

# 面向云服务信息安全评估的度量模型研究

陆月明, 张志辉

(北京邮电大学信息与通信工程学院, 北京 100876)

**摘要:** 针对云服务信息安全缺乏度量准则和度量不准的问题, 介绍了国内外相关度量标准的研究现状。针对可信云的信息安全度量需求, 总结了基于可信根的度量模型的优缺点, 指出未来的方向是一个兼顾可扩展性、实时性、隐私保护好、易移植且开销更小的云服务信息安全度量模型。

**关键词:** 可信云服务; 信息安全评估; 度量模型; 评估标准

**中图分类号:** TP393

**文献标识码:** A

**doi:** 10.11959/j.issn.2096-109x.2016.00075

## Research on metrics models for cloud services information security evaluation

LU Yue-ming, ZHANG Zhi-hui

(School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China)

**Abstract:** Due to the lack of metric standards and the metric imprecise problems of cloud service information security, the research status of the relevant standards at home and abroad were introduced. As for the demand for information security measurement requirements of the trusted cloud, the advantages and disadvantages of metric models based on the trusted root were analyzed. At last, the future research direction which was to study a scalable combined, real-time, privacy protected, easy to transplant and less cost metrics model was pointed out.

**Key words:** trusted cloud services, information security assessment, metrics model, evaluation criteria

### 1 引言

针对 IT 领域计算资源集约化、规模化和专业化的需求, 云计算 (cloud computing)<sup>[1]</sup> 的计算模式应运而生。云服务服务一方面不断提高生产效率, 但同时也暴露出各种不容小觑的信息安全问题, 这已经成为阻碍其发展的关键因素。要解决云服务信息安全问题, 首先提出其信息安全检测、度量、评估等模型或方法, 形成良性反馈机制, 促进和提高云服务信息安全质量。然而, 云服务信息安全评估面临诸多难题, 由于没有完备的评估标准和指标, 面临信息安全评估不了和评估不准的问题。

### 2 现有信息安全评估标准及面临的挑战

现有信息安全评估标准主要被信息产品或服务的用户、开发者、第三方评估者、管理员等使用, 涉及的信息产品和服务门类广, 部分还对特定产品给出信息安全评估标准。最常用的是信息技术安全性评估准则 (CC, common criteria), 简称“通用准则”。

通用准则是确定适用于一切 IT 安全产品和系统的评估准则, 具有普适性和通用性。通用准则只规定准则, 不涉及评估方法, 评估方法的选择留给其他的评估体制确定。通用准则提出了 3 个重要概念, 评估对象 (TOE, target of evalua-

tion)、保护轮廓(PP, protection profile)和安全目标(ST, security target)。TOE 包括作为评估主体的 IT 产品和系统以及相关文档。PP 和 ST 是用于描述待评估 IT 产品或系统的重要文档。PP 描述满足特定需求且独立于现实的一组安全要求,是目标说明。ST 描述依赖于现实的一组安全说明,是评估基础。通用准则由简介与一般模型、安全功能要求、安全保证要求这 3 部分组成,将信息安全的三性(保密性、完整性和可用性)作为整个准则的出发点。其中,安全功能要求提出了 11 个需要满足安全要求的功能组件类<sup>[2]</sup>,包括密码支持、用户数据保护、私密性等。安全保证要求提出了 9 个需要安全保证的类别<sup>[3]</sup>,包括生命周期支持、脆弱性评定、指导性文档等。安全功能要求和安全保证要求为云服务信息安全评估指标的拟定提供了全面的依据。

2000 年 7 月,美国 NIST (National Institute of Standards and Technology) 和 CSSPAB (Computer System Security and Privacy Advisory Board) 联合举办了一个针对安全度量的讨论会。该会议指出,通用准则虽然在指导安全评估方面是个很好的标准,但在全面解决安全度量问题方面还有很多需要进一步研究的内容<sup>[4]</sup>,包括信息安全度量定义、信息系统的安全度量、针对特定安全威胁的安全度量、定性的安全度量、大规模网络中的实时安全度量、安全度量

和保证等级等之间的关系,从而使人们对安全保护能有一个更加深刻的理解。

### 3 云服务安全度量模型及指标

2009 年 4 月,RSA 大会成立了云安全联盟 CSA (cloud security alliance),致力于云服务安全解决方案,发布了《云计算关键领域安全指南》<sup>[5]</sup>,从攻击者角度归纳云服务可能有账户或服务劫持、数据丢失或泄露、不安全 API、恶意内部人员等风险。

