DOI 10.15302/J-SSCAE-2016.06.012

基于主动防御的网络安全基础设施可信技术保障体系

张大伟，沈昌祥，刘吉强，张飞飞，李论，程丽辰

（北京交通大学信息安全体系结构研究中心，北京 100044）

摘要：本文介绍了网络安全基础设施可信保障体系建设的现状、问题及未来构建策略。通过对现有安全保障体系建设现状和存在问题的剖析，提出我国网络安全基础设施亟须构建基于主动防御思想的可信技术保障体系。为此，提出可信技术保障体系建设策略建议，主要包括：以自主创新的主动防御计算体系结构作为构建可信技术保障体系的突破点；在落实信息安全系统国产化的战略合作中一定要真正形成实质的本土化；加大自主创新力度，推动主动防御的理论研究、产品研发和工程应用；积极推进可信计算标准的制定和推广应用工作，以推动可信技术保障体系的规范化发展，开展试点示范。

关键词：主动防御；主动免疫；可信计算；可信技术保障体系；网络安全基础设施

中图分类号：TP309　　**文献标识码：**A

TC Assurance Architecture for Cybersecurity Infrastructure Based on Active Defense

Zhang Dawei, Shen Changxiang, Liu Jiqiang, Zhang Feifei, Li Lun, Cheng Lichen

(Center of Information Security Architecture in Beijing Jiaotong University, Beijing 100044, China)

Abstract: This paper introduces the status, problems, and future strategies of the cyberspace security infrastructure system, and proposes that cyberspace security infrastructure must be based on active defense. Therefore, this paper proposes several suggestions for a trusted technology insurance system, which include the following: In order to build a trusted technology insurance system, independent innovation in active defense must be the breaking point; key information security systems must be developed by local institutions; independent innovation must be increased; research, product development, and active defense applications must be promoted; the development of trusted computing standards must be promoted; and experimental demonstrations must be carried out.

Key words: active defense; active immunity; trusted computing; trusted technology insurance system; cybersecurity infrastructure

一、前言

随着网络技术和“互联网 +”应用的迅猛发展，国民经济和社会发展越来越依赖于基础信息网络和重要信息系统 , 互联网已广泛运用于从政府、社会到个人，从政治、金融到军事的信息管理中，网络空间的安全问题不可避免地成为当今各国国家安全领域的新命题。无论是发达国家还是发展中国家，都在加速构建各自的网络安全防御体系以保护关键的网络空间基础设施。

20 世纪 90 年代中后期至 21 世纪初，美国信息安全战略成为国家安全战略的正式组成部分。1998

收稿日期：2016-10-12；**修回日期：**2016-10-18

作者简介：张大伟，北京交通大学，副教授，主要研究方向为信息安全；E-mail: dwzhang@bjtu.edu.cn

基金项目：中国工程院重大咨询项目“网络空间安全战略研究”(2015-ZD-10)

本刊网址：www.enginsci.cn

年，美国国家安全局制定了《信息保障技术框架》（Information Assurance Technical Framework），提出了“纵深防御战略”（Defense-in-Depth），采用一个多层次的、纵深的安全措施来保障用户信息及信息系统的安全。2005 年，美国总统信息技术（IT）咨询委员会的报告《网络空间安全：迫在眉睫的危机》指出网络空间安全建设耗资巨大却漏洞百出，短期修复不解决根本问题。2006 年 4 月美国信息安全研究委员会发布了《联邦网络空间安全及信息保障研究与发展计划》，改变了无穷无尽打补丁的被动封堵查杀策略。奥巴马总统上任后，又先后发布了《网络空间国际战略》《国家网络安全保护系统》《美国网络行动政策》《增强关键基础设施网络安全》和《提高关键基础设施的安全性和恢复力》等，进一步增强了网络空间的主动防御能力。欧盟在网络空间安全方面也制定了一系列的政策和标准。1992 年，欧盟制定了《信息安全框架决议》，此后陆续出台了《关于网络和信息安全领域通用方法和特殊行动的决议》《关于对信息系统攻击的委员会框架协议》《欧洲信息社会安全战略》等政策，有效地保证了欧盟的信息安全。

