动态可信度量研究综述*

杨慧婷[1]，黄浩翔[2†]，郭学让[1]，郭庆瑞[1]，李 峰[1]，汪烈军[2]

（1. 国网新疆电力有限公司电力科学研究院，新疆 乌鲁木齐 830011；2. 新疆大学 计算机科学与技术学院，新疆 乌鲁木齐 830017）

摘 要： 随着数字化转型的加速推进及发展新质生产力的核心需求，重要信息系统在社会各领域得到广泛应用，然而其业务多样化、规模庞大化致使运行境况愈发复杂，如何有效保证其生命周期内的可信运行成为社会关注的焦点问题. 随着可信计算的应用被提升至国家战略层面，动态度量作为其核心技术之一，成为解决重要信息系统运行态可信难题的理想方案，但是如何保证动态度量的有效性及低性能开销成为一个极具挑战的问题. 首先，介绍了动态度量的应用背景，梳理了可信计算的基本概念及定义；其次，从动态度量的有效性、可信评估的精准性及度量架构的安全性三个方面分析了动态度量的关键因素，并给出了动态度量的定义. 接着，从动态度量模型的理论研究和工程研究（被度量对象的全面性、度量架构的安全性）两个方面对现有方案进行了深入探讨. 在此基础上，对动态度量面临的技术难题进行了总结分析并给出了未来解决思路. 最后，对动态度量技术未来发展及应用进行了展望.

关键词： 重要信息系统；动态度量；可信运行；主动免疫可信

DOI： 10.13568/j.cnki.651094.651316. 2024.07.23.0001

中图分类号： TP301 **文献标识码：** A **文章编号：** 2096-7675(2025)04-0385-016

引文格式： 杨慧婷，黄浩翔，郭学让，郭庆瑞，李峰，汪烈军. 动态可信度量研究综述[J]. 新疆大学学报(自然科学版中英文)，2025，42(4)：385-400.

英文引文格式： YANG Huiting，HUANG Haoxiang，GUO Xuerang，GUO Qingrui，LI Feng，WANG Liejun. A survey on trusted dynamic metrics technology[J]. Journal of Xinjiang University(Natural Science Edition in Chinese and English)，2025，42(4)：385-400.

A Survey on Trusted Dynamic Metrics Technology

YANG Huiting[1], HUANG Haoxiang[2], GUO Xuerang[1], GUO Qingrui[1], LI Feng[1], WANG Liejun[2]

(*1. State Grid Xinjiang Electric Power Co., Ltd. Electric Power Research Institute, Urumqi Xinjiang, 830011, China;*
2. School of Computer Science and Technology, Xinjiang University, Urumqi Xinjiang, 830017, China)

Abstract： As digital transformation and the core demand for new quality productivity accelerate, the important information systems have been widely applied in various fields of society. However, the diversification of business and magnification of scale have made their operational conditions increasingly complicated, and how to effectively ensure their trusted operation during their life cycle has become a common concern of society. With the deep application of the trustworthy computing rising to the national strategic level, dynamic metrics, as one of its core technologies, become an ideal solution to the problem of trustworthy operation state of important information systems. However, how to ensure the effectiveness and low performance overhead of dynamic measurement becomes an extremely challenging issue. Firstly, this paper introduces the application background of dynamic metrics, and then presents the basic concepts and definitions of trusted computing. Secondly, we analyse the key factors and challenges of dynamic metrics from three aspects: The validity of dynamic metrics, the accuracy of the trustworthy evaluation system and the security of the metrics architecture, and give the definition of dynamic metrics. Furthermore, the theoretical and engineering studies of dynamic metrics models (comprehensiveness of the metrics object and security of the metrics architecture) are discussed in depth. On the basis of previously stated, the technical challenges of dynamic metrics are summarized and analyzed. Finally, we put forward the future development and application of dynamic measurement.

Key words： important information system; dynamic measurement; trusted operation; active immunity trusted

---

* **收稿日期：** 2024-07-23

基金项目： 新疆维吾尔自治区高校基本科研业务费科研项目-培育类项目“基于可信计算的云应用主动可信防护架构关键技术研究”（202404120003）；新疆维吾尔自治区科技计划项目-自然科学基金-青年基金项目“基于区块链的云数据动态可信访问控制关键技术研究”（202404120022）.

作者简介： 杨慧婷（1991—），女，硕士，工程师，主要从事信息安全、电力通信的研究，E-mail：731613043@qq.com.

† **通讯作者：** 黄浩翔（1992—），男，博士，副教授，主要从事可信计算、云安全、访问控制的研究，E-mail：hhx_cs@xju.edu.cn.

0 引 言

“数智时代”的来临加速推动了全球数字化转型，极大地促进了社会的进步及管理模式的变革. 在数字化转型的驱动下，能源、金融、政务等重要领域的“业务上云”成为行业趋势. 然而，目前全球各国竞争日益加剧，局部冲突不断，关键信息基础设施正在成为“对手”谋取经济乃至政治利益的首要攻击目标. 新疆现代化发展要求构建风电、光伏发电等新能源产业，推动能源结构优化升级，关键信息基础设施的安全性不仅关乎自治区的长治久安，更对我国能源产业结构转型与调整至关重要. 但是随着数字化转型在社会各领域的深层次推进及延伸，以能源电力系统、云计算、物联网等为代表的重要信息系统的安全成为关键信息基础设施安全的核心前提，其呈现的分布性、动态性、不确定性使得运行过程安全防护的重要性和紧迫性日渐提高[1].

2011年，美国提出了通过瘫痪他国重要基础设施（如电网等）实现战略诉求的设想[2]. 近年来，国际社会相继发生了“乌克兰断电事件”[3]、“委内瑞拉国家电网攻击事件”[4]、“基于CVE-2022-29303漏洞的光伏电网攻击事件”[5]、“2025年亚冬会赛事信息系统攻击事件”及“黑龙江省内关键信息基础设施攻击事件”等多起重大安全事件，2025年5月巴基斯坦通过对印度包括电网、广播系统在内的关键信息基础设施进行攻击更是将前述设想变为现实. 随着能源、交通、医疗等关键基础设施深度互联，网络空间已经成为国家安全的新领域和国际竞争的新高地，网络安全已从“信息保护”升级为“文明生存底线”的守护战.

安全事件的频繁发生，意味着传统安全防护理念已不能满足“数字化转型”期重要信息系统的安全需求. 积极构建主动防御新体系，促使防御理念从被动转向主动，建立自我防护、主动免疫的安全框架保证重要信息系统运行过程的安全可信已迫在眉睫. 人类的认知能力存在局限性，设计系统不能穷尽所有逻辑组合，必定存在逻辑不全的缺陷，利用缺陷挖掘漏洞进行攻击是网络安全领域永恒的话题. 然而，依赖病毒查杀、防火墙、入侵检测的传统“老三样”封堵查杀方式难以应对利用逻辑缺陷的攻击. 此外，“老三样”属于被动防御，容易陷入“打鼹鼠（已知病毒）”的逻辑怪圈，面对新型攻击（如0 Day攻击等）缺乏及时性和灵活性（病毒库的更新永远滞后于新型病毒的产生）.

没有网络安全就没有国家安全，没有信息化就没有现代化[6]. 近年来，我国愈发重视信息安全领域的自主可控、安全可信，并将可信计算的应用提升至国家战略层面，积极构筑国家重要信息系统高安全等级防护体系.《国家网络空间安全战略》[7]提出“夯实网络安全基础，加快安全可信产品推广应用”的战略要求.《中华人民共和国网络安全法》[8]提出“加快推广安全可信的产品及服务”的要求，新修订的《信息安全技术网络安全等级保护基本要求》（简称等级保护2.0）[9]和《关键信息基础设施安全保护条例》更是明确要求全面使用安全可信的产品和服务对重要信息系统及应用进行动态可信验证. 然而，当前计算环境普遍缺乏可信产品及服务的深层次应用，重要信息系统的运行缺乏动态度量的可信保障. 可信计算作为一种实现网络与信息安全技术从“软安全”向“硬安全”过渡的新型技术，应用可信计算构筑网络安全防护体系已成为广泛共识. 基于主动免疫可信计算技术构建新型主动防御架构，保证重要信息系统运行过程的动态可信性不仅是保证数字经济有序、健康发展的重要基础，更是助力社会数字化转型的重要途径和必然选择[10].

本文首先介绍动态度量的应用背景及必要性，然后对可信计算相关基础知识、可信的主流定义进行了总结，并提出可信的定义. 其次，介绍了可信度量的基本概念及分类，总结并梳理了动态度量应具备的关键因素. 接着，从理论研究和工程研究（被度量对象全面性、度量架构安全性）两个方向分类讨论了现有动态度量方案，并基于此分析了不同动态度量方案的优势及不足；基于上述分析，对动态度量所面临的技术难题进行总结论述，并给出了预期解决方案. 最后，对动态度量技术进行了总结，以期推动动态度量技术的研究与发展.

1 可信计算技术概述

1.1 可信定义

当前，关于可信尚未形成统一定义，不同组织解释方式有所不同，其中较具代表性的有以下几种：

可信计算组织将可信定义为：如果一个实体的行为总是以预期的方式朝着预期的目标跃进，那么该实体是可信的.

