

· 院士讲坛 ·

按照《关键信息基础设施安全保护条例》 筑牢网络空间安全底线

沈昌祥

1 加强关键信息基础设施的安全建设, 意义重大而任务艰巨

当前, 网络空间已经成为继陆、海、空、天之后的第五大主权领域空间。网络安全是国际战略在军事领域的演进, 这对我国网络安全提出了严峻的挑战。习近平总书记指示: “没有网络安全就没有国家安全” “安全是发展的前提”, 并在“4·19”讲话中明确要求: “加快构建关键信息基础设施安全保障体系”。关键信息基础设施是国家安全、国计民生和公共利益的核心支撑。《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》明确强调, 要建立健全关键信息基础设施安全保障体系, 提升网络安全保障和维护国家主权能力。2021年7月30日国务院第745号令《关键信息基础设施安全保护条例》的发布, 对加快构建网络空间保障体系具有里程碑战略意义。

加快构建关键信息基础设施保障体系的关键在于自主创新, 在于深入研究网络安全的基础原理及其实质, 突破体系结构关键核心技术, 用安全可信的网络产品和服务构建系统工程, 其中最重要的是要有独创的安全可信网络产品。《中华人民共和国网络安全法》第十六条规定“国务院和省、自治区、直辖市人民政府应当统筹规划, 加大投入, 扶持重点网络安全技术产业和项目, 支持网络安全技术的研究开发和应用, 推广安全可信的网络产品和服务, 保护网络知识产权, 支持企业、研究机构和高等学校等参与国家网络安全技术创新项目”。《国家网络空间安全战略》提出“夯实网络安全基础”的战略任务, 强调“尽快在核心技术上取得突破”“加快安全可信的产品推广应用”。这次发布的《关键信息基础设施安全保护条例》第十九条明确要求“运营者应当优先采购安全可信的网络产品和服务”。

我国于20世纪90年代就开始研究基于免疫技术的综合安全防护体系, 使得信息网络系统如人体一样具有免疫力, 能主动识别、破坏、排斥进入机体的有害物质。创新发展基于主动免疫技术的可信计算技术体系, 推动其产业化, 完善网络安全等级保护制度, 为我国建设成为“技术先进、设备领先、攻防兼备”的网络强国的重大战略任务而努力奋进。

经过20多年可信计算技术与网络安全等级保护制度的创新性发展, 我国在构建主动防御网络安全保障体系, 确保关键信息基础设施安全运营等方面取得了重大经济和社会效益。面临霸权国家的网络核武器威胁, 我国全面进入数字化转型、网络化升级, 必须以科学网络安全观在核心技术突破和系统工程建设上跨越发展, 以等级保护2.0与可信计算3.0构建主动防御保障体系, 筑牢我国的网络安全防线。这项任务十分艰巨, 它涉及到网络空间自然科学和社会科学综合交叉的复杂系统, 所谓的安全范式或安全架构不能解决问题, 因此, 自主创新任重道远。

