主动免疫可信计算综述

A Survey on Active Immune Trusted Computing

张建标/ZHANG Jianbiao[1,2]，黄浩翔/HUANG Haoxiang[1,2]，胡俊/HU Jun[1,2]
（1. 北京工业大学，中国 北京 100124；
2. 可信计算北京市重点实验室，中国 北京 100124）
(1. Beijing University of Technology, Beijing 100124, China;
2. Beijing Key Laboratory of Trusted Computing, Beijing 100124, China)

DOI：10.12142/ZTETJ.202206003
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.tn.20221209.1035.002.html
网络出版日期：2022-12-10
收稿日期：2022-10-25

摘要：对主动免疫可信计算的基本思想及特征进行了重点阐述，并从标准体系、解决方案及产业发展3个方面对主动免疫可信计算进行详细介绍。认为随着等级保护2.0标准的实施，主动免疫可信计算技术已在保障重要信息系统的安全可信中发挥了重要的作用。

关键词：可信计算；主动免疫；主动防御；双体系结构；网络安全

Abstract: The basic ideas and characteristics of active immune trusted computing are expounded, and active immune trusted computing is then introduced in detail from three aspects of the standard system, solution, and industrial development. It is believed that with the implementation of level protection 2.0 standard, the active immune trusted computing technology has played an important role in ensuring the security and credibility of important information systems.

Keywords: trusted computing; active immune; active defense; dual system structure; cyber security

网络空间已成为继陆、海、空、天之后的第五大主权领域空间，没有网络安全就没有国家安全。提供安全可信的网络产品和服务是国家法律（《中华人民共和国网络安全法》[1]）、战略（网络空间安全战略[2]）和等级保护制度的要求。为配合网络安全法的实施，新修订的网络安全等级保护（简称等级保护2.0）标准[3]，突出了主动免疫可信计算支撑的一个中心三重防护的安全框架，通过可信验证确保各个环节的安全可信，保障国家重要信息系统的安全。

1 主动免疫可信计算介绍

1.1 基本思想

信息安全问题由图灵计算模型缺少攻防理念、冯·诺依曼架构缺少防护部件、工程应用无安全管控服务三大原始缺陷而引起[4]。传统的计算机体系结构专注于计算功能的实现，缺乏对安全防护的考虑。这就相当于一个人没有免疫系统，只能生活在无菌状态下。此外，人类对事物的认知存在局限性，而系统设计过程中所具有的逻辑组合无法穷尽，必然会存在逻辑不全的缺陷，而当前大部分网络安全系统主要是由防火墙、入侵监测和病毒防范等“老三样”组成，消极被动的封堵查杀不仅难以应对利用逻辑缺陷的攻击，且只能被动抵御已知病毒[5]。

相较于“老三样”，主动免疫可信计算能够实现计算机体系结构的主动免疫，其基本思想为：在计算机系统中建立一个可信根，可信根的可信性由物理安全、技术安全、管理安全共同确保；再建立一条可信链，从可信根开始到硬件平台、操作系统、应用，一级测量认证一级，一级信任一级，把这种信任扩展到整个计算机系统中，从而确保整个计算机系统的可信[6]。

主动免疫可信计算就是要为计算平台建立起免疫系统，是一种在运算的同时进行安全防护的新计算模式。该模式以密码为基因实施身份识别、状态度量、保密存储等功能，及时识别“自己”和“非己”成分，从而破坏并排斥进入机体的有害物质。这相当于为网络信息系统培育了免疫能力[7]。

1.2 主要特征

（1）新计算模式：计算同时进行安全防护

计算机最初的设计目标是为了解决复杂计算问题，因此其体系结构在设计时要解决的核心问题即是提高计算速度，但却忽略了安全问题，如系统任务难以隔离、内存无越界保护等。这直接导致网络化环境下的计算服务存在很多安全问

基金项目：北京市自然科学基金（M21039）

题，如源配置可被篡改、恶意程序被植入执行、利用缓冲区（栈）溢出攻击、非法接管系统管理员权限等[6]。主动免疫可信计算是一种运算时进行安全防护的新计算模式，该模式采用计算和防护并行的双体系结构，在计算的同时进行安全防护，使计算结果总是符合预期，计算全程可测可控，不被干扰。