沈昌祥院士[10]结合人类免疫系统的理念提出了主动免疫可信计算：计算、运算的同时进行安全防护，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，相当于为网络信息系统培育了免疫能力，使过程和操作行为在任意条件下的计算结果总是符合预期，开启了我国可信3.0防御与运算并行的“主动防御体系”新时代.

ISO/IEC将可信定义为[11]：参与计算的组件、操作或过程在任意条件下是可预测的，并能够抵御病毒和一定程度的物理干扰.

IEEE将可信定义为[12]：计算机系统所提供的服务的可信赖性是可论证的.

虽然国内外各组织或机构关于可信的具体描述有所不同，但其共性在于均强调了实体行为的可预测性，进而能够保证系统提供的服务是可信的. 本文认为，所谓可信即依托硬件可信芯片，在系统完整生命周期内，主动对参与系统运行的相关组件完整性和系统行为的可信性进行持续且不被干扰的可信度量，保证系统运行轨迹始终符合预期.

1.2　可信计算基础

可信计算将人类社会中较为完善的成功管理经验引入计算系统中，是一种以密码学为基础，以可信芯片为源头的增强计算机系统可信性的综合性信息安全技术. 可信计算主要思想是：在计算系统中，建立一个可信根，从可信根开始到硬件平台，到操作系统，再到应用，一级度量一级，一级认证一级，一级信任一级，把这种信任扩展到整个计算机系统，并采取防护措施，确保计算资源的完整性和行为的预期性，从而提高计算机系统的可信性.

可信根是集成在可信平台中的硬件模块，主要用于建立及保障兼具物理学意义和密码学意义的信任源点. 国际上，应用较为广泛的可信根是由可信计算组织（Trusted Computing Group, TCG）所提出的可信平台模块（Trusted Platform Module, TPM），体现了TCG以硬件芯片增强计算平台安全的基本思想. 但是，TPM是一个只能被动接受可信调用的硬件安全模块，缺乏主动度量和主动控制机制，无法构建主动防御体系.

在国内，从自身国情和技术出发，采用可信平台控制模块（Trusted Platform Control Module, TPCM）作为构建主动免疫可信体系的信任锚点，其具备主动控制和主动度量功能，改变了TPM作为被动调用设备的传统安全思路[13]，能够有效构建主动防御体系，如图1所示.

分类	技术机制	技术手段	可信根	体系结构	安全强度
TCG可信计算	被动可信	TPM作为外部设备串接于外总线，可信软件栈作为子程序库**被动调用**	TPM	串行	能够实现对计算系统的静态检测保护
主动免疫可信计算	主动可信	密码为基因，**主动识别**、**主动度量**、主动保密存储	TPCM	在原有的计算节点系统外构建一个逻辑上独立的可信子系统作为防护单元，从而构建**计算+防护的并行**双体系结构	能够主动抵御未知病毒、漏洞，能够实现对重要信息系统**动态**防护

可信根	连接方式	信任源点是否可信	设备类型	上电方式	信任链构建方式
TPM	连接至设备控制器**从设备**接口	在TPM外部，不可信	被动设备	CPU上电，然后初始化相应总线使用TPM芯片	可信度量根核（CRTM）最先执行并对后一级启动软件（如BIOS）进行可信度量，然后BIOS度量后续启动软件；如：CRTM->BIOS->OS Loader->OS Kernel
TPCM	连接至设备控制器**主设备**接口	在TPCM内部，可信	主动设备	先于计算平台CPU上电，取得计算平台控制权	由TPCM对计算平台启动过程的每一级（如BIOS、OS Kernel、Application等）进行可信度量并判定可信性

图 1　“被动”可信计算技术与“主动”可信计算技术对比

国际上，以TCG为代表的可信计算技术是一种基于TPM的软硬件结合的被动式可信计算组件，其通过向系统硬件、操作系统和应用提供可信调用接口来实现特定可信功能的被动可信技术（图2）.

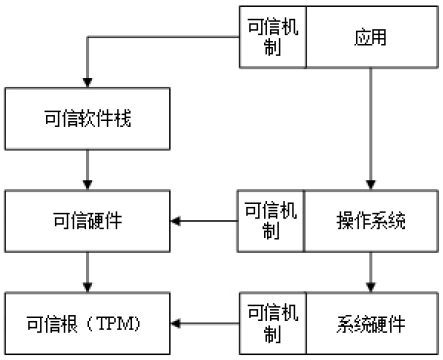

图 2 被动可信

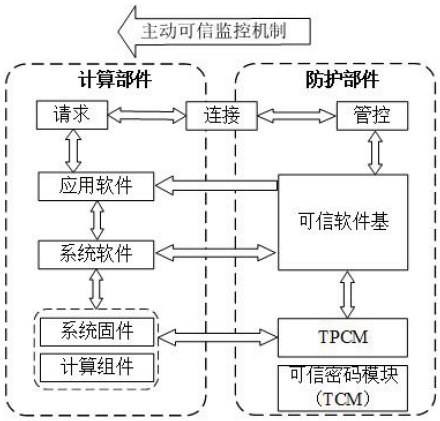

图 3 主动免疫可信架构

我国以沈昌祥院士为代表的研究人员从网络安全的基本理论出发，总结信息安全和可信计算的相关理论，经长期理论探索和工程实践，提出了可信3.0理论. 所谓可信3.0即主动免疫可信计算，是一种以双系统体系架构和主动防护为核心的全新可信计算体系结构框架（图3）. 该架构中，计算部件和防护部件解耦，构成逻辑上彼此独立的系统，防护部件对计算部件实施主动监控，以实现系统运行流程的主动可控. 防护部件安全性不依赖于操作系统和核心应用，可独立运行并实现动态防护，解决了TCG被动可信存在的诸多安全缺陷，是符合我国网络安全战略需求的可信计算理论.

1.3 可信度量

可信度量是依据基准值对被度量对象的完整性进行校验或对实体行为与预期描述契合程度进行评估的一种“可信度”量化方式. 可信度量主要包括静态可信度量和动态可信度量，其中静态度量主要是对数据完整性进行“加载时”可信校验，度量行为不具有连续性，其过程如图4所示.

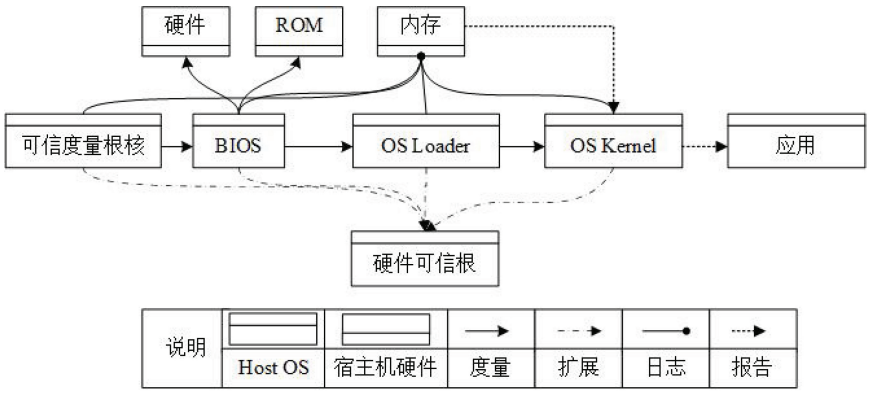

图 4 静态度量机制

随着系统的复杂化、攻击手段的多样化及环境的动态变化，静态度量已不能满足重要信息系统运行时的安全需求，“可信度”量化迫切需要动态、持续进行，能够有效表征系统运行时可信的动态度量成为研究的热点. 可信软件基标准[14]将动态度量定义为：在系统运行过程中，对系统完整性和行为安全性进行测量和评估的可信度量方法.

本文认为，动态度量是一种对“可信度”进行连续、动态量化的手段，即依据被度量对象的不同，基于合适的可信基准值域，采取可行且可靠的技术手段对被度量对象及其基准值域进行“连续”匹配的评估过程.

动态度量模型可使用四元组$DM=(Bv,Mo,Me,Ev)$描述，其中：Bv代表基准值域，表示被度量对象可信特性的特征值，作为判定被度量对象是否可信的参照标准；Mo代表被度量对象，包括系统或应用运行过程中涉及的主体、客体、操作和环境等多种能够反映运行状态的对象类型，如内核、代码段、文件、读写操作等；Me表示度量触发方式；Ev表示可信评估手段.

1.3.1　动态度量关键因素

从动态度量刻画运行态可信有效性、精准性及低性能损耗的角度出发，影响动态度量的关键因素如下：

（1）被度量对象的选取

动态度量的根本问题是准确、及时、全面地获取被度量对象[15]，被度量对象选取的全面性是决定动态度量粒度及度量有效性的关键因素. 如果仅对静态代码段、重要配置文件等静态对象进行完整性校验，表征运行态可信具有较大局限性，且无法应对瞬时攻击、控制流劫持攻击[16].

（2）度量、判定策略的制定

度量策略主要指依据系统安全要求及性能瓶颈问题，设置合适的度量触发条件. 而判定策略则是指可信评估准则. 从度量连续性的角度出发，动态度量行为应尽量连续以期能够精确刻画运行状态. 然而，连续的动态度量会给系统引入较大的性能开销，且在安全要求不高的系统中，高频度的动态度量不仅缺乏必要性，且会影响业务的连续性.

（3）度量点的部署

度量点是指度量行为执行点，其分布密度是影响针对恶意攻击的防御有效性及系统性能开销的重要因素.

