《可信计算体系结构》标准综述

安宁钰　赵保华　王志皓
(全球能源互联网研究院　北京　102209)
(国家电网先进计算及大数据技术实验室　北京　102209)
(可信计算北京市重点实验室　北京　100124)
(anningyu@foxmail.com)

An Overview of *Trusted Computing Structure Specification*

An Ningyu, Zhao Baohua, and Wang Zhihao
(*Global Energy Interconnection Research Institute, Beijing* 102209)
(*Advanced Computing and Big Data Technology Laboratory of SGCC, Beijing* 102209)
(*Beijing Municipal Key Laboratory of Trusted Computing, Beijing* 100124)

Abstract　Trusted computing is a kind of computing mode of computing and protecting parallel structure, and which can provide the ability of autonomous immunity to malicious code and illegal operation by keeping the integrity of computing environment and logic. Trusted computing architecture based on domestic cryptographic system, the trusted platform control module as a trusted root, a trusted motherboard platform, software as the core, with the network as the link, for a transparent and credible support for the upper application, so as to guarantee the application execution environment and network environment security. This paper introduces the related content of "trusted computing architecture" standard, including the basic principle and function of the basic framework, the core architecture of trusted computing components, trusted information system and trusted computing specification system. "Trusted computing architecture" standard provide specifications and guidelines for design and implementation of trusted computing products from the top, and it can effectively promote the orderly development of trusted computing technology and its industrialization, and provides a unified framework for formulating and revising and follow-up of trusted computing standards.

Key words　cyber security; trusted computing; dual architecture; trusted information system; top-level design

摘　要　可信计算是一种运算与保护并行结构的计算模式，通过保持计算环境及计算逻辑的完整性，为计算平台提供了对恶意代码、非法操作的自主免疫能力. 可信计算体系结构以国产密码体系为基础，以可信平台控制模块为信任根，以可信主板为平台，以软件为核心，以网络作为纽带，对上层应用进行透明可信支撑，从而保障应用执行环境和网络环境安全. 介绍了《可信计算体系结构》标准的相关内容，包括可信计算体系结构的基本原理及功能、核心组成部件、可信信息系统以及可信计算规范体系的基本框架.《可信计算体系结构》标准从顶层为可信计算产品的设计和实施提供规范和指南，可以有效促进可信计算技术及其产业化有序发展，并为后续可信计算系列标准的制定和修订提供一个统一的框架.

收稿日期：2017-03-15

关键词 网络安全;可信计算;双体系结构;可信信息系统;顶层设计
中图法分类号 TP309

随着计算机网络在电力、金融、国防等行业的深度应用,以窃取用户私密信息和破坏系统为目标的恶意代码攻击超过传统病毒成为最大安全威胁.传统的"防病毒、防火墙、入侵检测"的防护技术手段仅能修补已造成的破坏,并不能从根本上解决问题.可信计算[1-5]作为一种运算和防护并行的主动免疫的新计算模式,是改变传统的"封堵查杀"被动防御技术的基础,是构建纵深防御的信息安全保障体系核心技术.本标准从关键行业需求、典型成功案例、信息技术发展方向出发,规范可信计算体系结构、基本功能、核心部件以及组成可信计算信息系统的可信节点的关键特征,服务于实现信息化核心设备和基础设施的安全可控,为确保信息安全提供有力保障.

《中华人民共和国网络安全法》第十六条明确规定:"推广安全可信的网络产品和服务."我国已创新性地提出了"运算+防御"并行的可信计算体系结构基本理论,目前已进入可信计算"3.0时代"并形成了一定数量的产业化成果,在电力、广电等国家重要行业进行了大规模应用,达到了安全免疫效果,充分验证了我国自主创新的可信计算体系结构安全有效并具备可行性.