（2）双体系结构：计算部件+防护部件

如图1所示，主动免疫可信计算采用计算部件和防护部件并行的双体系结构。其中，计算部件即为通用计算系统，防护部件则是负责实施主动免疫可信计算的部件。主动免疫可信计算保持通用计算系统功能流程不变的同时，通过逻辑独立的防护部件，能够主动实施对计算部件（计算组件、系统固件、系统软件、应用软件）的可信监控，从而实现对计算部件全生命周期的可信保障。

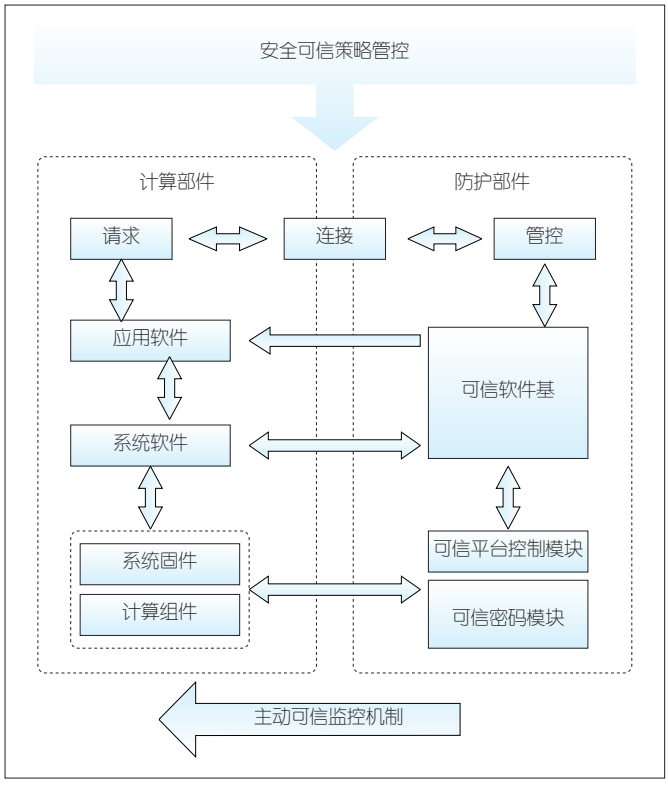
防护部件以并接于计算部件的可信平台控制模块（TPCM）作为可信根。TPCM在连接可信密码模块（TCM）的基础上增添对计算部件和外设的总线级控制功能，成为系统可信的源头。TPCM融合密码机制与控制机制，先于计算部件中央处理器（CPU）启动，主动对计算部件进行度量并实施控制。之后，可信软件基构建，对上承接可信管理机制，在安全策略规则的支配下实施主动监控；对下调度管理TPCM等可信硬件资源，协调完成主动度量及控制。

针对集中控管的网络环境安全需求，我们提出了三元三层对等可信网络连接架构，通过安全管理中心集中管理，对网络通信连接的双方资源实施可信度量和判决，有效防范内外合谋攻击。