2　动态度量研究技术分析

本文针对动态度量研究类型的不同，从理论研究、工程研究（被度量对象的全面性、度量架构的安全性）两个方面对动态度量技术进行阐述分析，具体研究架构如图5所示.

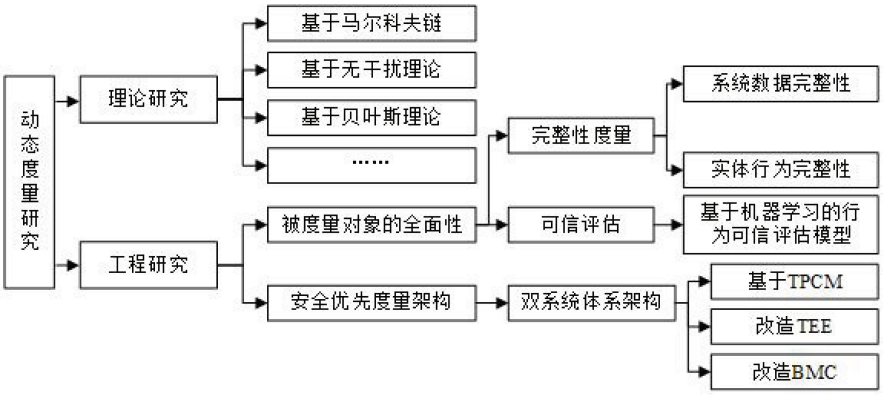

图 5　研究框架图

2.1　动态度量理论模型研究

可信度是一个具有一定趋势的动态变化数值，单次平均的度量值不能较好地反映实际状况[17]. 因此，可信度量化必须具备持续性及低离散性. 当前动态度量的相关研究领域，多从工程实现的角度探讨如何兼顾度量有效性及低性能开销，度量策略的设定、度量点的密度散布等带有较大的主观性，缺乏严谨的数据分析或理论支撑，无法有效反映运行态可信关系的复杂性. 此外，可信度的评估受主观经验、主观决策及有限理性的影响，动态可信评估结果的客观性和精准性存疑.

不断有学者利用数学方法或工具建立动态信任预测模型，如结合马尔科夫链建立动态度量模型[18−19]，层次化分析并量化系统动态可信性. 文献[20]基于历史证据窗口、直接信任树（Direct Trust Tree, DTT）机制[21]及诱导有序加权平均算子（Induced Ordered Weighted Averaging, IOWA）理论构建了一种动态信任预测模型，改善了传统信任预测模型动态能力不足的问题，弱化了信任度权重设置的主观性. 文献[22]通过引入Bayes理论，利用后验概率不断修正先验概率的方式动态评估系统运行态行为的可信性，具备较好的动态适应性及安全性. 文献[23]指出当前的动态度量方案缺乏数学模型的理论支撑、度量的实时性低，提出了一种基于无干扰理论的软件动态度量模型，是理论与工程结合的典型. 文献[24]基于无干扰理论提出了一种虚拟机启动过程的动态度量模型，增强了虚拟机启动过程的动态防护性. 然而基于无干扰理论的相关方案并未从理论的角度探讨如何设置度量触发时机，度量有效性、实时性及度量引入的性能开销间的平衡问题依旧悬而未决.

综上，目前动态度量领域，缺乏较为完善、统一的动态度量数学模型，且多数理论模型难以在实际系统中应用，理论成果和实际应用存在脱节现象，动态度量理论模型还需要结合实际系统深入研究.

2.2 基于完整性校验的动态度量研究

2.2.1 基于系统数据完整性的动态度量

完整性度量架构（Integrity Measurement Architecture, IMA）是国际上第一个基于TCG标准的度量架构[25]，其度量值是一个相对静态及稳定的值，只能表征系统加载时刻的可信性，无法保证运行时实际行为的可信性，属于“加载时度量”模式. 然而，随着系统安全性要求的提高及攻击方式的迭代更新，IMA对系统运行态可信刻画能力弱，无法有效应对TOC-TOU（Time of Check Time of Use）、ROP（Return-Oriented Programming）[15,26]等运行时攻击的劣势逐渐凸显.

Jager等[27]在IMA的基础上，引入CW-Lite模型，提出了PRIMA度量架构，丰富了被度量对象的选取、优化了度量策略，提高了度量模型的灵活性、度量的效率及表征运行态可信的有效性. 但其动态度量依赖特定的强制访问控制策略，可用性不足. Petroni等[28−29]通过对内核数据实施周期性的完整性度量来保证内核运行时可信，提高了内核应对运行时攻击的能力，但是应对瞬时攻击具有偶然性. 虽然上述动态度量模式较为可靠且已被付诸应用，但是对系统运行状态可信的表征能力有限（无法应对针对TOC-TOU的竞争条件缺陷攻击，即攻击者能够根据度量粒度在相邻两个度量时刻之间动态的插入攻击行为与恢复行为），且动态度量策略有待优化.

随着以开放、动态、分布式为核心特征的云计算、物联网等复杂系统在社会各领域的广泛应用，研究人员开始通过优化度量行为触发方式或扩大被度量对象的全面性等手段来提高对系统运行态可信的保障（表1）. BIND[30]的出现是推动可信度量触发方式由固定时间间隔触发向基于事件触发转变的一种早期尝试，其通过选择度量点并插入Hook函数，从而提高度量行为的有效性. 然而BIND不仅增加了代码实现的负担，且与以前的所有代码都不兼容. 随后，不断有学者对度量行为触发方式进行优化，如Dong等[31]通过对Rootkit等攻击行为建模，并以此作为触发可信度量的依据，文献[32]提出基于页表的动态可信度量方案，将度量触发时机延迟到代码页进入内存运行的时刻，文献[33-34]从“分页”的角度提出动态度量方案等.

文献[35-37]基于指令级插桩技术对被监控对象源码进行编辑，从而插入探针，当程序执行触发探针后跳转到度量逻辑中，达到动态触发度量行为的目的. 基于探针触发度量行为的相关方案能够保证系统生命周期内的运行可信，但是探针的分布密度是影响度量有效性与度量引入性能开销间平衡的关键问题，高密度探针势必会引入较大性能开销. 同时需要修改二进制源码也增大了实现难度，甚至会引入不可预期的安全隐患.

表 1 度量方案对比

方案	度量点位置	度量触发方式	被度量对象类型	细粒度性	实时性	开销	度量机制安全防护
IMA[25]	应用层	加载时度量	静态代码	中	差	小	不具备
PRIMA[27]	内核层	加载时度量+Hook触发	静态代码、信息流	细	好	较大	不具备
文献[28-29]	应用层	周期性度量	内核数据	中	一般	一般	不具备
BIND[30]	内核层	事件触发	静态数据	细	较好	较大	不具备
KIMS[31]	内核层	基于行为检测的事件触发	静态内核数据、动态数据结构	细	好	较大	具备
文献[32-34]	内核层	基于页加载事件触发	代码页	细	好	一般	不具备
文献[35-36]	内核层	基于探针事件触发	静态数据	细	较好	较大	具备
LKIM[38]	虚拟机监视层	加载及运行时度量	内核数据	细	好	较大	不具备

但是，上述方案也存在如下不足：

（1）度量点预设，度量触发方式为被动触发（即采用TCG被动调用的外挂式体系架构度量方式），度量机制不具备主动防御能力，只能被动接受计算部件调用. 动态度量策略的制定缺乏理论分析，主观因素较强，度量结果的可信性有待商榷，缺乏合适的数学模型在提高度量密度的前提下降低度量引入的性能开销；

（2）缺乏对系统运行过程的交互行为及内存数据等动态对象的可信评估；

（3）随机触发度量行为的方案中随机时间种子“软产生”，易被侦测探知，增大了TOC-TOU攻击风险；

（4）度量机制（防护部件的一部分）和计算部件串行运行会影响系统业务连续性，也缺乏对度量机制的安全防护，度量机制与应用、计算系统运行在同一环境中，面临较大的攻击面，存在被篡改或绕过的风险.

2.2.2　基于行为完整性的动态度量

随着计算系统的复杂化，其运行过程中呈现高动态性、灵活性及动态数据变化不确定性等特点. 越来越多的研究人员意识到，静态数据的可信性不足以充分表征运行过程中的动态可信，也不符合“行为符合预期”的可信本质[14]. 此外，随着RootKit[39−42]、ROP[43]、JOP[44]等新型攻击手段的出现及等级保护2.0中提出对重要信息系统行为进行可信评估的要求，采用合适手段对系统运行期间的行为进行量化，并基于此作为运行状态可信的举证支持是极具意义的. 国内外相关学者在行为可信度量（其过程如图6所示）方面进行了较多的研究及探索，主要包括三大类.