《可信计算体系结构》标准已历经国家标准项目研究阶段,并已成为中关村可信计算产业联盟的联盟标准之一.经多年发展和工程实践,该标准已成为可信计算业界的事实标准,标准规范了可信计算体系结构、基本功能、核心部件以及组成可信计算信息系统的可信节点的关键特征,统一产业界对我国自主创新具备主动防御能力的可信计算理论和技术结构的理解,服务于实现信息化核心设备和基础设施的安全可控,落实《中华人民共和国网络安全法》相关要求,为确保信息安全提供有力技术保障.

1 可信计算的国内外现状及发展趋势

1) 国外可信计算技术及标准研究现状

以可信平台模块[6-9](trusted platform module, TPM)为核心技术的可信计算组织(Trusted Computing Group, TCG)在可信计算方面的研究代表了国外可信计算技术的发展水平.TCG先后发布近百个可信计算相关规范,形成了规范体系(如图1所示),指导其产品开发和产业发展,其核心规范TPM2.0是TPM1.2的修订版本,目前已

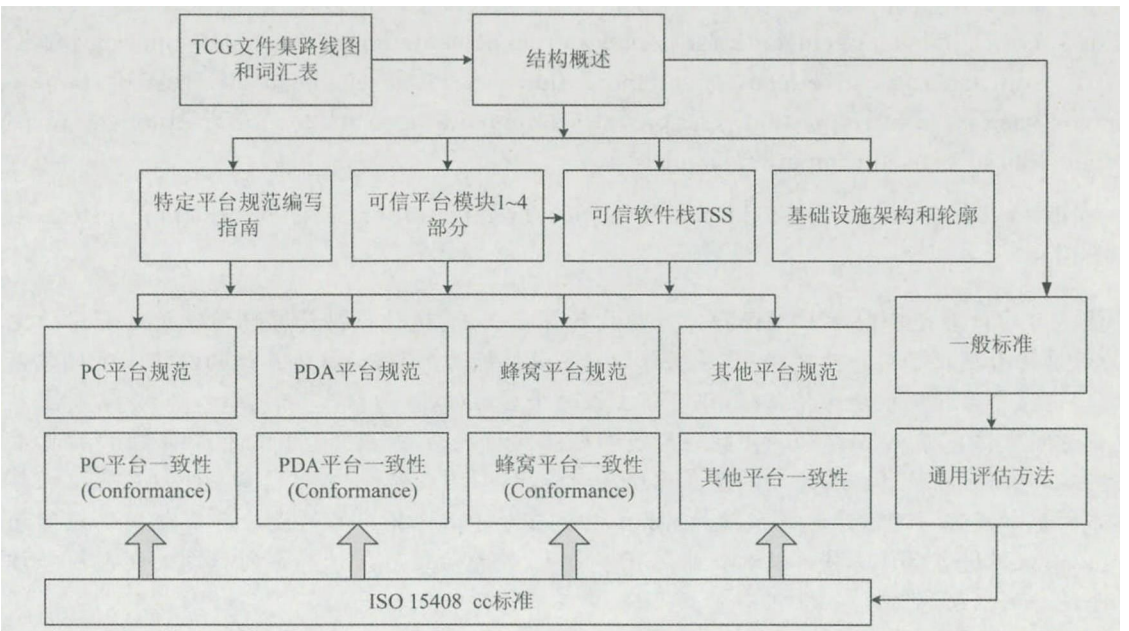

图1 TCG可信计算规范体系

被 ISO/IEC 吸纳为国际标准.

TCG 核心成员 IBM、HP、Intel 和微软等厂商依据其可信计算规范，已形成系列产品，但 TCG 构建的可信计算技术未考虑计算机最初设计对安全防护的简化，所提出的 TPM 本质上是一个外部设备，不具备形成可信计算体系结构的条件，同时其挂接式的工作方式需要上层应用软件进行大量改造，制约了其产品的应用.

2）国内可信计算技术及标准研究现状

可信计算是落实《网络安全法》的重要基础性技术手段. 我国在可信计算技术的研究上起步较早，目前已进入可信计算“3.0”时代，我国学者提出的运算和防御并行的双体系思想[1-3]，具备透明于业务应用的特征，使大规模工程应用成为可能，在此基础上设计的具备免疫能力的可信计算体系结构是我国可信计算技术发展过程中的重大创新，指导着我国可信计算产业发展，部分产品已在电力、广电等国家重要行业核心生产系统中进行了一定规模的成功应用，随着中关村可信计算产业联盟的推动，我国可信计算产业发展将更加快速.

