DOI 10.15302/J-SSCAE-2016.06.011

可信 3.0 战略：可信计算的革命性演变

沈昌祥，张大伟，刘吉强，叶珩，邱硕
（北京交通大学信息安全体系结构研究中心，北京 100044）

摘要：本文介绍了传统防御体系建设的现状、问题及未来构建策略。通过对现有防御体系建设现状和存在问题的剖析，以及可信计算的演变历程，提出了用可信 3.0 构建主动防御体系的思想，进一步给出了可信 3.0 主动防御在云计算中的应用，并针对网络安全动态变化存在的问题给出了切实可行的主动防御实施建议。

关键词：可信 3.0；主动防御；主动免疫；等级保护；防护框架
中图分类号：TP309　　**文献标识码：**A

The Strategy of TC 3.0: A Revolutionary Evolution in Trusted Computing

Shen Changxiang, Zhang Dawei, Liu Jiqiang, Ye Heng, Qiu Shuo
(Center of Information Security Architecture in Beijing Jiaotong University, Beijing 100044, China)

Abstract: This paper introduces the status, problems, and future strategies of the traditional defense system and analyzes issues in the current protection structure. We then propose the trusted computing (TC) 3.0 strategy, which is an active defense architecture based on active immunity. Furthermore, we give an example of TC 3.0 in cloud computing and provide some suggestions on enforcing active defense.

Key words: trusted computing (TC) 3.0; active defense; active immunity; multi-level protection; protection structure

一、前言

近年来网络攻击手段不断变化和升级，我国的网络安全态势依然严峻。中国互联网信息中心发布的《中国互联网发展状况统计报告》指出，截至 2016 年 6 月，我国网民规模达 7.1 亿，互联网普及率达 51.7 %[1,2]。高速发展的互联网带给我们便利的同时，安全问题也很突出，国家互联网应急中心 (CNCERT) 2015 年共发现 1.05×10^5 多个木马和僵尸网络控制端；互联网恶意程序数量近 1.48×10^6 个，较 2014 年增长 55.3 %；分布式拒绝服务（DDoS）攻击的态势严峻，2015 年前三季度，1 Gbit/s 以上的 DDoS 攻击次数近 3.8×10^5 次，日均攻击次数 1 491 次。

随着云计算、大数据、物联网的发展，越来越多的信息系统部署到云上，尤其是关系国计民生与

收稿日期：2016-10-12；修回日期：2016-10-18
作者简介：沈昌祥，中国工程院，院士，北京交通大学，教授，主要研究方向为信息安全；E-mail: 13911888336@163.com
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

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

企业生存的基础设施和工业信息系统，倘若这些系统中的漏洞被发现后加以利用，后果将不堪设想。传统的封堵查杀的被动防御手段，已经凸显出在技术防护方面的不足[3-5]，构建主动防御体系势在必行。

二、传统防御体系建设中的问题

等级保护制度是我国网络安全防护体系的重要依据。等级保护工作自 1994 年实施以来，取得了较大的成就，发挥了重要的作用。但在目前的等级保护建设中仍存在一定的问题。

1. 安全管理人员对等级保护工作的重视程度还不够

安全管理人员认识还不到位，防范意识不足，管理不规范，工作方式简单，缺乏手段；在工作中，标准化的安全技术管理工具缺失，同时又由于攻击手段的多样性，即便建立良好的相应保障措施，仍旧会存在管理规范的漏洞，这些都影响信息安全等级保护制度的全面落实[6]。

2. 安全基础不可控，主动防御缺失

当前信息安全的主题是主动防御，等级保护更像是一种前置的保护手段，消极被动的防护措施始终是治标不治本，很难从源头上保障信息系统的安全[7]。

3. 技术标准不能与时俱进

伴随着云计算、物联网、大数据等的发展，新兴技术产业所提供的便捷服务越来越多地受到企业与用户的青睐，巨大的市场潜力下面带来的便是可怕的安全问题，等级保护政策标准的滞后，已经无法满足新型信息系统的安全需求[8]。

三、可信 3.0 构建主动免疫防御体系

可信计算的发展经历了几个阶段。最初的可信 1.0 来自计算机可靠性，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) 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、可信报告等为手段，实现计算机的单机保护。不足之处在于：未从计算机体系结构层面考虑安全问题，很难实现主动防御。我国的可信计算技术已经发展到了 3.0 阶段的“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”[9]。