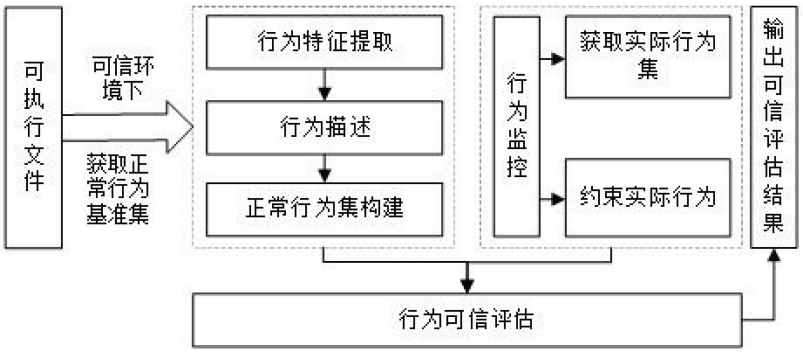

图 6　基于行为的动态度量流程

（1）系统调用短序列模型

文献[45]指出系统的动态可信性只需关注与可信相关的行为，而系统调用作为内核向应用提供系统资源服务的核心手段，许多攻击行为是通过系统调用来实现[46]. 而系统或进程的正常行为都可以由其正常运行时产生的系统调用序列描述，因此可以通过对运行过程中的系统调用进行建模来描述预期可信行为.

早在20世纪90年代就有国外研究人员通过建立系统调用短序列模型的方式来对应用程序运行过程中的异常行为进行检测. 文献[47-48]等提出的基于系统调用序列的N-gram检测方法，通过预设常数N，并利用枚举训练数据集中所有相邻且唯一长度为N的序列以获得应用程序的正常行为，然后使用长度为N的滑动窗口顺序匹配检测到的系统调用序列，具有训练速度快的优点. 然而，上述方案只能识别训练过程中遇到的小于或等于N的系统调用序列，检测效率低下且可信属性模糊. 此后，相关学者围绕短序列模型不断创新，如文献[49]通过引入非定长模式算法改进系统调用序列行为模型，文献[50]基于短序列模型利用马尔科夫链标识系统调用的状态转移特性等.

（2）静态分析

静态分析主要利用可执行二进制文件格式，通过反编译手段提取指令序列，或提取系统调用、函数调用构造控制流分析图，并以此作为特征建立恶意代码检测模型. 但是系统调用与上层应用间存在着语义隔离，仅从系统调用无法与应用行为建立严谨映射关系，具备一定的局限性[23]. 研究人员尝试综合考虑系统调用或者应用编程接口（Application Programming Interface, API）的语法和语义，以图、状态机、机器学习等作为工具对行为进行研究[51−52].

文献[53]通过对应用程序源代码的静态分析获取其行为模型，该模型是通过静态分析构建系统调用正常行为序列的早期尝试. 文献[54]将静态分析的目标替换成二进制代码，要求重写二进制可执行程序，并在函数调用前后插入空操作用来减少状态机的不确定性. 该方案具有不依赖于特定的编程语言和计算机体系结构的优点，但是方案的实现需要修改二进制可执行程序，实现困难且会引入不可预知的风险.

虽然相当多的研究方案都依赖静态分析[55]，但是静态分析也有其众所周知的局限性：

1）缺乏系统的方法大规模验证静态分析结果，其度量结果的准确性无法得到充分有效的保障；

2）静态分析的方法虽然效率高，但是系统或应用的运行具有不确定性，依赖静态分析无法完备预测实际的动态运行过程，存在误报率高、可信评估完备性低的问题；

3）容易受到攻击者不断改进的混淆技术（所谓混淆是将代码转换成一种功能上等价，但难于阅读和理解的形式的行为）影响，攻击者应用混淆技术能够增大恶意代码被分析的难度，从而使得可信度量的消息倍增.

（3）动态分析

动态分析方式根据软件执行的审计历史，学习软件的正常系统调用序列模型，是一种自动模型构建技术，其通过观察软件执行从而构建正常行为模型. 文献[56]最早提出动态分析的解决方案，文献[57]提出并设计了一种新的Android应用动态分析框架，文献[58]提出一种工业控制系统背景下的动态长度链信任传递模型，满足工业控制系统实时性要求. 上述方案所构建的模型低估了预期行为的复杂性，模型仅考虑训练期间观察到的行为，但并非所有有效的程序执行都已被观察. 张帆等[23]结合无干扰理论建立了软件实施可信度量模型，该方案无需学习训练，根据预编写的软件预期行为规范对软件实时行为进行可信评估，其优点在于结合理论模型建立了通用的可信度量框架，但是软件预期行为规范的编写依赖于漏洞的预先定位，缺乏对未知攻击的防御能力.

动态行为分析的技术弥补了静态分析在检测效果方面的不足，但是并非所有有效的执行行为都已被观察，尤其随着系统、应用等复杂化，其行为类型愈发多元，目前的技术难以将所有行为都纳入到可信评估的范围内，无法产生较为完备的度量结果. 同时，在实时性要求较高的系统或应用中，频繁地对行为进行动态完整性度量，会产生较为明显的时延，影响业务的连续性或用户的体验感. 此外，内核层的系统调用与应用层的进程间存在语义断层且具有重复性，如果不考虑系统调用的上下文语义或参数，从系统调用角度无法与应用行为建立严谨映射关系，具备一定的局限性.

2.2.3 基于机器学习的行为动态度量

重要信息系统往往承担跨节点繁杂的计算任务，系统实际运行过程中行为并不严格按照预想的行为机械执行，而是具备一定的松弛度（行为可信并非二元化判定，而是具备一定基准值域范围的可信评估），基于完整性的行为动态度量已不能满足重要信息系统的高可信需求.

依托算力的解放、云计算、物联网等技术深层次的下沉与应用及人工智能被列入国家发展战略[59]等一系列契机，开启了人工智能研究及应用的新高潮[60]. 随着机器学习的成熟与运用，引入机器学习对恶意行为进行建模，构建能够精准识别系统运行态行为是否可信的动态度量模型成为研究动态度量的一种新思路.

文献[61]引入深度学习框架对勒索软件的行为进行分析，通过卷积和循环神经网络对恶意行为的高级特征进行提取，显著提高了针对恶意行为的检测精度，降低了漏报率和误报率. Das等[62]提出一种基于系统调用的恶意行为检测方案GuardOL，该方案使用一种新的频率集中模型（FCM）从已知的恶意软件样本中学习恶意行为模式以构建行为特征. GuardOL基于构建的特征利用多层感知器进行分类训练，用于运行时对执行程序进行恶意或良性的分类. 实验表明GuardOL可以检测到不修改系统调用库的内核层次恶意软件，且在执行的前30%内检测到46%的恶意软件；甚至在执行100%时，误报率小于3%. 但是，该方案无法检测到一些操作系统调用内部指令或系统调用表条目的内核Rootkits（例如，Adore-ng、Sk2rc2）. 文献[63]指出系统安全仅依靠阻断和防御是远远不够的，提出了一种基于当前应急响应系统通用的行为和参数基线的入侵行为检测方案，但是该方案中所谓行为基线的构建仅仅依赖现有通用恶意行为，针对未知恶意攻击的检测效果不佳.

主动学习提出了一种恶意代码检测方法，通过分析进程在执行过程中对操作系统资源的访问行为，构造了用于描述完整系统资源访问的数据依赖网络，建立合适的系统调用行为评估模型. 实验表明，在训练样本仅为总体样本数量1%的情况下，该方法的检测正确率达到94.45%，而错误率仅有5.55%；相比传统基于统计分类器的检测方法，错误率降低了36.5%.

目前，基于机器学习构建系统运行中的动态行为模型仍然处于发展阶段，还存在着许多未来工作和挑战：

（1）基于机器学习的动态行为分析技术提高了检测模型的灵活度及检测率，能够很好地分析恶意样本的行为信息，但是其检测效率有待提高.

（2）现有的基于机器学习的恶意代码检测方案能够有效检测已知攻击，但是多依赖于对已发现的恶意代码数据进行训练学习而得到的模型进行分类，未来可以考虑与数据挖掘领域进行深度结合，以期能够对未知攻击（如0 Day漏洞）进行预警.

（3）随着以指令压缩、指令替换、指令交换、指令扩展和添加垃圾指令为主要手段进行代码特征模糊的模糊变换策略[64]逐步被应用到恶意代码的编写中，攻击方式被检测的难度增大. 如何提取更为精确的特征来构建系统运行过程的动态行为可信评估模型也将成为未来基于机器学习检测恶意代码的一项待突破的研究.

虽然基于机器学习建立动态度量行为评估模型能够有效刻画系统运行状态，也存在着一些不足：当前针对

人工智能系统本身的攻击在逐年指数递增，若训练数据受到扰动或被偏见性标注，则可能输出不恰当结果. 这种对抗扰动显然会极大地误导对系统状态的可信评估. 训练数据的可信性、学习模型的可信性已成为保证基于人工智能对系统运行态可信预测的重要基石. 保护人工智能系统的可信性已然成为应用机器学习的动态度量技术需要慎重考虑的关键点.

2.3　安全架构优先的动态度量研究

TCG被动度量架构不仅缺乏主动度量能力、防护部件自身安全防护能力较弱[26]，且防护和计算串行执行的度量方式会引入较大的性能开销. 虽然随着安全优先架构[65]的提出，防护部件自身安全性问题得到了缓解，但是防护部件仍属于被动调用的一方，不具备主动防护能力.

随着基于可信计算技术构建新型安全架构成为国际共识，中国提出了运算和防护并存的主动免疫可信计算理论，计算部件和防护部件逻辑独立、并行运行的双系统体系架构使得构建强安全性、高效的主动动态度量框架成为可能. 本节讨论基于双系统体系架构的动态度量相关研究.