我国在可信计算技术的研究和应用过程中，先后形成了《信息安全技术 可信计算规范 可信平台主板功能接口》(GB/T 29827—2013)、《信息安全技术 可信计算规范 可信连接架构》(GB/T 29828—2013)、《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 29829—2013) 3 个国家标准，仅对密码支撑平台、可信主板和可信网络连接技术进行了规范，远未覆盖可信计算技术的全部环节，尚未构成可信计算标准体系，缺乏可信计算体系结构的技术规范，使相关产品难以互联互通，已严重制约了我国可信计算产业发展和技术应用，难以从技术标准层面对《网络安全法》的贯彻实施进行全面支撑.

3）可信计算技术发展趋势

目前，主动防御是我国国家层面的战略性目标，我国具备主动控制功能的可信计算技术在实现主动防御上具有先天优势，能够为关键信息基础设施提供可信、可控、可管的主动防御能力. 随着云计算、物联网等新型应用的不断发展，带来了新的安全挑战，传统的基于“封、堵、查、杀”的被动防护手段已无法满足安全需求，可信计算技术是实现新型应用安全需求的有效技术手段. 双体系结构的可信计算提供了一种有效的技术手段，相关技术思路已经在国际上得到肯定，Intel，ARM 的新一代芯片产品以及微软的 Windows10 中都应用了可信计算，其中借鉴了我国的可信计算技术思路.

2 《可信计算体系结构标准》的主要内容

2.1 研究内容概述

随着计算机网络在电力、金融、国防等行业的深度应用，以窃取用户私密信息和破坏系统为目标的恶意代码攻击超过传统病毒成为最大安全威胁. 传统的“防病毒、防火墙、入侵检测”的防护技术手段仅能修补已造成的破坏，并不能从根本上解决问题. 可信计算作为一种运算和防护并行的主动免疫的新计算模式，是改变传统的“封堵查杀”被动防御技术的基础，是构建纵深防御的信息安全保障体系核心技术. 本标准从关键行业需求、典型成功案例、信息技术发展方向出发，规范可信计算双体系结构的基本原理、核心组成部件及相互关系、可信信息系统环境下的各类可信节点的技术特征以及可信计算规范体系的主体结构等内容，充分考虑技术的发展方向，使可信计算体系结构标准更具前瞻性和指导性；从顶层规划可信计算标准规范簇的总体框架，明确其相互关系，为可信计算技术相关标准规范的制定和修订提供方向性指导. 其核心内容主要包括：

1）规范我国具有主动免疫功能的可信计算体系的基本原理和功能；

2）规范可信计算核心部件的组成和相互关系；

3）规范可信网络环境中的节点组成和相互关系.

2.2 基本原理及功能

我国可信计算视可信计算节点为独立的主动控制防护节点，与通用计算节点共用同一套软硬件计算平台，共同构成可信计算的双系统体系结构模式. 该体系结构以国产密码体系为基础，以可信平台控制模块为信任根，以可信主板为平台，以软件为核心，以网络作为纽带，对上层应用进行透明可信支撑，从而保障应用执行环境和网络环境安全. 其基本原理图如图 2 所示：