可信 3.0 已经形成了自主创新的体系，并在很多领域开展了规模应用。我国经过长期攻关，取得了巨大的创新成果，包括：平台密码方案创新，提出了可信计算密码模块（TCM），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；提出了可信平台控制模块（TPCM），TPCM 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）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，实现信任链在“加电第一时刻”开始建立；提出可信基础支撑软件框架，采用宿主软件系统 + 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。创新点可概括为：“自主密码为基础，可控芯片为支柱，双融主板为平台，可信软件为核心，对等网络为纽带，生态应用成体系”。

同时经过多年技术攻关和应用示范，可信 3.0 已具备了产业化条件。可信 3.0 标准体系逐步完备，相关标准的研制单位达 40 多家，覆盖芯片、整机、软件和网络连接等整个产业链，授权专利达 40 多项，标准的创新点都作了技术验证，有力支撑了产业化。在 2014 年成立了中关村可信计算产业联盟，推动可信 3.0 的产业化工作。联盟成员单位已有 180 多家，组成了 13 个专业委员会，涵盖了包括“产学研用”各界的可信计算产业链的各个环节，具有广泛的代表性。可信 3.0 在一些关键信息基础设施安全保障建设中成功应用。主动免疫的主动防御可信计算技术产品已成功应用于中央电视台可信直播环境和国家电网电力调度系统防护系统等，成功构筑了符合等级保护四级的防御体系。

四、可信 3.0 的主动防御策略在云计算模式中的应用

结合主动免疫的主动防御思想和等级保护的防御体系，我们提出了“以主动免疫的可信计算为基础、访问控制为核心，构建可信安全管理中心支持下的积极主动三重防护框架”的主动防御策略（见图 1）。

主动免疫的三重防护主动防御框架以主动免疫可信计算技术为核心，围绕安全管理中心形成由安

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

全计算环境、安全区域边界和安全通信网络组成的纵深积极防御体系，在防御体系的各层面建立保护机制、响应机制和审计机制之间的策略联动。

云计算提供了动态伸缩的虚拟化资源，通过网络为用户提供多种服务，云计算面临的安全风险是由其自身的技术特点和服务模式引起并导致的。目前，可信计算主要在两个方面服务于云安全：一是为云中各节点的安全机制提供可信保障，防止安全机制被破坏、被篡改；二是为安全机制提供可信协同，将不同的安全机制集成起来，从整体上服务于云安全[10]。

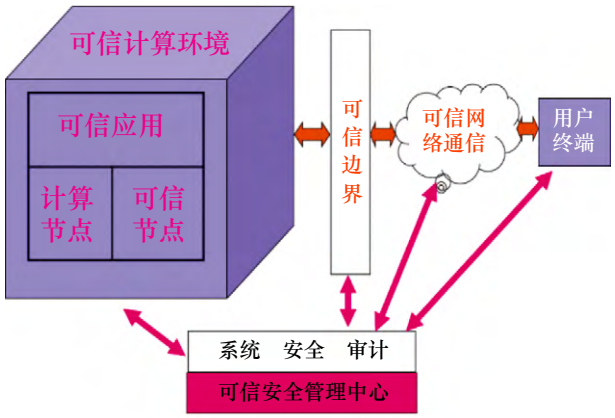

图 1 主动免疫的三重防护主动防御框架

可信云架构为云服务提供了系统的可信计算服务功能，提供了可信的安全保障机制，具体为：通过建立云架构下的可信链，为虚拟运行环境提供可信保障；通过建立基于可信第三方的监控技术，可以有效监控云服务的执行，解决云服务不可信问题；通过基于可信根支撑的隔离技术，可以在云环境建立起具有可信保障的多层隔离防线，为虚拟机提供安全可信的隔离环境；通过可信接入技术提供可信的云环境接入方法，解决开放云环境所带来的一系列安全问题[11]。

可信云架构是云环境安全管理中心、宿主机、虚拟机和云边界设备等不同节点上可信根、可信硬件和可信基础软件通过可信连接组成的一个分布式可信系统，支撑云环境的安全，并向云用户提供可信服务。一般而言，可信云架构需要与一个可信第三方相连，由可信第三方提供云服务商和云用户共同认可的可信服务，并由可信第三方执行对云环境的可信监管。可信云计算体系安全框架如图 2 所示[12]。