[收稿日期] 2021-08-30

[作者简介] 沈昌祥(1940—), 男, 中国工程院院士, 集美大学双聘院士, 从事密码工程、信息安全体系结构、网络安全等方面的研究。

2 敢于自主创新, 树立安全可信科学网络安全观

2.1 认清网络安全本质, 主动化解安全风险

要认清网络安全基础原理与实质, 网络安全的主要根源在于系统本身存在的脆弱性和人为攻击的威胁。基于图灵机的计算设备是工具, 当初设计时, 因不存在人为破坏情况, 无需防止别人恶意攻击, 系统构建无需安全性考量, 因此其选用的模型在原理上很少涉及攻防理念; 同时, 冯·诺依曼体系结构也缺乏防护部件, 而造成当前的计算系统极大的脆弱性。而现在人们意识到, 由计算设备构成的信息基础设施关系到资产财富、国家主权, 黑客用病毒获取金钱, 敌对势力以 APT 实施暴恐, 霸权国家发动网络战侵占他国主权, 这些都对网络空间安全构成重大的威胁, 暴露出网络空间在强大威胁下自身极其脆弱的重大安全风险。再者, 从科学原理上来说, 这种重大安全风险的本质在于人们对 IT 认知逻辑的局限, 在设计信息系统时不能穷尽所有的逻辑组合, 只局限于处理与完成计算任务有关的逻辑组合, 而造成大量未处理的逻辑缺陷隐患, 进一步形成了难以应对他人利用逻辑缺陷进行攻击的风险, 使网络安全成为永远的命题。为了有效防御威胁方的攻击, 减少脆弱性, 降低风险度, 必须从逻辑正确验证理论、计算体系结构和系统工程构建等方面进行科学技术创新, 以解决逻辑缺陷被攻击者利用的问题。只有通过构建主动应对攻击的防御体系, 使威胁者攻而无效, 确保完成计算任务的逻辑组合不被篡改和破坏, 才能实现正确计算的目标。这就是基于主动免疫技术的安全可信防御体系, 相当于为网络信息系统培育了免疫力。

2.2 离开“封堵查杀”, 建立主动免疫防护新理念

当前大部分网络安全系统主要由防火墙、入侵监测、病毒查杀和打补丁等模块和方式来组成, 这种“封堵查杀”的模式难以应对利用逻辑缺陷进行的攻击, 反而增加了自身的脆弱性。因为: 一, 它是根据已发生过的特征库内容进行比对查杀, 而层出不穷的新漏洞与攻击方法是防不胜防的; 二, 其功能部件属于超级用户, 违背了最小特权用户的安全原则, 也可以被攻击者控制, 成为网络攻击的平台。例如, “棱镜门”就是利用世界著名防火墙收取情报, 篡改病毒库后把正确程序当作病毒杀死, 从而导致系统瘫痪。最近, 美国东海岸输油管道控制系统被勒索病毒中断, 也是被动防护造成的, 结果迫使拜登总统宣布美国进入紧急状态。因此, 只有实施具有主动免疫能力的安全可信防御体系, 才能有效抵御已知和未知的各种攻击。

3 坚持自立自强, 构建主动免疫安全可信保障体系

3.1 建立主动免疫安全可信新计算模式

针对图灵机原理中缺少安全机理, 创新性地提出一种计算运算与安全防护同时进行的新计算模式, 即以密码为基因, 由此产生抗体, 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份, 从而破坏和排斥进入机体的有害物质。这与人体免疫类似, 自身能防御有害入侵, 确保机体逻辑缺陷不被恶意攻击者所利用。

主动免疫安全可信计算实现计算运算与安全防护并行操作, 计算全程可测可控, 不受干扰, 只有这样才能使计算结果总是与预期一样。这种新的计算模式改变了传统的只讲求计算效率, 而不讲安全防护的极其脆弱的计算模式。

3.2 构造“计算+防护”并行双重体系结构

冯·诺依曼体系结构由运算、控制、存储、输入输出等器件组成计算部件, 缺少防护部件; 因此, 传统的安全防护只是嵌入功能模块, 难以防御对计算部件的主动攻击。只有建立与计算部件并列的防护部件双体系结构, 以防护部件并行的动态方式, 对计算部件运算过程进行是否正确的核验, 才能发现异常及时处置, 达到主动免疫防护效果。

在图 1 所示的双体系结构中, 采用了一种安全可信策略管控下的运算和防护并列的主动免疫的新计算体系结构, 以可信密码模块 (TCM) 连接可信平台控制模块 (TPCM) 组成可信根, 由策略产生

可信检验规则，由可信软件基根据安全可信策略规则实施身份识别、状态度量、保密存储等功能，及时发现异常并加以处置，从根本上防止恶意代码对计算部件（主机）的攻击。这种以双重体系结构为核心的安全架构，使计算机像人体一样具有了免疫能力。

3.3 建设“一个中心 + 三层防护”保障体系框架

网络化基础设施、云计算、大数据、工业控制、物联网等新型信息化环境需要安全可信作为基础和发展的前提，必须进行可信度量、识别和控制。采用安全可信体系框架可以确保体系结构、资源配置、操作行为、数据存储和策略管理等可信，从而达到系统级主动防护的目的。