在我国，重要基础设施网络主要是指电信、广播电视、铁路、银行、海关、税务、民航、电力、证券、保险等国内重要行业所使用的网络信息系统。目前，这些重要基础设施网络的安全防护多依据信息系统等级保护国家标准，其中，《信息系统安全等级保护定级指南》(GB/T22240) 规定当前我国信息安全等级保护从低到高分为五级。《信息系统安全等级保护基本要求》(GB/T22239) 明确了网络安全的技术和管理要求，《信息系统等级保护安全设计要求》(GB/T25070) 明确了网络信息系统的安全设计要求，是构建我国网络安全防护体系技术框架的基础 [1~3]。但随着网络攻击手段的日益复杂化与网络攻击工具的日趋多样化，单纯的基于封堵查杀的被动防护手段已无法满足重要基础设施网络的安全需求 [4~6]。从更深层面来看，这实际上是由于我国网络安全防护体系在安全方案设计、安全产品联动、安全机制设计等方面存在方向性问题，导致我国网络安全防护技术体系存在先天缺陷，同时影响了我国网络安全产业生态环境的改善 [7,8]。

因此，构建主动防御的网络空间安全保障体系已成为世界各国的共识。在此背景下，研究基于新的理论方法和技术手段构建网络安全基础设施保障体系具有重要的现实意义。

二、主动免疫的可信计算技术

网络空间的安全防御与人类社会类似。在人类社会中，信任是人们合作、交流的基础。网络空间具有开放互联的特点，允许两个网络实体未经实际认证、审查就可以进行交互，这就为恶意攻击提供了便利。如果我们在缺乏信任的情况下贸然交互，会带来损失。为解决这一问题，我们需要找到一种方法，让用户可判断与自己交互的实体是否可信，这就是可信计算的基本思想。可以说，网络空间中的可信计算思想来源于人类社会的成功管理经验 [9]。

传统的防火墙、防病毒、入侵检测系统（IDS），都是基于被动防御的思想，不能主动防御、积极防御。必须从体系结构入手解决信息安全的基本问题，基于主动免疫的主动防御可信计算技术可有效提高系统整体的防护效果 [9]。可信计算是指计算的同时进行安全防护，使计算结果总是与预期一样，计算全程可测可控，不被干扰。可以说，可信计算就是一种运算和防护并存的主动免疫的新计算模式，具有身份识别、状态度量、保密存储等功能，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。可信计算通过在硬件上引入可信芯片，从结构上解决了个人计算机体系结构简化带来的脆弱性问题。基于硬件芯片从平台启动开始，到应用程序的执行，构建完整的信任链。一级认证一级，一级信任一级，未获得认证的程序不能执行，从而使信息系统实现自身免疫，构建高安全等级的信息系统 [10]。主动免疫的双体系结构如图 1 所示。

三、主动防御的可信技术保障体系

为解决我国重要信息系统面临的安全威胁，我们应当回归等级保护的技术思路，以访问关系为核心实现安全能力，通过主动防御保障安全强度，通过统一安全策略管理安全功能，通过纵深防御体系控制安全风险，构建网络安全防护技术框架。