#### 3.1 云服务信息安全度量和评估框架

云服务信息安全可以从不同的角度确定其度量框架,这里只从评估者角度确定这种分布式系统或服务的信息安全度量框架。图 1 给出了云服务信息安全度量和评估框架。该框架首先对云服务信息安全功能进行形式化,分成不同的信息安全功能类和族,抽象出族中的组件和依赖关系,并确定功能元素。针对信息安全可测要求,提出功能元素的量化方法和指标基准,最终形成标准,提供给评估者,解决云服务信息安全评估中评估不了和评估不准的问题。

在这个框架中,关键点在于信息安全度量模型能否全面形式化云服务的信息安全功能要求。模型形式化中的遗漏内容,包括认证等重要功能类,会导致信息安全上的缺陷。形式化中的错误依赖关系,包括信任传递等重要功能内容,会导致信息安全上存在后门。所以,云服务信息安全功能形式化是度量模型中的核心。

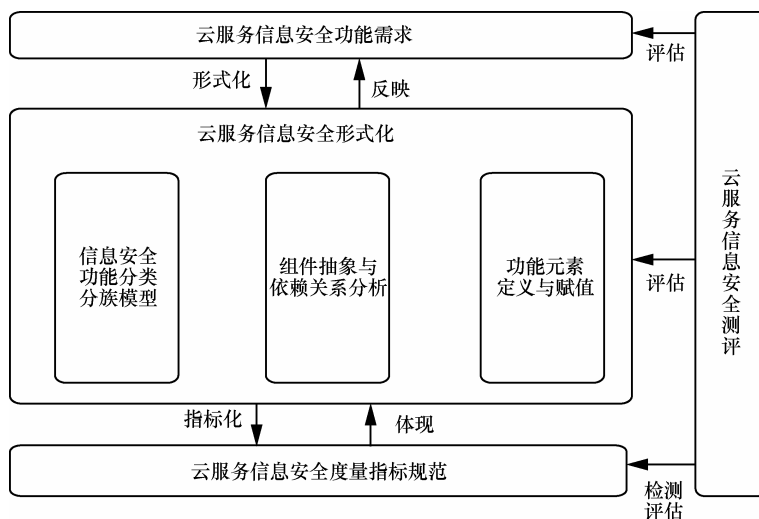


图 1 云服务信息安全度量和评估框架

由于云服务涉及计算资源、存储资源、进程等实体的信息安全，在云服务信息安全功能形式化中，对每个实体建立独立的度量模型，在实体之间建立信任和安全功能的传递，可以评估整个分布式系统的信息安全。

云服务信息安全功能形式化后，产生信息安全的度量指标，包括加密、鉴别等，作为整个模型的输出。测评者能够对这些度量指标进行基准测试和量化，实现信息安全的可测量、可重复、可比较等。下面介绍几种云服务信息安全形式化和具体的度量模型。

### 3.2 可信云服务信息安全形式化

可信是云服务中重要的信息安全功能类<sup>[6]</sup>，这里主要讨论可信度量模型，其主要包括的内容如下。

#### 1) 身份验证与访问控制

身份认证是所有信息服务类产品均要面对的问题。身份认证不仅是对云租户的认证，也是对云服务商的认证，是一种双向认证机制。此外，租户无法判断云服务供应商是否完全忠诚地执行了其设定的操作，因此应该对数据进行访问控制。

#### 2) 物理完整性

物理完整性是指支撑云服务硬件的物理安全及环境安全。云服务供应商应该保证硬件被置于相对安全稳定的环境，具有应对自然灾害的能力。通常出于节约成本与安全的考虑，云服务硬件被安置在较偏远地区。另外，最终交付云租户的服务不应含有未授权的后门。

#### 3) 数据完整性

云服务供应商应对租户数据进行完整性保

护的首选措施是加密存储，但这也带来一系列问题。比如，加密存储后如何对数据进行快速检索。为节省存储空间，云服务供应商会自动删除重复数据，加密后如何对数据去冗余化操作？当某租户合约期满后，云服务供应商会删除其存储在云上的数据，但这种数据删除措施不一定是不可恢复的。当下一位租户访问这块存储区域时，有可能会恢复该存储区的数据，云服务商应该采取适当措施避免这种情形的发生。数据完整性保护还应该解决的一个问题是数据存在性证明。存储在云端的数据是海量的，用户如何在有限带宽下通过接收少量数据便可确认其数据仍然是有效的？这也是需要解决的问题。

#### 4) 容错性与容侵性

虚拟化技术是服务的核心。云端存在很多租户，云服务供应商应该保证各租户之间是完全隔离的，避免不良租户利用云服务漏洞对其他租户实施攻击。分布式拒绝服务（DDoS, distributed denial of service）是一种司空见惯的网络攻击模式，云服务如何抵御这些网络攻击？