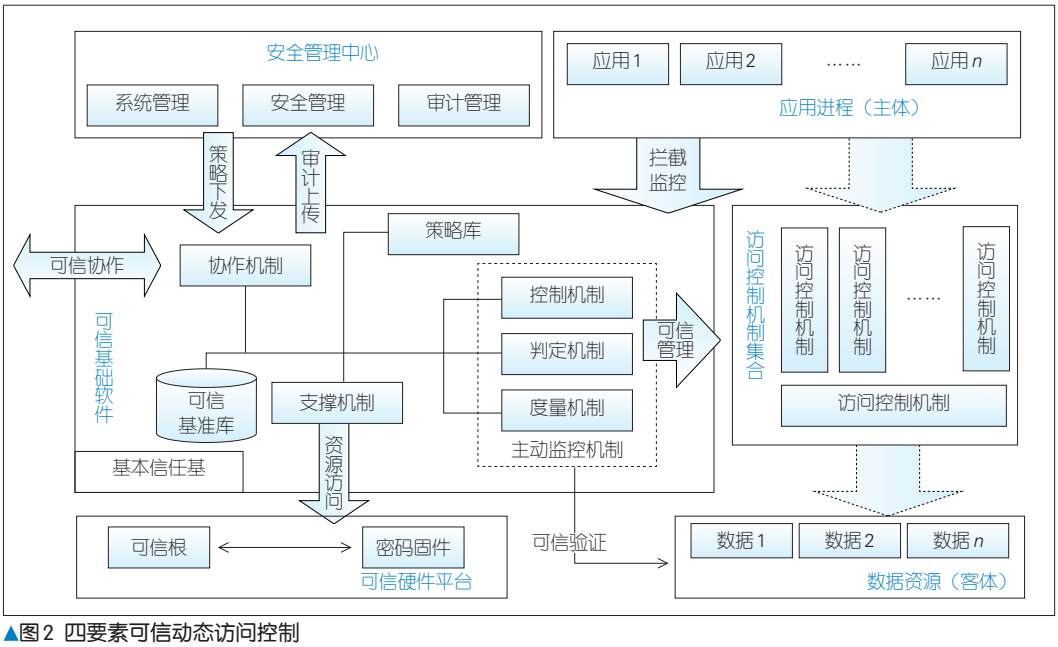
（3）四要素可信动态访问控制

传统访问控制机制是实现系统安全的有效措施，它基于主体、客体和操作三要素，控制主/客体的操作行为，保证系统访问的安全。但传统无计算环境要素的访问控制策略模型只基于授权标识属性进行操作，不作可信验证。这带来了难防篡改的安全缺陷，如恶意用户假冒合法实体进行资源访问、合法实体被篡改导致越权访问资源破坏、破坏被授权客体的完整性、计算环境的重要配置文件被篡改[8]等，访问控制过程的可信性无法保障。

因此，我们必须对访问控制过程中的“主体、客体、操作、环境”四要素进行动态可信度量、识别和控制，如图2所示。



▲图1 计算+防护的双体系结构



▲图2 四要素可信动态访问控制

（4）三重防护框架

一个中心三重防护，就是针对安全管理中心和安全计算环境、安全区域边界、安全通信网络的安全合规进行方案设计，建立以计算环境安全为基础，以区域边界安全、通信网络安全为保障，以安全管理中心为核心的信息安全整体保障体系。2019年12月实施的国家标准《信息安全技术 网络安全等级保护基本要求》（GB/T 22239—2019）更加强调了安全通信网络、安全区域边界和安全计算环境的可信验证要求，即实现以可信验证为支撑的一个中心三重防护，如图3所示。

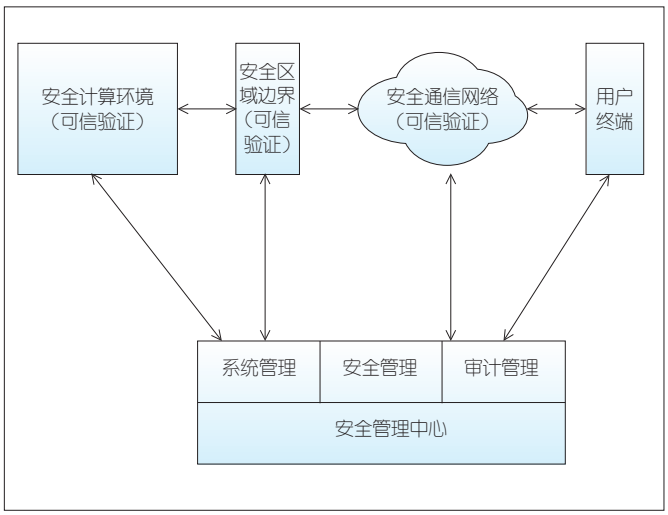
2 主动免疫可信计算研究进展

2.1 标准体系

2006年中国进入可信计算规范和标准的制定阶段，国家密码管理局制定了《可信计算平台密码技术方案》和《可信计算密码支撑平台功能与接口规范》。2007年在国家信息安全标准化委员会的主持下，北京工业大学可信计算实验室牵头，联合几十家单位，开始“可信平台控制模块”等4个主体标准和“可信计算体系结构”等4个配套标准的研究工作，构建了中国可信计算标准的体系框架，为后续制定一系列的可信计算国家标准奠定了基础。目前中国已经发布的可信计算相关标准如表1所示。