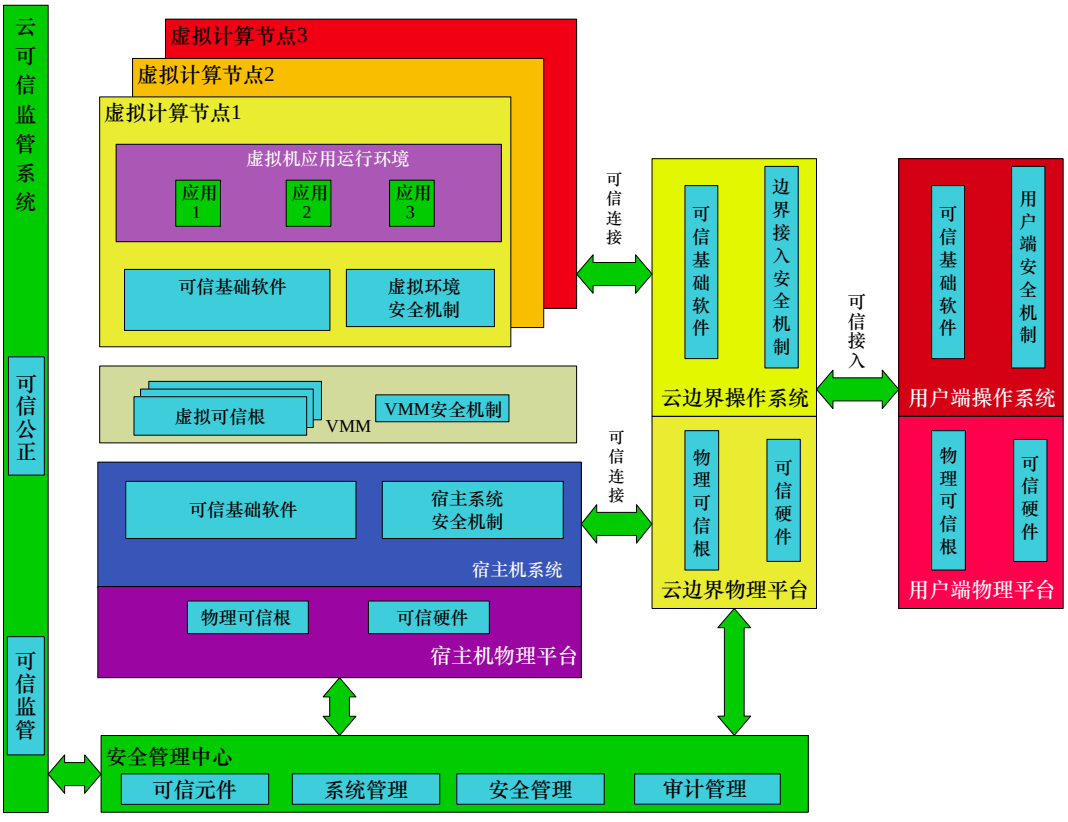

图 2 可信云计算体系安全框架

注：VMM：虚拟机监视器

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

可信云架构中，各节点的安全机制和可信功能不同，因此可信基础软件所执行的可信功能也有所区别。这些可信功能互相配合，为云环境提供整体的可信支撑功能。架构中的各安全组件功能如下。

1. 安全管理中心

安全管理中心上运行着云安全管理应用，包括系统管理、安全管理和审计管理等机制。安全管理中心上的可信基础软件是可信云架构的管理中心，它可以监控安全管理行为，并与各宿主机节点上的可信基础软件相连接，从体系上实现安全。

2. 云边界设备

云环境的边界设备运行边界接入安全机制。可信基础软件与边界安全接入机制耦合，提供可信鉴别、可信验证等服务，保障边界安全接入机制的可信性。

3. 宿主机

宿主机可信基础软件的可信支撑机制需保障宿主机安全机制和虚拟机管理器安全机制的安全，同时还要为虚拟机提供虚拟可信根服务。而宿主机安全机制的主动监控机制则相当于云环境的一个可信服务器，它接收云安全管理中心的可信管理策略，将云安全管理中心发来的策略本地化，依据可信策略向虚拟环境提供可信服务。

4. 虚拟机

虚拟机上的可信基础软件为自身的可信安全机制提供支持，同时对虚拟机上的云应用运行环境进行主动监控。虚拟机、宿主机和安全管理中心的可信基础软件，实际构成了一个终端－代理服务器－管理中心的三元分布式可信云架构。