2.3.1　基于主动免疫可信思想的动态度量

主动免疫可信计算在密码体制和体系结构方面突破了国际可信计算的局限性[66−68]，以TPCM为信任锚点构建了计算、防护并行的双系统体系架构（图3）. TPCM能够先于主机计算部件上电启动，并在计算部件的生命周期内与其并行运行，实现运算的同时主动开启对计算系统的安全防护，为网络系统培育免疫能力，使操作和行为在任意条件下的计算结果总是符合预期.

文献[69]基于TPCM对主动动态度量技术展开研究，指出受限于硬件设计及生产能力，TPCM所代表的计算部件、防护部件并存、共行的双系统体系架构的实现还存在较大困难，因此实验部分只进行了形式化验证及安全分析. 随着硬件生产技术能力的提升，满足TPCM双体系结构思想的基于可信根的渐进式并行可信执行环境架构被提出[70].

随着可信执行环境技术（Trusted Execution Environment, TEE）的快速发展及应用，基于TEE为防护部件提供隔离受保护的可信运行环境，同时度量组件为系统、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，为运行态的动态防护问题提供了一种新的解决思路.

文献[71]指出位于TEE[72]中的度量组件与其他目标应用程序（Target Application, TA）共享可信OS的上下文，任何TA被攻击都可能影响度量组件的安全性，因此提出将度量机制验证和证明部分迁移到一种类似Intel（SGX）的飞地环境中执行，称为Scanclave. vTSE[73]利用SGX的物理隔离性为虚拟可信根（virtual Trusted Platform Module, vTPM）实例提供可信运行环境，能够动态保护vTPM在运行过程中的代码及数据的机密性和完整性，但是该方案并未体现“动态性”.

大量研究表明，SGX面临着包括侧信道攻击[74]、内存越界访问等[75]在内的多种攻击威胁，通过攻击获得的敏感数据可以帮助攻击者绕过SGX提供的数据机密性保证[76]. 改造SGX实现双系统架构保证运行态可信存在以下不足：

（1）SGX自身架构局限性. Enclave处于用户态，自身无法执行系统调用，需要与不可信区域进行交互，无法保证计算部件与防护部件具备较强逻辑独立性，增大了安全风险（Enclave和Non-Enclave共享大量的系统资源[77]，导致SGX无法抵御侧信道攻击）.

（2）系统开销较大. 计算部件和防护部件串行执行，需要频繁进出Enclave. 文献[78-82]针对Ecall和Ocall间切换的开销测试数据显示，Ecall的开销大约为8 000个时钟周期，Ocall的开销大约为10 000个时钟周期，远远高于系统调用平均约150个时钟周期的性能开销.

TrustZone[83]是ARM对可信计算的硬件实现解决方案，其通过将系统软硬件资源划分为安全世界（Security World, SW）和普通世界（Normal World, NW），两个世界均具备独立的系统资源支持，为构建计算、防护并行运行且逻辑相互独立的双系统体系架构提供了新的解决思路. 相关研究表明[34,84−85]，可以利用TrustZone的安全机制提升度量组件的安全等级，防止作为信任锚点的度量、监控机制被绕过甚至被篡改.

综上所述，TrustZone的架构和机制更易于构建符合可信3.0思想的主动防御体系及计算与防护并行的双系统架构. 且从理论上而言，TrustZone中SW和NW通过总线进行通信，性能要优于SGX.

此外，也有其他学者结合主动免疫可信思想，提出基于基板管理控制器（Baseboard Management Controller,

BMC）的服务器动态度量相关方案[86−88]，BMC作为具有独立的处理器、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监测和控制，防护机制运行在BMC中能够实现“计算”和“防护”并行的双体系结构，有效提升系统安全性.

当前，用“可信计算筑牢网络安全防线”已成为国际主流，网络安全从被动防御向主动防御转变是技术发展的必要趋势. 中国自主创新的主动免疫可信计算新模式具备相当的理论及安全优势，值得期待的是随着可信计算领域的专家学者的努力，一系列软硬接口标准[10]逐渐完善，TPCM软硬件生态建设逐渐成熟. TPCM的工程化实现也初见曙光，其计算部件与防护部件相互分离、并行运行的架构优势以及其作为硬件可信根所具备的硬件级安全优势，能够为动态度量难题的解决提供可预期的美好前景. 相信未来，主动免疫可信计算在云计算、物联网等关乎国家基础设施安全的关键领域能够得到深层次广泛的应用.

2.3.2 对比分析

如表2所示，由于TEE本身架构的缺陷（易受侧信道攻击、安全区域可使用内存少等）及安全区域与正常区域切换所引入的性能开销，使得依赖TEE构建的双系统体系架构在保证应用运行态可信方面存在诸多不足. 随着具备主动度量功能且计算与防护架构并行的可信硬件（TPCM等）的发展，上述机制应互为补充，相互协调.

表 2 基于安全架构优先的动态度量机制对比

硬件机制	安全性	系统开销	主动性	实时监控能力	架构思想	缺陷
SGX	高	大	不具备	不具备	为度量监控部件构建隔离受保护的运行环境	增大开发难度，无法抵御侧信道攻击，可信关系建立在CPU而非信任根，且性能开销较大
TrustZone	高	小	具备	具备（度量监控机制支持下）	符合双系统体系架构思想	安全防护较为粗粒度，不能抵御物理攻击
TPCM	较高	较小	具备	具备	双系统体系架构	工程量化实现难，上下游生态不完善
BMC	高	小	具备	具备（度量监控机制支持下）	符合双系统体系架构思想	自身安全性不高

3 动态度量技术难题及未来解决方案

随着数字化转型的加速推进，各类重要信息系统朝着动态、分布式的方向转变，传统以静态完整性度量为核心的度量方法已不再适用. 虽然基于安全优先架构思想的动态度量方案相较于普通动态度量方案，提升了对防护部件自身安全性的保障，减少了度量引入的系统性能开销. 但从应用落地的角度出发，其安全性及性能有待提升，基于前述章节描述，动态度量技术面临的技术难题及相应的解决方案如下：

（1）“度量组件”自身安全性保障难题

理想情况下，以系统内核模块或应用层软件形式存在的“监控、度量逻辑”（简称为度量组件）是运行在基于可信根建立信任拓展关系的计算平台上，自身安全性能够得到有效保障（如不会被篡改或绕过等）. 然而在实际应用中，存在以下问题：1）信任链拓展会伴随着信任衰减，操作系统层或应用层的度量组件存在一定的安全风险；2）基于硬件可信根，利用可信启动构建的计算平台初始可信状态只能表明加载时刻度量行为的有效性，不能严格保证度量组件在后续运行过程中始终保证可信.

当前，随着攻击范式的快速迭代，一旦度量组件的可信性被破坏，建立在其上的相关安全防护措施的安全基础就不存在，度量结果不具任何意义. 中国自主创新的主动免疫可信计算新模式具备完备的理论及安全优势，随着推动主动免疫可信计算工程实际应用的TPCM标准的出台及部分可信计算厂商对TPCM芯片的工程实现，其计算部件与防护部件相互分离、并行运行的架构优势以及其作为硬件可信根所具备的硬件级安全优势，能够为动态度量架构安全性及提高度量效率等问题的解决提供可行的方案. 因此，为了避免度量组件自身的安全风险，考虑引入硬件辅助技术保证其安全性，如为度量组件构造可信执行环境（如TPCM、TrustZone、CPU安全核等），保证实施安全监控的相关逻辑代码无法被不可信内核篡改或绕过.

（2）安全性与业务连续性间的权衡难题

1）对于动态可信度量而言，较为理想的情况下是能够实时地对被度量对象（如重要信息系统、应用等）进

行度量，并依据度量结果进行高效的反馈控制. 但是高频率的可信度量在提高安全性的同时，也会引入较大的额外性能开销，系统或者应用的业务连续性会受到较大影响. 因此，度量点的合理分布及度量触发时机的合理设置显得尤为重要：

a. 现有方案设置度量点均需要修改源码，这可能会引入更为不可控的安全风险. 因此，应大力推动主动免疫可信在系统或应用运行生命周期全流程的参与，构建以“计算”+“防护”的双系统体系结构为基础，以可信软件基为核心，以可信代理为触点的主动免疫架构，无需修改应用程序，能够有效降低攻击面.

b. 选取合适的数学工具构建动态可信度量模型，并根据应用场景及安全需求的不同，动态设置相应的度量策略来保证度量时机触发的合理性，从而实现度量行为的有效性及度量引入的性能开销的可控性.

2）被度量对象的多层次、全面化分析在带来高安全性、细粒度的可信度量优势的同时，也带来两个难题：①当度量对象由静态转向动态，难以构造基准值域轮廓，被度量对象的精准评估较为困难；②全面化分析导致度量状态空间爆炸[89]. 根据所述，未来期望从如下三个方面解决问题：

a. 引入深度学习构建更为精准的系统预期动态行为模型：随着生成式人工智能的广泛应用，结合生成式人工智能对被度量对象行为进行动态建模及深度分析，并在系统运行过程中不断实时调整优化模型，建立能够反映被度量对象实时状态的约简后特征模型，推动可信度量机制朝着多元化、精确化评估体系迈进.

b. 引入边云协同理念，构建云、边、端多级联动的高效可信判定架构：如“云端学习，分级决策”：利用云端丰富的计算资源对行为进行建模，边缘侧对可信行为和异常行为进行实时判定，云端对敏感行为进行深度判定等.

c. 高效的行为评估模型：动态度量不可避免地引入较大的性能开销，尤其是当完整性度量转向针对运行态“行为”可信进行评估时，运行过程的动态性及复杂性所带来的行为多样性会导致性能开销剧增，未来可以考虑结合哈希树和链表等提高评估效率.

