问题，采用 0DAY 漏洞和网络武器的网络攻击，容易被攻击者反向利用[1]。因此，传统的“封、堵、查、杀”手段已经过时，找漏洞、打补丁的传统思路不利于网络整体安全，也不利于计算环境的稳定，在对稳定性、可靠性、实时性要求极高的工业控制、物联网等领域中的适用性明显不足。从应用侧角度看待网络安全问题，会导致安全目标的发散、安全资源的浪费以及安全效果的弱化。

为了防御网络攻击，网络安全的解决方案必须收敛，安全目标也必须收敛，重点是确保完成计算任务的逻辑组合不被篡改和破坏，以实现正确计算的目标。围绕这个安全目标，从逻辑正确验证理论、计算体系结构和计算工程应用模式等方面进行科学技术创新，解决逻辑缺陷不被攻击者利用的问题，形成攻防矛盾的统一体，为信息系统建立主动免疫能力。现阶段从计算体系结构的优化入手，通过创造主动免疫的可信计算架构和主动免疫的计算模式，从而改变传统的只讲计算效率、不注重安全防护的片面计算模式[2]。

3.3　主动免疫可信计算体系架构

可信计算是指计算的同时进行安全防护，计算全程可测可控、不被干扰，使计算结果总是与预期结果一样。可信计算采用了安全可信策略管控下的运算和防护并存的、主动免疫的新计算节点体系结构，以密码为基础实施身份识别、状态度量、保密存储等功能，及时识别“自己”和“非己”成分，从而破坏与排斥进入机体的有害物质，为网络信息系统培育了免疫能力。可信计算体系架构的特征是：以自主密码为基础、控制芯片为支柱、双融主板为平台、可信软件为核心、可信连接为纽带、策略管控成体系、安全可信保应用。

可信计算的发展经历了 3 个阶段。最初的可信 1.0 来自计算机的可靠性，主要以故障排除和冗余备份为手段，是基于容错方法的安全防护措施。可信 2.0 以可信计算组织（TCG，trusted computing group）出台的 TPM1.0 为标志，主要以硬件芯片作为信任根，以可信度量、可信存储和可信报告等为手段，实现计算机的单机保护。目前，我国的可信计算技术已经发展到了 3.0 阶段，建立了主动防御体系，确保全程可测可控、不被干扰，即防御与运算并行的主动免疫计算模式。

主动免疫计算模式通过平台密码方案创新，提出可信计算密码模块（TCM，trusted cryptography module），采用 SM 系列国产密码算法，并自主设计了双数字证书认证结构；可信平台控制模块（TPCM，trusted platform control module）作为自主可控的可信节点植入可信根，先于中央处理器（CPU）启动并对基本输入输出系统（BIOS，basic input output system）进行验证；将可信度量节点内置于可信平台主板中，构成了宿主机 CPU 加可信平台控制模块的双节点，实现在“加电第一时刻”开始建立信任链；可信基础支撑软件框架采用宿主软件系统加可信软件基的双系统体系结构；提出基于三层三元对等的可信连接框架，提高了网络连接的整体可信性、安全性和可管理性[3]。

4　以可信计算自主免疫体系为核心，推进面向未来的网络安全能力建设

为了解决网络空间安全问题，《国家网络空间

安全战略》中强调要加快对安全可信产品的推广应用，《网络安全法》第 16 条强调要推广安全可信的网络产品和服务，国家等级保护制度 2.0 标准要求全面使用安全可信的产品和服务来保障关键基础设施安全。在下一阶段的网络安全建设中，要围绕国家战略、法律、制度的总体部署，争分夺秒地开展面向未来的网络安全能力建设。

4.1　建设“带菌共存”的主动免疫能力

以云、物、大、智、移为代表的新技术深刻地改变了业务环境，关键信息基础设施正在快速向数字化、智能化、智慧化方向演进。通过网络方式提供服务逐步成为关键信息基础设施的主要应用场景，由此带来的网络安全威胁也呈现多样化和未知性趋势。由于外来安全设备形成的“无菌”环境和“真空”环境代价高昂且无法实现，因此，在计算机体系结构中实现主动免疫，使漏洞和缺陷无法被轻易利用，建设“带菌共存”的关键信息基础设施主动免疫能力成为切实可行的解决方案。通过可信计算环境、可信边界、可信通信网络组成可信环境 3 重防护，达到“攻击者进不去、非授权者重要信息拿不到、窃取保密信息看不懂、系统和数据篡改不了、系统工作瘫不成、攻击行为赖不掉”的防护效果。

4.2　建设面对未知风险的威胁发现能力

基于“零信任”原则建立数据驱动下的动态、可信的关键信息基础设施技术体系，将安全基线融合到系统建设的全生命周期中，并在各个环节进行安全审计，及时进行安全加固、策略配置优化和改进，切实加强系统的自身防护能力，提升安全措施的效能，减少安全隐患，降低可能被外部攻击者利用的风险，确保系统“不带病”运行。以此为基础，对国家关键基础设施进行全景网络绘图，摸清关键信息基础设施的网络拓扑、联网情况、关键系统、设备型号和存在的漏洞等。构建多维度的态势要素数据、云端数据和威胁情报，实现边界安全、终端安全、系统防护、应用安全和数据安全的完整态势感知，并利用安全数据结合相应的病毒库、漏洞库、案例库、知识库以及情报共享，建立监测模型，实现态势的全面、及时和有效感知。

4.3　建设适应组合攻击的安全防护能力

面对渐变的业务生态和突变的技术生态，我国关键信息基础设施还不具备应对多样性和未知性网络安全威胁的能力，运营单位对网络安全的全局洞察力和局部管控能力有待进一步加强。习近平总书记指出：“网络安全是动态的而不是静态的，需要树立主动防御、动态综合的防护理念。”贯彻落实习近平总书记网络强国战略思想，就需要变革传统的网络安全防护理论，积极适应网络安全的动态特点，基于主动防御思想，坚持正确的技术路线，从关键信息基础设施保护实际出发，逐步建立适应组合攻击的安全防护能力。

参考文献：

[1] 沈昌祥. 可信计算构筑主动防御的安全体系[J]. 信息安全与通信保密, 2016(6): 34.
SHEN C X. Trusted computing constructs a security system for active defense[J]. Information Security and Communications Privacy, 2016(6): 34.

[2] 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]. Science China (Informations), 2010, 40(2): 139-166.

[3] 沈昌祥. 用可信计算构筑网络安全[J]. 中国信息化, 2015(11): 33-34.
SHEN C X. Constructing network security with trusted computing[J]. Zhongguo Xinxihua, 2015(11): 33-34.

[作者简介]

李旸照（1986− ），男，湖北黄冈人，博士，中国长江三峡集团有限公司高级工程师，主要研究方向为网络安全和工业控制。

沈昌祥（1940− ），男，浙江奉化人，中国工程院院士，国家集成电路产业发展咨询委员会委员、国家信息化专家咨询委员会委员、国家三网融合专家组成员，主要研究方向为网络安全和密码工程。

田楠（1988− ），男，湖北宜昌人，中国人民解放军 91977 部队工程师，主要研究方向为网络安全和密码工程。