2.2 解决方案

TPCM作为构建主动免疫可信计算体系的信任锚点，具备主动控制和度量功能。当前，根据应用平台的不同，TPCM主要有3种构建形式：计算部件主板上增加TPCM；多核CPU的一个核作为TPCM；通过外部设备互连（PCI）插卡接入TPCM。



▲图3 可信验证支撑的一个中心三重防护

▼表1 可信计算国家标准

标准编号	名称
GB/T 29827—2013	信息安全技术 可信计算规范 可信平台主板功能接口
GB/T 29828—2013	信息安全技术 可信计算规范 可信连接架构
GB/T 29829—2022	信息安全技术 可信计算密码支撑平台功能与接口规范
GB/T 36639—2018	信息安全技术 可信计算规范 服务器可信支撑平台
GB/T 37935—2019	信息安全技术 可信计算规范 可信软件基
GB/T 38638—2020	信息安全技术 可信计算 可信计算体系结构
GB/T 40650—2021	信息安全技术 可信计算规范 可信平台控制模块

1）TPCM结构有两种主流的呈现方式。

（1）独立TPCM芯片：多用于以嵌入式系统为代表的计算资源有限的平台中，能够降低计算平台资源开销，且具备较高的物理可信性。文献[9]所述基于TPCM芯片的三阶三路可信平台主动防护架构方案表明，实验芯片通过直接存储器访问（DMA）协议或CPU共享总线交换数据，降低了系统开销，具备较高的安全性。

（2）基于基板管理控制器（BMC）构建TPCM：BMC具有独立处理器、内存和存储空间的服务器度量器件，能够实现对服务器硬件设备的主动监测和控制，成为构建“计算”与“防护”并行的主动免疫双体系结构的理想方案。北京工业大学可信计算重点实验室基于BMC构建服务器启动及运行过程，对“计算”和“防护”并行主动免疫架构进行了较为丰富的研究。随着TPCM相关的产、学、研、用多领域深度融合以及相应接口标准的完善，TPCM软硬生态建设及工程应用已趋于成熟。

2）随着多核CPU计算平台/服务器在实际中应用，基于其多核特性，构建计算核、安全核并行的主动免疫可信架构成为一种高效的解决思路。以海光、申威为代表的国产服务器生产商均研发了多核可信服务器，有效提高了国产服务器的安全性。在文献[10]中，安全防御机制由与普通处理器并行运行的安全处理器来充当，实现硬件级别的物理隔离，具备较高的安全性。但是由于物理隔离导致安全处理器对主机内存语义信息的获取较为困难，因此主动可信度量的结果较为粗粒度，且该方案只是对静态代码段进行周期性度量，度量有效性较低。文献[11]提出了一种改进的针对飞机硬件的攻击免疫超级监控可信架构。该架构基于轻量级精简指令集计算机（RISC）CPU来独立运行可信监控系统（TMS），实现TMS与主处理器系统（MPS）的安全隔离，使得对手很难

通过软件进行攻击。

3）外接可信插卡：通过外接可信插卡的方式实现防护部件，能实现对旧计算系统改造，降低了实现难度和工程成本。如华虹设计推出的高速串行计算机扩展总线标准（PCIE）可信加固卡提供了一组串行外设（SPI）Master接口，用于对计算平台主机基本输入输出系统（BIOS）进行主动度量，并可用来控制计算机主板上电时序的多组隔离输入/出开关控制系统，从而实现芯片层面的主动控制要求。文献[12]通过在异构计算网络加速卡上设置控制逻辑芯片、安全可信芯片及PCIE总线开关，构造了一种基于异构计算的安全可信卡。文献[13]提出了一种PCIE和MINIPCIE双接口的通用安全可信接口卡，能够通过TCM芯片与主板复杂可编程逻辑器件（CPLD）和CPU之间的信号传递及控制实现主动度量及端口主动控制功能。