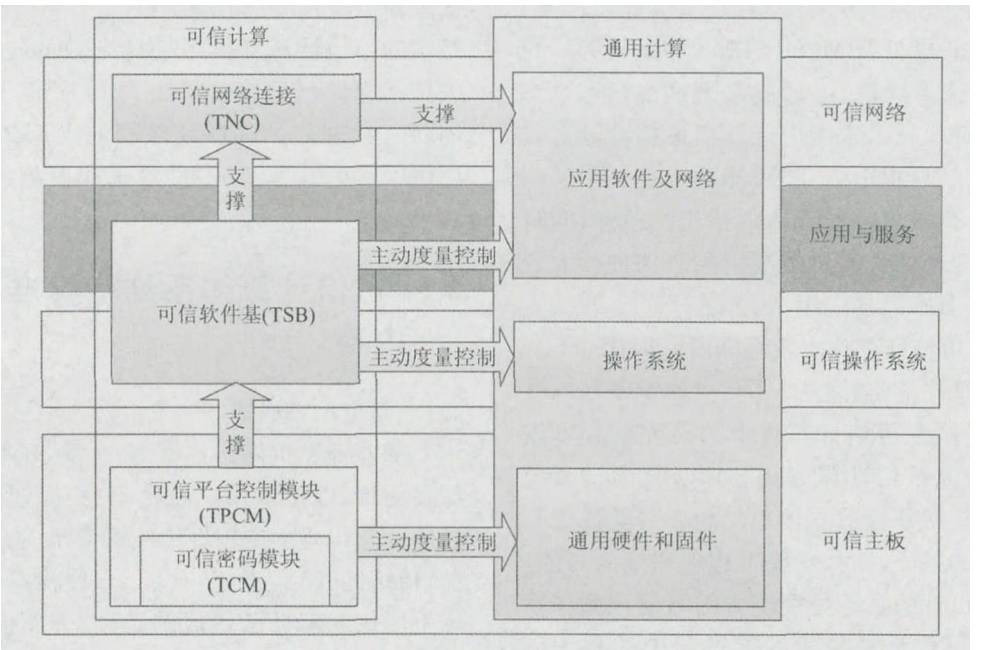

图 2　平台可信体系结构原理图

可信计算基本功能包括可信度量、可信存储和可信报告三大基本功能以及信任链构建、主动免疫、可信协作等支撑功能.

2.3　可信计算核心组成部件

可信计算核心组成部件包括可信密码模块(TCM)、可信平台控制模块(TPCM)、可信平台主板、可信软件基(TSB)和可信网络连接五大核心部件. 其结构组成如图 3 所示：

图 3　可信计算核心组成部件

2.4　可信信息系统中的节点

可信计算信息系统(如图 4 所示)由基于可信计算体系结构的各类可信节点、可信通信网络和可信管理中心构成. 可信节点根据功能和需求的不同可以分为终端节点(包含桌面终端和嵌入式终端)、计算节点、存储节点、网络节点. 可信管理中心对各类可信节点和可信网络进行管理. 各类可信节点间以及和可信安全管理中心间通过可信网络连接进行通信，共同构成可信网络.

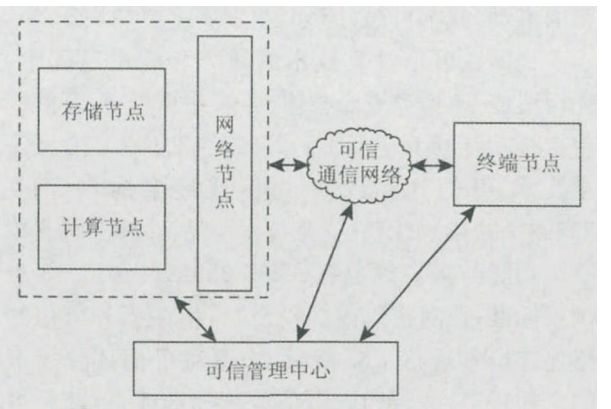

图 4　可信信息系统

2.5　可信计算规范体系基本框架

可信计算规范基本框架可以从主体规范、支撑规范和配套规范 3 个方面进行划分，具体内容如图 5 所示. 其中，主体规范是对可能以实物形式存在的可信计算基础部件进行的规范，支撑规范是对评估和管理和运营要素进行规范，应用规范是对基于主体规范和支撑规范构建的各类可信产品、设备、信息系统以及各行业应用进行规范.

1) 主体规范

规范可信计算体系结构中核心部件的功能、性能以及接口要求等内容.