（3）动态区域敏感数据安全防护难题

系统运行过程中堆、栈等数据动态变化区域的可信度量是动态度量相关研究方案中较少涉及的领域. 为了更为精准地描述运行态安全，被度量对象从静态区域（如静态代码段、配置文件、链接库文件等）向动态区域转变是可信度量领域亟待解决的难题. 未来针对动态数据的安全防护应从多个层面入手，建立起多层次、多维度的立体安全防护体系：

1）信任锚点的建立：基于可信机制建立起可信启动、可信运行的完整信任链延伸，从而保证动态区域敏感数据拥有一个较为可信的可信前提.

2）引起动态区域敏感数据攻击行为的阻止：可以考虑系统调用行为及控制流行为监控技术与人工智能相结合的主体恶意行为鉴别技术，降低动态区域敏感数据泄露的风险.

3）引入动态追踪技术和污点追踪技术[90]，实现对运行态不可信数据的污点标记.

4）隔离防护：结合硬件防护机制为动态区域敏感数据提供隔离、受保护的可信运行环境.

4　总 结

没有网络安全就没有国家安全. 在当前社会高度数字化的“数智时代”，以数据和网络为核心的关键信息基础设施的安全是构筑国家安全防线的重要基础. 当前，使用可信计算技术构建新一代主动防护架构已成为广泛共识，在关乎国计民生的关键基础网络设施中，依据国家网络安全法律、战略、等级保护制度及网络安全产业发展规划的要求，推广可信计算技术在各领域深层次的应用，对重要信息系统进行动态可信验证，筑牢网络安全防线是极具意义的.

本文对可信动态度量进行了综述性研究及分析. 首先，对动态度量的应用背景及可信计算基础概念、可信定义进行了阐述. 其次，从动态度量的理论模型和工程实现两个方面对现有动态度量方案进行了详细阐述，并从保证被度量对象的全面性、度量点设置的低离散性、度量架构的安全性对所述方案进行了综合对比分析. 进而，基于前述分析对当前动态度量领域面临的技术难题进行了总结，并提出了相应解决思路.

希望通过本文的讨论、探索、思考及对应用新技术解决动态可信度量难题的展望，能够为动态可信度量的发展和应用开辟更加广阔的道路.

参考文献：

[1] IBRAHIM F A M，HEMAYED E E. Trusted cloud computing architectures for infrastructure as a service：Survey and systematic literature review[J]. Computers & Security，2019，82：196-226.

[2] CLARKE R A，KNAKE R K. Cyber war：The next threat to national security and what to do about it[M]. Pymble，Australia：Harper Collins Publishers，2010.

[3] 王勇，王钰茗，张琳，等. 乌克兰电力系统BlackEnergy病毒分析与防御[J]. 网络与信息安全学报，2017，3(1)：46-53.
WANG Y，WANG Y M，ZHANG L，et al. Analysis and defense of the BlackEnergy malware in the Ukrainian electric power system[J]. Chinese Journal of Network and Information Security，2017，3(1)：46-53. (in Chinese)

[4] 吕磅，韩嘉佳，孙歆，等. 基于深度神经网络的电力无线终端安全接入测试[J]. 浙江电力，2023，42(10)：101-106.
LYU B，HAN J J，SUN X，et al. Access security testing for wireless power terminals based on DNN[J]. Zhejiang Electric Power，2023，42(10)：101-106. (in Chinese)

[5] SU L X，LI Z Z，GOU G P，et al. Identifying exposed ICS remote management device using multimodal feature in the wild[C]//2023 IEEE International Performance，Computing，and Communications Conference (IPCCC). November 17-19，2023，Anaheim，CA，USA. IEEE，2023：220-227.

[6] 本报评论员. 没有网络安全就没有国家安全[N]. 解放军报，2018-04-23(1).
Our Commentator. Without cybersecurity，there can be no national security[N]. PLA Daily，2018-04-23(1). (in Chinese)

[7] 中华人民共和国国家互联网信息办公室. 国家网络空间安全战略(全文)[EB/OL]. (2016-12-27)[2024-06-06]. https://www.cac.gov.cn/2016-12/27/c_1120195926.htm.
Cyberspace Administration of China. National cyberspace security strategy (full text)[EB/OL]. (2016-12-27)[2024-06-06]. https://www.cac.gov.cn/2016-12/27/c_1120195926.htm. (in Chinese)

[8] 中华人民共和国国家互联网信息办公室. 中华人民共和国网络安全法[EB/OL]. (2016-11-07)[2024-06-08]. https://www.cac.gov.cn/2016-11/07/c_1119867116.htm.
Cyberspace Administration of China. Cybersecurity law of the People's Republic of China[EB/OL]. (2016-11-07)[2024-06-08]. https://www.cac.gov.cn/2016-11/07/c_1119867116.htm. (in Chinese)

[9] 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]. 北京：中国标准出版社，2019.
State Administration for Market Regulation，National Standardization Adminnistration. Standardization Administration of the People's Republic of China. Information security technology—baseline for classified protection of cybersecurity：GB/T 22239—2019[S]. Beijing：Standards Press of China，2019. (in Chinese)

[10] 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.
SHEN C X. To create a positive cyberspace by safeguarding network security with active immune trusted computing 3.0[J]. Journal of Information Security Research，2018，4(4)：282-302. (in Chinese)

[11] Communications Security Establishment，Communications-Electronics Security Group，Information Technology Promotion Agency，et al. Common criteria for information technology security evaluation：ISO/IEC 15408：1999[S]. California：SAGE Publishing，1999.

[12] AVIZIENIS A，LAPRIE J C，RANDELL B，et al. Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Transactions on Dependable and Secure Computing，2004，1(1)：11-33.

[13] 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.
SHEN C X，GONG B. The innovation of trusted computing based on the domestic cryptography[J]. Journal of Cryptologic Research，2015，2(5)：381-389. (in Chinese)

[14] 国家市场监督管理总局，国家标准化管理委员会. 信息安全技术可信计算规范可信软件基：GB/T 37935—2019[S]. 北京：中国标准出版社，2019.
State Administration for Market Regulation，National Standardization Adminnistration. Standardization Administration of the People's Republic of China. Information security technology—trusted computing specification—trusted software base：GB/T 37935—2019[S]. Beijing：Standards Press of China，2019. (in Chinese)

[15] 陈志锋，李清宝，张平，等. 基于内存取证的内核完整性度量方法[J]. 软件学报，2016，27(9)：2443-2458.
CHEN Z F，LI Q B，ZHANG P，et al. Kernel integrity measurement method based on memory forensic[J]. Journal of Software，2016，27(9)：2443-2458. (in Chinese)

[16] 潘传幸，张铮，马博林，等. 面向进程控制流劫持攻击的拟态防御方法[J]. 通信学报，2021，42(1)：37-47.

PAN C X，ZHANG Z，MA B L，et al. Method against process control-flow hijacking based on mimic defense[J]. Journal on Communications，2021，42(1)：37-47. (in Chinese)

[17] JIANG R，XIN Y，CHEN Z X，et al. A medical big data access control model based on fuzzy trust prediction and regression analysis[J]. Applied Soft Computing，2022，117：108423.

[18] 庄琇，蔡勉，沈昌祥. 基于交互式马尔可夫链的可信动态度量研究[J]. 计算机研究与发展，2011，48(8)：1464-1472.
ZHUANG L，CAI M，SHEN C X. Trusted dynamic measurement based on interactive Markov chains[J]. Journal of Computer Research and Development，2011，48(8)：1464-1472. (in Chinese)

[19] 罗新星，唐振宇，赵玉洁. 基于马尔可夫链的可信软件动态评估模型[J]. 计算机应用研究，2015，32(8)：2400-2405.
LUO X X，TANG Z Y，ZHAO Y J. Dynamic software reliability assessment based on Markov chain[J]. Application Research of Computers，2015，32(8)：2400-2405. (in Chinese)

[20] 李小勇，桂小林. 动态信任预测的认知模型[J]. 软件学报，2010，21(1)：163-176.
LI X Y，GUI X L. Cognitive model of dynamic trust forecasting[J]. Journal of Software，2010，21(1)：163-176. (in Chinese)

[21] 李小勇，桂小林，赵娟，等. 一种可扩展的反馈信任信息聚合算法[J]. 西安交通大学学报，2007，41(8)：879-883.
LI X Y，GUI X L，ZHAO J，et al. Novel scalable aggregation algorithm of feedback trust information[J]. Journal of Xi'an Jiaotong University，2007，41(8)：879-883. (in Chinese)

[22] 郁宁，王高才. 基于可信期望的跨域访问安全性研究[J]. 计算机应用研究，2020，37(11)：3406-3410+3416.
YU N，WANG G C. Study on cross-domain access security based on trusted expectations[J]. Application Research of Computers，2020，37(11)：3406-3410+3416. (in Chinese)

[23] 张帆，徐明迪，赵涵捷，等. 软件实时可信度量：一种无干扰行为可信性分析方法[J]. 软件学报，2019，30(8)：2268-2286.
ZHANG F，XU M D，ZHAO H J，et al. Real-time trust measurement of software：Behavior trust analysis approach based on noninterference[J]. Journal of Software，2019，30(8)：2268-2286. (in Chinese)

[24] 黄浩翔，张建标，袁艺林，等. 基于无干扰理论的虚拟机可信启动研究[J]. 软件学报，2023，34(6)：2959-2978.
HUANG H X，ZHANG J B，YUAN Y L，et al. Research on trusted startup of virtual machine based on non-interference theory[J]. Journal of Software，2023，34(6)：2959-2978. (in Chinese)

[25] SAILER R，ZHANG X，JAEGER T，et al. Design and implementation of a TCG-based integrity measurement architecture[C]//Proceedings of the 13th USENIX Security Symposium. San Diego，CA，USA. USENIX Association. 2004：1-16.