我国网络安全防护技术框架设计的核心思想包括以下几方面。

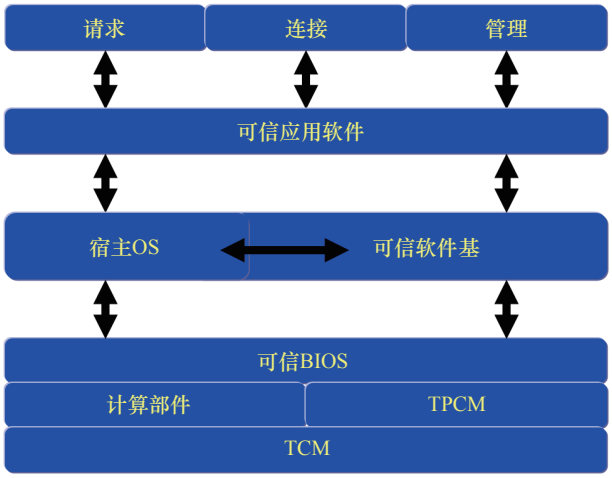

图 1　主动免疫双体系结构图

注：OS：操作系统；BIOS：基本输入输出系统；TPCM：可信平台控制模块；TCM：可信密码模块

1. 在安全机制层面，应围绕访问关系，实现实体可信、关系可控

在信息系统中，实体表现为代表用户执行操作的主体（如执行程序）以及作为信息容器的客体（如文件，设备，存储数据等），实体间关系则通过主体对客体的读写等访问行为来建立。理清信息系统中与业务流程相关的主体、客体和访问关系，通过可信度量和可信验证机制确保主体和客体的可信，通过访问控制机制确保访问关系可控，可以在确保业务流程正常运作的情况下排除异常操作，让信息系统免疫于已知和未知的安全威胁，是一种从根本上加强信息系统安全保护能力的方法。

2. 在安全保障层面，应基于主动免疫，实现安全机制的结构化保障

安全保障确保安全机制的可靠运行，它决定安全机制自身的强度，是我国等级保护四级以上安全系统的主要考核指标。在我国信息安全产业受制于人的现状下，通过主动免疫的可信计算技术支撑安全机制，实现安全机制的执行部件可信、安全配置可信、连接可信，以实现结构化的安全保障，是唯一现实可行的选择。

3. 在安全策略层面，应在统一管理下，实现安全机制间的策略联动

安全机制提供了对实体进行安全控制的能力，安全控制的具体过程还是通过部署在安全机制之上的安全策略来实现。各安全机制上的安全策略应统一服务于业务流程的安全需求，并根据安全需求和威胁的变化而变化。为了有效管理安全功能，各安全机制的策略不能孤立地部署，而应通过安全机制间的策略联动形成一个有机整体，并由安全管理员通过信息系统的安全管理中心统一进行管理，以主动的方式应对安全需求和安全威胁的变化。

4. 在安全体系层面，应基于业务流程，构建纵深防御体系。

当前以高级持续性威胁（APT）为代表的立体化、组合式的攻击手段，要求信息安全防护机制也应根据业务流程的特点，构建多层次、多位置的纵深防御体系作为对抗。纵深防御体系不是凭空产生，而是在对业务流程进行归类、流程分析和风险评估的基础上，划分系统安全区域，并对各安全区域的计算环境、区域边界和通信网络分别部署不同功能的安全机制而实现的。纵深防御体系能够集中资源重点保护核心区域，有效防止安全攻击的扩散，对重要信息系统安全风险的可控性有重大意义。

四、对策建议

以自主创新的主动防御可信计算体系结构作为构建可信网络空间安全技术保障体系的突破点，需要创新体制机制，协同国家安全和企业利益，创新技术研发和产业化资源组织模式，发挥产业联盟在标准制定、联合攻关和产业化应用推广方面的作用，积极推进试点、示范应用。

1. 推进创新体制机制，协同国家安全和企业利益，逐步形成产业发展的内生动力

国家出台政策为自主可控可信产品提供市场应用空间，使技术创新、性能提升与产业应用协同发展。例如，党、政、军和核心要害系统国产化替代工程全部由国家出资支持，在替代工程实施中预留出专用资金对所应用可信产品的集成适配和优化进行提升完善，弥补直接研发资金缺口。不断推动可信计算产品的产业链发展，积极优化产业生态环境，从而有效提高企业在可信技术保障产品研发方面的内生动力。