安全可信计算体系框架应从技术和管理两个方面进行设计。将信息系统安全防护体系划分为安全计算环境、安全区域边界、安全通信网络三层防护，以及由系统资源、安全策略、审计监控组成的管理中心，构成了安全可信管理中心支持下的主动免疫三重防护框架，如图 2 所示。基于该框架，制订了信息系统等级保护安全设计技术要求的国家标准（GB/T 25070—2010）。在国家重要信息系统建设中推广应用十余年，证明了该框架科学合理，取得了重大经济和社会效益。由此，成为网络安全法确定等级保护制度（等保 2.0）新标准的基本要求、测评要求和技术要求统一的标准框架，要求关键信息基础必须按照该框架做到可信、可控、可管。

3.4 执行四要素可信动态访问控制

人机交互可信是发挥 5G、数据中心等新基建动能作用的源头和前提，必须对人的操作访问策略四要素（主体、客体、操作、环境）进行动态可信度量、识别和控制。这样，才能纠正传统访问控制策略模型局限于授权标识属性进行操作。而不做可信验证，难防篡改的安全缺陷错误。另外，传统访问控制不考虑环境要素（代码及参数）是否被破坏，难以防止恶意代码攻击。为此，必须对环境要素在可信验证基础上依据策略规则进行动态访问控制（见图 3）。

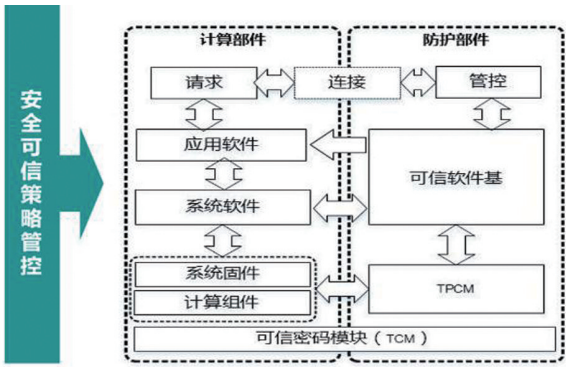


图 1 安全可信的双体系结构

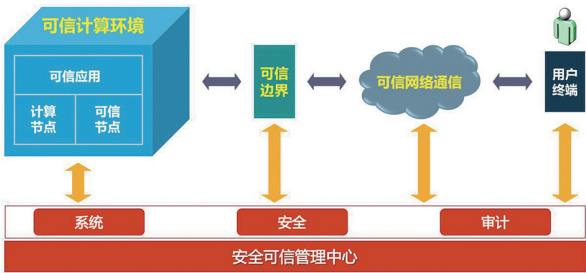


图 2 安全可信管理中心支持下的主动免疫三重防护框架

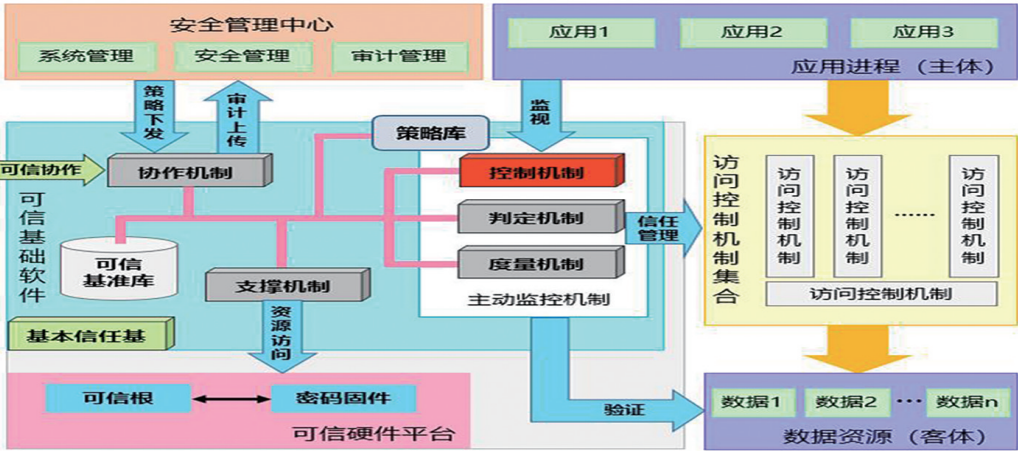


图 3 四要素可信动态访问控制流程图

3.5 加强“五环节”全程“技”“管”融合管控

按照网络安全法、密码法、等级保护制度、关键信息基础设施保护制度的要求，按照风险分析定级、备案建设、测评整改、监督检查和感知反制等五个环节进行保护、保障和保卫（见图 4）。