5. 可信第三方

可信第三方是云服务商和云用户都认可的第三方，如政府的云计算监管部门，测评认证中心等。可信第三方向云架构提供可信公正服务和可信监管功能。

6. 用户可信终端

云用户终端上也可以安装可信基础软件和构造可信计算基。安装可信基础软件并构造了可信计算基的用户终端即为用户可信终端。

五、对策建议

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，基于等级保护的主动防御思想，构筑以主动免疫为特征的主动防御体系。

1. 实现被动防护与主动防御的过渡，将主动免疫融入等级保护

当今信息安全的主要特征是要建立主动防御体系，而等级保护作为我国目前主要的前置保护手段，消极被动防御治标不治本，不符合主动防御的思想。可信计算 3.0 能够实现计算机体系结构的主动免疫，及时识别“自己”和“非己”成分，漏洞缺陷不会被轻易利用。我们急需将传统的三重防护上升为可信计算环境、可信边界、可信通信网络组成的可信环境下的三重防护，构建主动免疫的主动防御体系。

2. 建立健全网络安全技术支撑体系，完善可信主动防御新标准的制定

现行网络安全防护政策标准的滞后，难以满足新型信息化系统的安全需求。物联网、云计算、移动互联网呈现出新特点和新需求，更多的行业应用接入到互联网；云计算呈现出边界消失、服务分散、数据迁移的特点；移动互联、智能终端的普及在用户终端层面带来新的安全威胁，这些都对信息安全防御提出了新的挑战。

建立健全云计算、大数据、物联网、工业系统等新型信息系统的主动免疫、主动防御的标准和等级保护技术标准，完善实施定级、测评、管理全过程的技术支持，以达到攻击者进不去、非授权者重要信息拿不到、窃取保密信息看不懂、系统和信息篡改不了、系统工作瘫不成和攻击行为赖不掉的防护效果，从而达到‘主动防御方能有效防护’的效果。

3. 从国情出发，按需适度、安全，逐步发展完善主动防御体系

在由被动防御向可信主动防御的转变过程中，不能操之过急，要坚持正确的技术路线，从国情出发，按需适度、安全地打好基础，逐步发展完善。

参考文献

[1] 沈昌祥. 构建积极防御综合防范的防护体系[J]. 电力信息与通信技术, 2004, 2(5):1-3.
Shen C X. Construction of the active defense and comprehensive prevention protection system [J]. Information Security and Communications Privacy, 2004, 2(5):1-3.

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

[2] 中国互联网络信息中心. 第38次中国互联网络发展状况统计报告 [EB/OL]. (2016-08-03)[2016-10-08]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201608/t20160803_54392.htm.
China Internet Network Information Center. The 38th statistical report on internet development in China [EB/OL]. (2016-08-03) [2016-10-08]. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/201608/t20160803_54392.htm.

[3] 沈昌祥. 云计算安全与等级保护[J]. 信息安全与通信保密, 2012(1): 12-14.
Shen C X. Cloud computing security and hierarchical protection [J]. Information Security and Communications Privacy, 2012(1): 12-14.

[4] 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. Building a defense security system with trusted computing [J]. Information Security and Communications Privacy, 2016(6): 34.

[5] 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]. Scientia Sinica Informationis, 2010, 40 (2): 139-166.

[6] 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): 9-13.
Zhang W L. Discussion the status of information security base on graded protection [J]. Information Security and Technology, 2014 (9): 9-13.

[7] 宋言伟, 马钦德, 张健. 信息安全等级保护政策和标准体系综述[J]. 信息通信技术. 2010, 4(6): 58-63.
Song Y W, Ma Q D, Zhang J. Information security level protection policies and standard system [J]. Information and Communications Technologies, 2010, 4(6): 58-63.

[8] 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 hierarchical protection [J]. Netinfo Security, 2008 (11): 14-15.

[9] 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.

[10] 沈昌祥. 云计算安全[J]. 信息安全与通信保密, 2010(12):12.
Shen C X. The Security of Cloud Computing [J]. Information Security and Communications Privacy, 2010 (12):12.

[11] 沈昌祥. 坚持自主创新加速发展可信计算[J]. 计算机安全, 2006(6): 2-4.
Shen C X. Independent innovation to accelerate the development of trusted computing [J]. Network and Computer Security, 2006(6):2-4.

[12] 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. Building a cyberspace security system with trusted computing [J]. China Information, 2015(11):33-34.

(C)1994-2019 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net