2. 实现开放互利共赢，信息安全系统国产化战略要实现实质本土化

在关键信息系统与国外企业的合作中，不能简单地用企业利益进行衡量，而是应从国家信息安全角度出发，开发自主的安全策略和架构，并据此实施严格的可信度量和检查，用主动免疫机制保障信息的真实

可控。实现关键安全技术的本土化落地，实现开放互利共赢，从技术、商业、法律上真实可行。

3. 加大自主创新力度，重大科研项目立项加入主动防御课题

主动防御的可信计算技术的重要性已经毋庸置疑，我国的可信计算技术在体系结构、运作模式和服务模式方面都有所创新，政府应加强对主动防御可信计算技术的支持力度，在国家重大、重点科技立项中对有自主知识产权的可信计算技术研究给予持续支持，以推动主动防御的理论研究、产品研发和工程应用。

4. 积极推进可信计算标准制定、推广，开展试点示范

目前，相关标准的缺乏已经严重制约了可信计算的创新发展和产业化，在国际谈判中失去了国际话语权，处于被动的局面。加快推进可信计算相关标准的制定和推广势在必行。同时应在重点行业开展试点示范应用，发现问题，总结经验，优化完善，逐步扩大规模，形成全产业链生态环境。同时，针对基础软件和重点产品，如桌面操作系统、嵌入式操作系统、云计算系统，积极推荐主动防御体系的示范应用，更好地完善可信技术保障体系，提高网络空间安全保障能力。

参考文献

[1] 张伟丽. 信息安全等级保护现状浅析[J]. 信息安全与技术, 2014, 9(1): 9–13.
Zhang W L. Discussion on the status of information security base on multi-level protection[J].Information Security and Technology, 2014,9(1): 9–13.

[2] 王大川, 王永书, 林红. 浅议计算机信息系统安全等级保护[J]. 中国公共安全: 学术版, 2009(3):4–10.
Wang D C, Wang Y S, Lin H. Analysis of computer information system multi-level protection[J]. China Public Security: Academic Edition, 2009(3): 4–10.

[3] 朱建平, 李明. 信息安全等级保护标准体系研究[J]. 信息技术与标准化, 2005(5): 21–24.
Zhu J P, Li M. The standard research of Information Security multi-level protection[J]. Information Technology & Standardization, 2005(5): 21–24.

[4] 罗玲. 浅析信息安全与等级保护技术[J]. 黑龙江科技信息, 2015(12): 35–40.
Luo L. Analysis of information security and multi-level protection technology[J]. Heilongjiang Technology Information, 2015(12): 35–40.

[5] 沈昌祥. 等级保护整改的技术路线[J]. 信息网络安全, 2008(11): 14–15.
Shen C X. The rectification routes of multi-level protection[J]. Information Network Security, 2008(11): 14–15.

[6] 沈昌祥, 左晓栋. 信息安全等级保护的焦点[J]. 信息安全与通信保密, 2004(4): 16–18.
Shen C X, Zuo X D. THE focus of information security multi-level protection[J]. Information Security and Communications Privacy, 2004(4): 16–18.

[7] 沈昌祥. 加快推进信息安全等级保护工作[J]. 信息网络安全, 2008(5): 4–7.
Shen C X. Accelerate the work of information security multi-level protection[J]. Information Network Security, 2008 (5): 4–7.

[8] 马力, 毕马宁, 任卫红. 安全保护模型与等级保护安全要求关系的研究[J]. 信息网络安全, 2011(6): 1–4.
Ma L, Bi M N, Ren W H. Analysis of relationship between security models and multi-level security protection requirements[J]. Information Network Security, 2011(6): 1–4.

[9] 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(2): 139–166.
Shen C X, Zhang H G, Wang H M. Research and development of trusted computing[J]. China Science: Information Technology, 2010(2): 139–166.

[10] 沈昌祥. 大力发展我国可信计算技术和产业[J]. 信息安全与通信保密, 2007(9): 19–21.
Shen C X. Developing the trusted computing technology and industry[J]. Information Security and Communications Privacy, 2007(9): 19–21.