3.6 取得“六不”防护效果

按照新计算模式、双体系结构、三层防护框架、四要素访问控制和五环节全程管控，能达到“六个不”的防护效果，即攻击者进不去、非授权者重要信息拿不到、窃取保密信息看不懂、系统和信息改不了、系统工作瘫不成和攻击行为赖不掉（见图 5）。“WannaCry”“Mirai”“黑暗力量”“震网”“火焰”“心脏滴血”等计算机木马或病毒将不查杀而自灭。

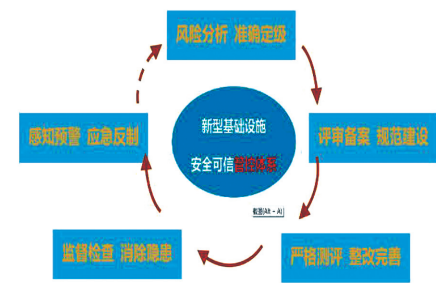


图 4 五环节全程管控



图 5 “六不”防护效果

以主动免疫防治“WannaCry”勒索病毒为例。2017 年 5 月 12 日“WannaCry”在全球范围大规模爆发。该病毒会释放敲诈程序 tasksche.exe，对磁盘文件进行加密导致系统锁死，同时开价要求对方付款后解锁，从而实施勒索。如果采用可信计算 3.0 技术建设的系统（如中央电视台的可信制播环境），以主动免疫防护体系功能机制，并行于主机的可信部件进行实时核验，阻止非授权和不符合预期结果的勒索病毒程序运行，就可以使勒索病毒攻而无效。

4 开创可信计算 3.0 新时代，筑牢网络空间安全防线

我国可信计算源于 1992 年正式立项研制成功的“主动免疫的综合防护系统”，经过长期攻关、军民融合，形成了自主创新的主动免疫可信体系（可信计算 3.0），其中不少技术已被国际可信计算组织（TCG）采纳。

4.1 创建主动免疫双结构体系框架

主动免疫是中国可信计算革命性创新的集中体现。我国自主创建了主动免疫双结构体系框架，如图 6 所示。在双结构体系框架下，采用自主创新的对称、非对称相结合的密码体制作为免疫基因；通过主动度量芯片组成控制模块（TPCM）植入可信根，在此基础上加以全程动态并行控制，实现了 TPCM 对计算平台的主动控制；在可信平台主板上嵌入了可信度量控制节点，实现了计算和可信双节点融合；软件由可信基础层实现宿主操作系统和可信控制软件基的双重软件系统，在不改变应用软件的前提下依据可信策略对执行点进行可信验证，达到主动防御效果；网络层采用三层三元对等的可信连接架构，在访问请求者、访问连接者和管控者（即策略仲裁者）之间进行三重控制和鉴别，解决了防止合谋攻击的难题，提高系统整体连接的可信性。