[26] 刘孜文，冯登国. 基于可信计算的动态完整性度量架构[J]. 电子与信息学报，2010，32(4)：875-879.
LIU Z W，FENG D G. TPM-based dynamic integrity measurement architecture[J]. Journal of Electronics & Information Technology，2010，32(4)：875-879. (in Chinese)

[27] JAGER E T，SAILER R，SHANKAR U. Policy-reduced integrity measurement architecture (PRIMA)[C]//Proceedings of 11th ACM Symposium on Access Control Models and Technologies. New York，USA. 2006：19-28.

[28] PETRONI Jr N L，FRASER T，MOLINA J，et al. Copilot-a coprocessor-based kernel runtime integrity monitor[C]//Proceedings of the International Conference. San Diego，CA，USA. USENIX Association. 2004：1-8.

[29] PETRONI N L Jr，HICKS M. Automated detection of persistent kernel control-flow attacks[C]//Proceedings of the 14th ACM Conference on Computer and Communications Security. Alexandria Virginia USA. ACM，2007：103-115.

[30] SHI E，PERRIG A，VAN DOORN L. BIND：A fine-grained attestation service for secure distributed systems[C]//2005 IEEE Symposium on Security and Privacy (S&P'05). Oakland，CA，USA. IEEE，2005：154-168.

[31] DONG S W，XIONG Y，HUANG W C，et al. KIMS：Kernel integrity measuring system based on TrustZone[C]//2020 6th International Conference on Big Data Computing and Communications (BIGCOM). Deqing，China. IEEE，2020：103-107.

[32] 吴远. Windows应用程序的可信度量技术研究与实现[D]. 南京：南京理工大学，2012.
WU Y. Research and Implementation of Trust Measurement Technology for Windows Applications[D]. Nanjing：Nanjing University of Science and Technology，2012. (in Chinese)

[33] 吴涛，杨秋松，贺也平. 基于邻接点的VMM动态完整性度量方法[J]. 通信学报，2015，36(9)：169-180.
WU T，YANG Q S，HE Y P. Method of dynamic integrity measurement for VMM based on adjacency data[J]. Journal on Communications，2015，36(9)：169-180. (in Chinese)

[34] 蔡梦娟，陈兴蜀，金鑫，等. 基于硬件虚拟化的虚拟机进程代码分页式度量方法[J]. 计算机应用，2018，38(2)：305-309+315.
CAI M J，CHEN X S，JIN X，et al. Paging-measurement method for virtual machine process code based on hardware virtualization[J]. Journal of Computer Applications，2018，38(2)：305-309+315. (in Chinese)

[35] VADUVA J A, DASCALU S, FLOREA I M, et al. Observations over SPROBES mechanism on the TrustZone architecture[C]//2019 22nd International Conference on Control Systems and Computer Science (CSCS). Bucharest, Romania. IEEE, 2019: 317-322.

[36] 汪自旺, 庄毅, 晏祖佳. 一种移动安全域动态完整性度量方案[J]. 小型微型计算机系统, 2021, 42(11): 2422-2427.
WANG Z W, ZHUANG Y, YAN Z J. Probe-based dynamic integrity measurement scheme for mobile devices using ARM TrustZone[J]. Journal of Chinese Computer Systems, 2021, 42(11): 2422-2427. (in Chinese)

[37] GE X Y, VIJAYAKUMAR H, JAEGER T. Sprobes: Enforcing kernel code integrity on the TrustZone architecture[J]. Procedia Computer Science, 2014: 1793-1795.

[38] PETER A L, MCGILL K N. LKIM: The Linux kernel integrity measurer[J]. Johns Hopkins APL Technical Digest, 2013, 32(2): 509-516.

[39] JOY J, JOHN A, JOY J. Rootkit detection mechanism: A survey[C]// Advances in Parallel Distributed Computing. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011: 366-374.

[40] ABIJAH ROSELINE S, GEETHA S. A comprehensive survey of tools and techniques mitigating computer and mobile malware attacks[J]. Computers & Electrical Engineering, 2021, 92: 107143.

[41] JUNNILA J. Effectiveness of Linux rootkit detection tools[D]. Oulu: University of Oulu, 2020.

[42] LI Y G, CHUNG Y C, HWANG K, et al. Virtual wall: Filtering rootkit attacks to protect Linux kernel functions[J]. IEEE Transactions on Computers, 2021, 70(10): 1640-1653.

[43] BUCHANAN E, ROEMER R, SHACHAM H, et al. When good instructions go bad: Generalizing return-oriented programming to RISC[C]//Proceedings of the 15th ACM Conference on Computer and Communications Security. Alexandria Virginia USA. ACM, 2008: 27-38.

[44] BLETSCH T, JIANG X X, FREEH V W, et al. Jump-oriented programming: A new class of code-reuse attack[C]//Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. Hong Kong, China. ACM, 2011: 30-40.

[45] 李晓勇, 左晓栋, 沈昌祥. 基于系统行为的计算平台可信证明[J]. 电子学报, 2007, 35(7): 1234-1239.
LI X Y, ZUO X D, SHEN C X. System behavior based trustworthiness attestation for computing platform[J]. Acta Electronica Sinica, 2007, 35(7): 1234-1239. (in Chinese)

[46] MAGGI F, MATTEUCCI M, ZANERO S. Detecting intrusions through system call sequence and argument analysis[J]. IEEE Transactions on Dependable and Secure Computing, 2010, 7(4): 381-395.

[47] FORREST S, HOFMEYR S A, SOMAYAJI A, et al. A sense of self for unix processes[C]//Proceedings 1996 IEEE Symposium on Security and Privacy. Oakland, CA, USA. IEEE, 1996: 120-128.

[48] HOFMEYR S A, FORREST S, SOMAYAJI A. Intrusion detection using sequences of system calls[J]. Journal of Computer Security, 1998, 6(3): 151-180.

[49] 蔡洪波, 单征, 范超, 等. 基于非定长系统调用序列的程序行为动态度量方法[J]. 计算机应用研究, 2016, 33(4): 1154-1158.
CAI H B, SHAN Z, FAN C, et al. Dynamic measurement of program behavior based on variable-length system call sequence[J]. Application Research of Computers, 2016, 33(4): 1154-1158. (in Chinese)

[50] LI H, SHAN Z, CHAO F, et al. A model of short sequence matching and Markov estimating on behavior recognition for anomaly detection[J]. International Journal of Advancements in Computing Technology, 2014, 6(1): 106.

[51] 杨维永, 刘苇, 崔恒志, 等. SG-Edge: 电力物联网可信边缘计算框架关键技术[J]. 软件学报, 2022, 33(2): 641-663.
YANG W Y, LIU W, CUI H Z, et al. SG-edge: Key technology of power internet of things trusted edge computing framework[J]. Journal of Software, 2022, 33(2): 641-663. (in Chinese)

[52] MARICONTI E, ONWUZURIKE L, ANDRIOTIS P, et al. MaMaDroid: Detecting Android malware by building Markov chains of behavioral models[C]//Proceedings 2017 Network and Distributed System Security Symposium. San Diego, CA. Internet Society, 2017: 1-34.

[53] WAGNER D, DEAN R. Intrusion detection via static analysis[C]//Proceedings 2001 IEEE Symposium on Security and Privacy. Oakland, CA, USA. IEEE, 2001: 156-168.

[54] GIFFIN J T, JHA S, MILLER B P. Detecting manipulated remote call streams[C]//11th USENIX Security Symposium (USENIX Security 02). San Francisco, CA, USA. 2002: 1-19.

[55] GENS D, SCHMITT S, DAVI L, et al. K-miner: Uncovering memory corruption in Linux[C]//Proceedings 2018 Network and Distributed System Security Symposium. San Diego, CA. Internet Society, 2018: 1-15.

[56] FELT A P，CHIN E，HANNA S，et al. Android permissions demystified[C]//Proceedings of the 18th ACM Conference on Computer and Communications Security. Chicago Illinois USA. ACM，2011：627-638.

[57] DAWOUD A，BUGIEL S. Bringing balance to the force：Dynamic analysis of the Android application framework[C]//Proceedings 2021 Network and Distributed System Security Symposium. Virtual. Internet Society，2021：1-18.

[58] SHANG W L，XING X Y. ICS software trust measurement method based on dynamic length trust chain[J]. Scientific Programming，2021：6691696.