TrustZone的快速发展为防护部件提供了隔离受保护的可信运行环境，同时防护部件为系统、应用提供丰富的可信度量、监控等功能，这种构建模式契合双系统体系架构的核心思想，成为构建主动免疫可信方案的一种改造思路[14]。文献[15]从控制流的角度提出了一种动态度量方案，该方案基于TrustZone构建内核飞地，从而确保监控度量模块无法被攻击者篡改或绕过，最终确保动态度量过程的可信性。文献[16]中的TrustZone架构实现了一种双系统体系架构下的主动度量机制，使得位于安全世界的防护部件能够主动对非安全世界的计算部件进行度量。

2.3 产业发展

2014年4月16日，由中国工程院沈昌祥院士提议，中国电子信息产业集团、北京工业大学、中国电力科学研究院等60家单位发起的中关村可信计算产业联盟正式成立。目前，该联盟成员包括国有企业、民营企业、上市公司、研究院所、大专院校等网络安全领域各种单位200多家，涉及中国可信计算产业链的各个环节，覆盖了产、学、研、用、测各界，有效推动了可信计算的产业化和市场化。2020年10月28日，国家网络安全等级保护制度2.0与可信计算3.0攻关示范基地在北京工业大学揭牌成立。目前，基于TPCM国家标准，主板并加可信SoC、多核CPU可信核及外接可信插卡3种产品形态已被研发并大量推广应用[4]。“白细胞”等可信软件基产品的发布标志着中国自主创新的基于可信技术的新一代网络安全技术路线实现产业化。

3 对比分析

1999年，IBM、HP、Intel和微软等著名IT企业发起并成立了可信计算平台联盟（TCPA），2003年TPCA改组为可信计算组织（TCG），这标志着可信计算开始向泛计算领域应用扩展。TCG可信计算技术是以可信赖平台模块（TPM）芯片来增强计算平台的安全性。这种可信计算技术防护部件的安全性依赖于计算部件，因此存在着被旁路或篡改的风险。此外，TCG采用被动调用的外挂式体系结构，这种结构不仅缺乏主动防御能力，且计算和防护串行执行，难以符合等级保护2.0标准中对重要信息系统实施主动、动态安全防护的要求。

主动免疫可信计算提出了“计算+防护”的双体系结构，防护部件逻辑独立于计算平台。该结构不仅有效防止源于通用计算系统的广泛攻击，而且有效提高了性能。TPCM作为可信根，能够先于主机计算部件上电启动，实现对计算平台的主动控制。无须修改应用软件，TPCM上运行的可信软件基接管系统软件的内核层系统调用，实现主动、动态防护。表2给出了可信计算技术对比分析。

4 结束语

提供安全可信的网络产品和服务是国家网络安全法律、国家网络空间安全战略和国家等级保护制度的要求。2021年9月施行的关键信息基础设施安全保护条例，强调运营者应当优先采购安全可信的网络产品和服务。随着等级保护2.0标准的实施，主动免疫可信计算技术已在保障重要信息系统的安全可信中发挥了重要的作用。但在面对云计算、移动互联、物联网和工业控制系统等应用场景，我们还需要深入进行主动免疫可信计算关键技术研究、相关标准制定、产品研制、适配测试和推广应用。

▼表2 可信计算技术对比

	技术机制	可信根	体系架构	技术手段	安全强度	对业务影响/性能
TCG可信计算	被动可信	TPM	串行	TPM串接于外总线，可信软件栈作为子程序库被动调用	能够实现对计算系统的串行静态检测保护	需要对应用、系统进行适配更改/低
主动免疫可信计算	主动免疫可信	TPCM	计算+防护并行双体系结构	密码为基因，主动识别、主动度量、主动保密存储	能够主动抵御未知病毒、漏洞，能够对重要信息系统动态防护	不修改应用，计算与防护并行进行/高