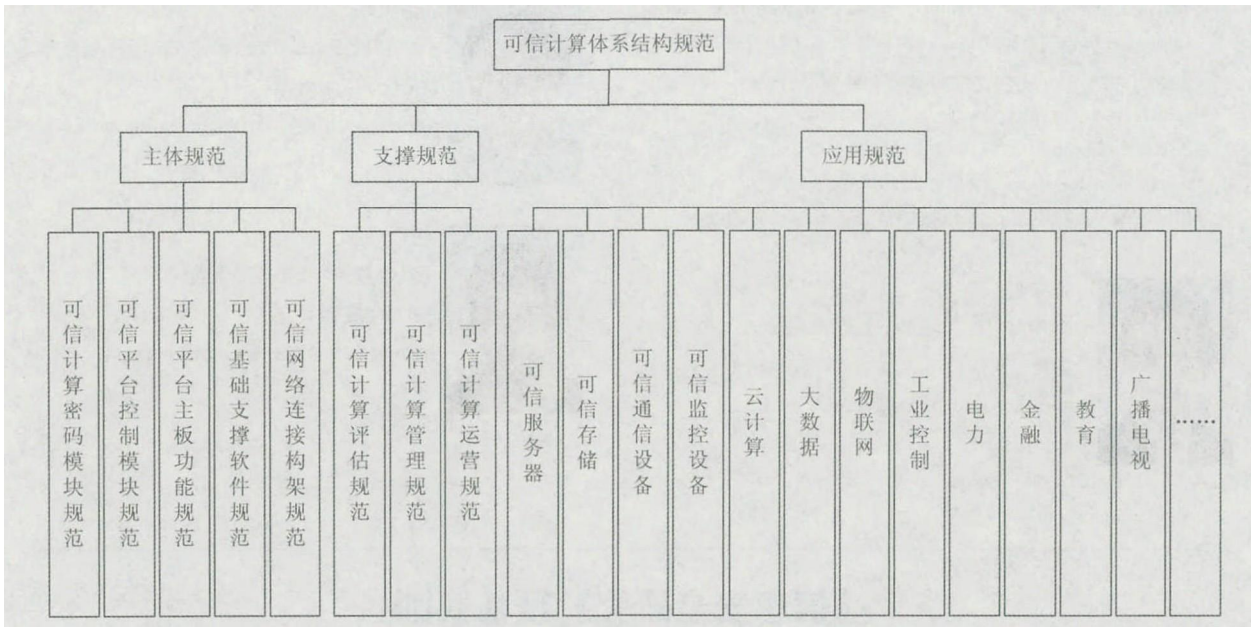

图 5　可信计算系列规范

2）支撑规范

对可信计算产品在评估中所涉及的要素进行规范；对可信计算产品管理运营过程中所涉及的要素进行规范.

3）应用规范

应用规范的内容包括三大系列规范：可信产品和设备规范、可信信息系统规范和可信计算行业应用规范. 可信产品和设备系列规范对各类可信计算产品和设备作出具体规范，包括可信服务器、可信存储等；可信信息系统系列规范是对各类可信信息系统作出具体的规范，包括云计算、工业控制等规范；可信计算行业应用系列规范是针对各行业特点制定的具体可信计算规范和实施细则.

3　结　　论

可信计算是一种运算与保护并行结构的计算模式，通过保持计算环境及计算逻辑的完整性，为计算平台提供了对恶意代码、非法操作的自主免疫能力. 我国已创新性地提出了“运算＋防御”并行的可信计算体系结构基本理论，目前已进入可信计算“3.0 时代”并形成了一定数量的产业化成果，在电力、广电等国家重要行业进行了大规模应用，达到了安全免疫效果. 该体系结构以国产密码体系为基础，以可信平台控制模块为信任根，以可信主板为平台，以软件为核心，以网络作为纽带，对上层应用进行透明可信支撑，从而保障应用执行环境和网络环境安全.《可信计算体系结构》标准从顶层为可信计算产品的设计和实施提供规范和指南，可以有效促进可信计算技术及其产业化有序发展，并为后续可信计算系列标准的制定和修订提供一个统一的框架.