[59] 刘晗，李凯旋，陈仪香. 人工智能系统可信性度量评估研究综述[J]. 软件学报，2023，34(8)：3774-3792.
LIU H，LI K X，CHEN Y X. Survey on trustworthiness measurement for artificial intelligence systems[J]. Journal of Software，2023，34(8)：3774-3792. (in Chinese)

[60] 秦臻，庄添铭，朱国淞，等. 面向人工智能模型的安全攻击和防御策略综述[J]. 计算机研究与发展，2024，61(10)：2627-2648.
QIN Z，ZHUANG T M，ZHU G S，et al. Survey of security attack and defense strategies for artificial intelligence model[J]. Journal of Computer Research and Development，2024，61(10)：2627-2648. (in Chinese)

[61] ABUTU G，WEISSMAN D，HOFFMANN P，et al. DeepCodeLock：A novel deep learning-based approach for automated ransomware detection using behavioral signatures[EB/OL]. (2024-11-01)[2025-06-23]. https://d197for5662m48.cloudfront.net/documents/publicationstatus/230298/preprint_pdf/ea6b2b3cfa90784e39a283a63acf0a39.pdf.

[62] DAS S，LIU Y，ZHANG W，et al. Semantics-based online malware detection：Towards efficient real-time protection against malware[J]. IEEE Transactions on Information Forensics and Security，2016，11(2)：289-302.

[63] MENG Q，WANG X M，YANG K，et al. Research on intrusion tolerance system based on behavioral baseline and defense-in-depth architecture[C]//International Conference on Mechatronics and Intelligent Control (ICMIC 2024). Wuhan，China. SPIE，2025：1-13.

[64] CONG S，ZHAN K L，LIANG C，et al. Digital currency features oriented fine-grained code injection attack detection[J]. Journal of Computer Research and Development，2021，58(5)：1035.

[65] MENG D，HOU R，SHI G，et al. Security-first architecture：Deploying physically isolated active security processors for safeguarding the future of computing[J]. Cybersecurity，2018，1(1)：2.

[66] 沈昌祥，田楠. 按“等保2.0”用主动免疫可信计算筑牢“新基建”网络安全防线[J]. 信息安全与通信保密，2020，18(10)：2-9.
SHEN C X，TIAN N. Building a “new infrastructure” network security defense line with active immune trusted computing according to “equal security 2.0”[J]. Information Security and Communications Privacy，2020，18(10)：2-9. (in Chinese)

[67] 王晓，张建标，曾志强. 基于可信平台控制模块的可信虚拟执行环境构建方法[J]. 北京工业大学学报，2019，45(6)：554-565.
WANG X，ZHANG J B，ZENG Z Q. Construction method of trusted virtual execution environment based on trusted platform control module[J]. Journal of Beijing University of Technology，2019，45(6)：554-565. (in Chinese)

[68] 芮志清，梅瑶，陈振哲，等. SeChain：基于国密算法的RISC-V安全启动机制设计与实现[J]. 计算机研究与发展，2024，61(6)：1458-1475.
RUI Z Q，MEI Y，CHEN Z Z，et al. SeChain：Design and implementation of RISC-V secure boot mechanism based on domestic cryptographic algorithms[J]. Journal of Computer Research and Development，2024，61(6)：1458-1475. (in Chinese)

[69] 田健生，詹静. 基于TPCM的主动动态度量机制的研究与实现[J]. 信息网络安全，2016，16(6)：22-27.
TIAN J S，ZHAN J. Research and implementation of active dynamic measurement based on TPCM[J]. Netinfo Security，2016，16(6)：22-27. (in Chinese)

[70] 黄坚会，张江江，沈昌祥，等. 基于TPCM可信根的双体系可信终端计算架构[J]. 通信学报，2025，46(4)：1-14.
HUANG J H，ZHANG J J，SHEN C X，el at. Dual system trusted terminal computing architecture based on TPCM-RoT[J]. Journal on Communications，2025，46(4)：1-14. (in Chinese)

[71] MORBITZER M. Scanclave：Verifying application runtime integrity in untrusted environments[C]//2019 IEEE 28th International Conference on Enabling Technologies：Infrastructure for Collaborative Enterprises (WETICE). Napoli，Italy. IEEE，2019：198-203.

[72] 冯登国，刘敬彬，秦宇，等. 创新发展中的可信计算理论与技术[J]. 中国科学：信息科学，2020，50(8)：1127-1147.
FENG D G，LIU J B，QIN Y，et al. Trusted computing theory and technology in innovation-driven development[J]. Science in China (Information Sciences)，2020，50(8)：1127-1147. (in Chinese)

[73] 严飞，于钊，张立强，等. vTSE：一种基于SGX的vTPM安全增强方案[J]. 工程科学与技术，2017，49(2)：133-139.
YAN F，YU Z，ZHANG L Q，et al. vTSE：A solution of SGX-based vTPM secure enhancement[J]. Advanced Engineering

Sciences，2017，49(2)：133-139. (in Chinese)

[74] VANOVERLOOP D，SÁNCHEZ A，TOFFALINI F，et al. TLBlur：Compiler-assisted automated hardening against controlled channels on off-the-shelf intel SGX platforms[EB/OL]. (2024-07-02)[2024-07-05]. http://nebelwelt.net/files/25SEC.pdf.

[75] KUMAR S，PANDA A，NERLIKAR A，et al. A tug-of-war between static and dynamic memory in intel SGX[C]//2025 38th International Conference on VLSI Design and 2024 23rd International Conference on Embedded Systems (VLSID). Bangalore，India. IEEE，2025：272-277.

[76] 赵波，袁安琪，安杨. SGX在可信计算中的应用分析[J]. 网络与信息安全学报，2021，7(6)：126-142.
ZHAO B，YUAN A Q，AN Y. Application progress of SGX in trusted computing area[J]. Chinese Journal of Network and Information Security，2021，7(6)：126-142. (in Chinese)

[77] 董春涛，沈晴霓，罗武，等. SGX应用支持技术研究进展[J]. 软件学报，2021，32(1)：137-166.
DONG C T，SHEN Q N，LUO W，et al. Research progress of SGX application supporting techniques[J]. Journal of Software，2021，32(1)：137-166. (in Chinese)

[78] ZAHID M J S. Integration of intel SGX with confidential measurement control for enhanced remote attestation[J]. Authorea Preprints，2025：1-10.

[79] WEISSE O，BERTACCO V，AUSTIN T. Regaining lost cycles with HotCalls：A fast interface for SGX secure enclaves[C]//2017 ACM/IEEE 44th Annual International Symposium on Computer Architecture (ISCA). Toronto，ON，Canada. IEEE，2017：81-93.

[80] TIAN H L，ZHANG Q，YAN S M，et al. Switchless calls made practical in intel SGX[C]//Proceedings of the 3rd Workshop on System Software for Trusted Execution. Toronto Canada. ACM，2018：22-27.

[81] WANG Z Y，ZHOU Y Z. Analysis and evaluation of intel software guard extension-based trusted execution environment usage in edge intelligence and internet of things scenarios[J]. Future Internet，2025，17(1)：32.

[82] WEICHBRODT N，AUBLIN P L，KAPITZA R. SGX-perf：A performance analysis tool for intel SGX enclaves[C]//Proceedings of the 19th International Middleware Conference. Rennes France. ACM，2018：201-213.

[83] JIAN Z L，LIU X，DONG Q K，et al. SmartZone：Runtime support for secure and efficient on-device inference on ARM TrustZone[J]. IEEE Transactions on Computers，2025，74(6)：2144-2158.

[84] BUSCH M，MAO P，PAYER M. Global confusion：TrustZone trusted application 0-days by design[C]//Proceedings of the 33rd USENIX Security Symposium. Philadelphia，PA，USA. IEEE，2024：24SEC4.

[85] GOES C，SOUSA J，NETO J B，et al. Key-encapsulation mechanisms embedded in trusted execution environment：An evaluation[C]//2025 IEEE International Conference on Consumer Electronics (ICCE). Las Vegas，NV，USA. IEEE，2025：1-6.

[86] 徐万山，张建标，袁艺林，等. 基于BMC的服务器可信启动方法研究[J]. 信息网络安全，2021，21(5)：67-73.
XU W S，ZHANG J B，YUAN Y L，et al. Research on trusted server startup method based on BMC[J]. Netinfo Security，2021，21(5)：67-73. (in Chinese)

[87] 孙亮，陈小春，钟阳，等. 基于可信BMC的服务器安全启动机制[J]. 山东大学学报(理学版)，2018，53(1)：89-94.
SUN L，CHEN X C，ZHONG Y，et al. Secure start up mechanism of server based on trusted BMC[J]. Journal of Shandong University(Natural Science)，2018，53(1)：89-94. (in Chinese)

[88] 苏振宇. 基于国产BMC的服务器安全启动技术研究与实现[J]. 信息安全研究，2017，3(9)：823-831.
SU Z Y. Research and implementation of secure boot technology for server based on domestic BMC[J]. Journal of Information Security Research，2017，3(9)：823-831. (in Chinese)

[89] 庄琭，沈昌祥，蔡勉. 基于行为的可信动态度量的状态空间约简研究[J]. 计算机学报，2014，37(5)：1071-1081.
ZHUANG L，SHEN C X，CAI M. Research on state space reduction of behavior-based trusted dynamic measurement[J]. Chinese Journal of Computers，2014，37(5)：1071-1081. (in Chinese)

[90] SANG Q，WANG Y H，LIU Y W，et al. AirTaint：Making dynamic taint analysis faster and easier[C]//2024 IEEE Symposium on Security and Privacy (SP). San Francisco，CA，USA. IEEE，2024：3998-4014.

责任编辑：刘 敏