TCG：可信计算组织　TPCM：可信平台控制模块　TPM：可信平台模块

参考文献

[1] 中华人民共和国网络安全法 [N]. 人民公安报, 2016-11-08(3)
[2] 中国网信网. 国家网络空间安全战略(全文) [J]. 中国信息安全, 2017(1): 26-31
[3] 国家市场监督管理总局, 国家标准化管理委员会. 信息安全技术 网络安全等级保护基本要求: GB/T 22239—2019 [S]. 2019
[4] 沈昌祥, 田楠. 主动免疫可信计算打造安全可信网络产业生态体系 [J]. 信息通信技术与政策, 2022(8): 1-6. DOI: 10.12267/j.issn.2096-5931.2022.08.001
[5] 李刚. 创新驱动 构筑网络强国安全保障——沈昌祥院士谈技术可信计算的创新与发展 [J]. 中国信息安全, 2015(2):46-51
[6] 沈昌祥. 用可信计算构筑网络安全 [J]. 求是, 2015(20):33-34
[7] 沈昌祥. 用主动免疫可信计算3.0筑牢网络安全防线营造清朗的网络空间 [J]. 信息安全研究, 2018, 4(4): 282-302. DOI: 10.3969/j. issn. 2096-1057.2018.04.001
[8] VERC. 美国国家安全局(NSA)"酸狐狸"漏洞攻击武器平台技术分析报告 [EB/OL].[2022-10-22].https://www.cverc.org.cn/head/zhaiyao/news20220629-FoxAcid.htm
[9] 黄坚会, 沈昌祥, 谢文录. TPCM三阶三路安全可信平台防护架构 [J]. 武汉大学学报(理学版), 2018, 64(2): 109-114. DOI: 10.14188/j. 1671-8836.2018.02.002
[10] JIA X Q, HE Y, WU X Y, et al. Performing trusted computing actively using isolated security processor [C]//Proceedings of the 1st Workshop on Security-Oriented Designs of Computer Architectures and Processors. ACM, 2018: 2-7. DOI: 10.1145/3267494.3267498
[11] CHENG D X, ZHANG C, LIU J W, et al. An attack-immune trusted architecture for supervisory aircraft hardware [J]. Chinese journal of aeronautics, 2021, 34(11): 169-181. DOI: 10.1016/j.cja.2021.03.004
[12] 毕革新, 刘铁军, 张晶威, 等. 一种基于异构计算的安全可信卡及安全可信方法: CN111737698A [P]. 2020
[13] 邹武, 张鲁峰, 周魏. 一种PCIE和MINIPCIE双接口的通用安全可信接口卡: CN109739791A [P]. 2019-05-10
[14] 董攀, 丁滟, 江哲, 等. 基于TEE的主动可信TPM/TCM设计与实现 [J]. 软件学报, 2020, 31(5): 1392-1405. DOI: 10.13328/j.cnki.jos.005953
[15] 张英骏, 冯登国, 秦宇, 等. 基于Trustzone的强安全需求环境下可信代码执行方案 [J]. 计算机研究与发展, 2015, 52(10): 2224-2238. DOI: 10.7544/issn1000-1239.2015.20150582
[16] 尹超, 周霆, 黄凡帆. 一种基于TrustZone架构的主动可信度量机制设计 [J]. 信息通信, 2020, 33(9): 17-20

作 者 简 介

张建标，北京工业大学教授、博士生导师；主要研究领域为可信计算、系统安全和区块链；先后主持和参加科研项目20余项；获北京市科学技术进步二等奖；已发表论文80余篇，授权专利20余项。

黄浩翔，北京工业大学在读博士研究生；主要研究领域为可信计算、云安全、可信访问控制；已发表论文4篇，申请专利10余项。

胡俊，北京工业大学讲师；主要研究领域为可信计算、云安全、工控安全；获2项科研成果奖；负责通用可信软件基、可重构TCM模拟器等可信计算开源软件项目；出版可信计算专著2本，申请专利10余项。