参　考　文　献

[1] 沈昌祥. 用可信计算构筑网络安全[J]. 求是，2015（20）：33-34

[2] 沈昌祥，陈兴蜀. 基于可信计算构建纵深防御的信息安全保障体系[J]. 四川大学学报：工程科学版，2014，46(1)：1-7

[3] 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

[4] 冯登国，秦宇，汪丹，等. 可信计算技术研究[J]. 计算机研究与发展，2011，48(8)：1332-1349

[5] 沈昌祥，公备. 基于国产密码体系的可信计算体系框架[J]. 密码学报，2015，2(5)：381-389

[6] Trusted Computing Group. TCG Specification Architecture Overview，Version 1. 2 [EB/OL]. 2003（2011-01-25）[2017-02-15]. . https://www. trustedcomputinggroup. org

[7] Trusted Computing Group（TCG）. TCG Software Stack（TSS）Specification，Version 1. 10 [R/OL]. （2011-01-25）[2017-02-15]. http://www. trustedcomputinggroup. org/developers/software_stack

[8] Trusted Computing Group. TNC Architecture for Interoperability [EB/OL]. (2011-01-25) [2017-02-15]. http://www.trustedcomputinggroup.org/resources/tnc_architecture_for_interoperability_specification

[9] Trusted Computing Group. Mobile Trusted Module Specification Reversion1 [S/OL]. (2011-01-25) [2017-02-15]. https://www.trustedcomputinggroup.org/specs/mobilephone

安宁钰
工学硕士，工程师，主要研究方向为信息安全、可信计算.
anningyu@foxmail.com

赵保华
工学硕士，工程师，主要研究方向为信息安全、可信计算.
zhaobaohua@geiri.sgcc.com.cn

王志皓
工学硕士，工程师，主要研究方向为信息安全、可信计算.
wangzhihao@geiri.sgcc.com.cn

《信息安全研究》征稿简则

一、《信息安全研究》是由国家发改委主管、国家信息中心主办的中文学术期刊，主要刊登信息安全研究领域的原创性研究成果，其内容覆盖信息安全领域的各个学科。

二、《信息安全研究》主要以论文、技术报告、短文、研究简报、综述等形式进行报道，所刊登的论文均经过同行专家严格的评审。

三、文稿要求

论文：有创新学术见解的研究成果的完整论述，对该学术领域的发展有积极推进意义，字数不受限制。

技术报告：面向信息安全领域的，先进、实用的创新开发成果的技术总结。

综述：对新兴的、活跃的学术研究领域或技术的评述。字数不受限制。

四、来稿注意事项

1. 来稿要求论点明确，数据可靠，条理清晰，文字精练，字迹清楚。

2. 为了使审理过程顺利进行，在投稿的同时，稿件应符合论文模板要求，并且无学术不端问题。模板内容详见本刊网站。

3. 稿件首页包括下列内容：题目、真实姓名、详细工作单位、城市及邮政编码、中文摘要和5~7条关键词。英文题目、汉语拼音的姓名、工作单位的英文译名、英文文摘(200个左右实词)和5~7条与中文关键词对应的英文关键词。文后要有作者简介及照片（作者简介包括姓名、最高学历、职称及主要研究方向）。

4. 来稿必须做到清稿、定稿。稿件中的外文字母必须分清大、小写，正、斜体；上、下角的字母、数码和符号，其位置高低应区别明显。

5. 文中的计量单位一律使用《中华人民共和国法定计量单位》。文中图表只附最必要的，插图要精绘，图中文字书写清楚。插图和照片必须是清绘图和原照片(或高精度扫描图)。图、表应排在正文中的相应位置上。图、表和公式分别用阿拉伯数字全文统一编号。

6. 参考文献只择最主要的列入，综述文章的参考文献可根据内容而定。未公开发表的资料请勿引用，可作为脚注。

五、本刊接收网上投稿。投稿信箱：ris@cei.gov.cn　网上投稿：http://ris.sic.gov.cn