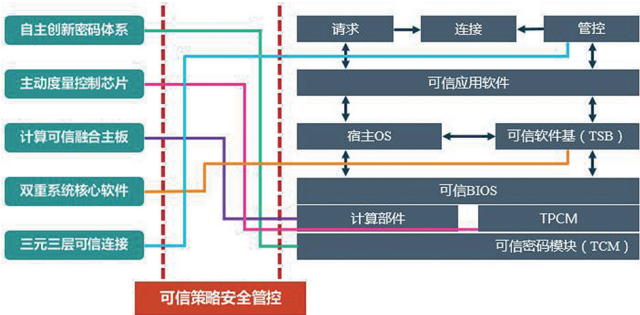


图 6 主动免疫双结构体系框架图

4.2 开创可信计算 3.0 新时代

主动免疫双结构体系框架开创了以系统免疫为特性的可信计算 3.0 新时代（如图 7 所示）。可信计算 1.0 以世界容错组织为代表，主要特征是通过容错算法、故障诊查实现计算机部件的冗余备份和故障切换，提高系统可靠性。可信计算 2.0 以 TCG 为代表，主要特征是 PC 节点安全性，通过主程序调用子程序以外部挂接的 TPM 模块实现静态串行度量。中国的可信计算 3.0 的主要特征是系统免疫性，其保护对象为以系统节点为中心的网络动态链，构成“宿主 + 可信”双节点可信免疫架构，在宿主机运算的同时由可信节点进行并行动态安全监控，实现对网络信息系统的主动免疫防护。可信计算 3.0 防御特性如表 1 所示。

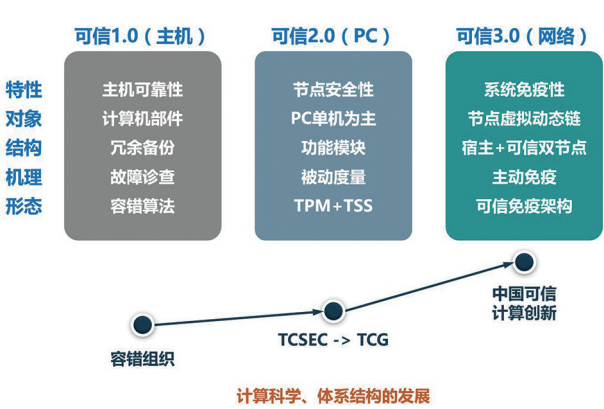


图 7 可信计算发展路径

表 1 可信计算 3.0 防御特性

分项	特性
理论基础	计算复杂性，可信验证
应用适应面	适用服务器、存储系统、终端、嵌入式系统
安全强度	强，可抵御未知病毒、未知漏洞的攻击、智能感知
保护目标	统一管理平台策略支撑下的数据信息处理可信和系统服务资源可信
技术手段	密码为基因、主动识别、主动度量、主动保密存储
防范位置	行为的源头，网络平台自动管理
成本	低，可在多核处理器内部实现可信节点
实施难度	易实施，既可适用于新系统建设也可进行旧系统改造
对业务的影响	不需要修改原应用，通过制定策略进行主动实时防护，业务性能影响 3% 以下

4.3 用可信计算 3.0 筑牢关键信息基础设施安全防线

《国家中长期科学和技术发展规划纲要（2006—2020 年）》明确提出：以发展高可信网络为重点，开发网络信息安全技术及相关产品，建立信息安全技术保障体系。“十二五”规划中有关重大工程项目都把可信计算列为发展重点。国家重要信息系统，如增值税防伪、彩票防伪、二代居民身份证安全系统都采用可信计算 3.0 作基础支撑。中国可信计算已经成为保卫国家网络空间主权的战略核心技术，已在国家核心系统和关键信息基础设施得到规模化成功应用。如中央电视台用可信计算 3.0 建成了可信、可控和可管的数字化制播环境，确保媒体的政治安全。由此可见，国家战略和法律要求推广安全可信的网络产品和服务是科学合理的。2020 年 10 月 28 日成立了国家等级保护 2.0 制度与可信计算 3.0 攻关示范基地，将大力推进关键信息基础设施安全保障体系的建设。

典型成功案例：可信计算 3.0 成功用于国家电网电力调度控制系统安全防护。2014 年国家发展和改革委员会令第 14 号明确以可信计算架构实现国电调度控制系统等级保护四级。目前电力调度控制可信平台已覆盖三十多个省级以上调度控制中心，涉及十几万个节点、约四万座变电站和一万座发电厂，有效抵御大量攻击，确保长期稳定供电。

最近，美国也大力推广零信任架构，从表象上来看，这种架构与安全可信属异曲同工之举。但是，所谓零信任的永不信任永远验证的概念、安全功能模块串行嵌入架构、动态访问控制核心技术等，其科学性、先进性、可行性等方面存在很多问题，必须进行科学的分析和验证，不能盲目跟风！

我们一定要抢占网络空间安全核心技术战略制高点，解决核心技术受制于人的问题，自主创新、自立自强，筑牢国家网络空间安全防线。