### 3.3 基于可信根的链式度量模型

可信根是构建可信系统的基础模块，可信计算组织（TCG, trusted computing group）将其划分为可信度量根（RTM）、可信存储根（RTS）、可信报告根（RTR）这3种基本类型，它们负责完成TCG的度量、存储、报告机制。一般默认这3个可信根都是绝对可信的。TCG给出的基于可信根的信任链参考模型如图2所示。

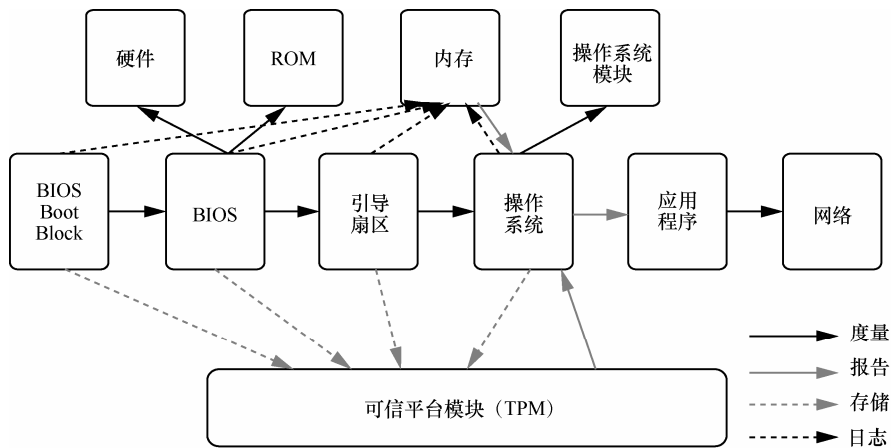


图2 基于可信根的信任链参考模型

文献[7]给出了基于可信根的信任链传递和控制权转移过程,如图3所示。其中,可信平台构造模块(TBB, trusted building blocks)是信任源,由软件可信度量根核(CRTM, core root of trust for measurement)和硬件模块TPM(trusted platform module)构成。第1、3、5步进行完整性度量,第2、4、6步转交执行权限。系统通电启动后,信任边界最初仅限于信任度量根核CRTM,完整性度量从此处开始。沿着信任链目标模块被验证通过后,执行权限被转移到该模块,同时信任边界也被拓展到该模块。在整个度量过程中,信任边界逐级拓展到整个系统而不仅仅局限于信任度量根。

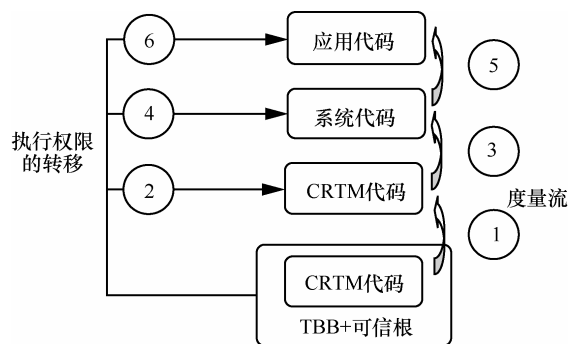


图3 基于可信根的信任链传递和控制权转移过程

TCG采用了一种迭代计算散列值的方式完整可信度量,并称其为“扩展”操作。即将平台配置寄存器(PCR, platform configuration regis-

ters)中的可信度量值与新的可信度量值连接之后,再次计算散列值并将其作为新的完整性度量值存储到寄存器中。这种迭代计算的“扩展”操作,使PCR中所存储的可信度量值不仅能够反映当前度量的软件完整性,也能够反映计算机系统的启动序列。当应用程序的完整性或计算机系统启动序列发生任何改变时,都将引起存储到寄存器中的可信度量值产生相应的变化。

综上,TCG提出的基于可信根的链式度量模型将硬件与软件相结合,能够有效地实现可信度量,且易实现。但由于需要硬件,一定程度上增加了度量成本。

### 3.4 可信静态度量

2004年,IBM在文献[8]中提出IMA(integrity measurement architecture)架构,其度量的关注点是基于TCG的完整性度量思路,侧重对各种软件代码和文件的完整性度量,度量时刻是在加载到内存时进行的,并通过TPM来进行保护。IMA度量机制主要由以下3个组件组成(如图4所示)。

#### 1) 度量组件

该组件决定运行环境中的3W问题,即什么部件需要被度量、什么时候度量、如何安全存储度量报告。度量方法采用SHA1计算散列值。

#### 2) 完整性挑战组件

该组件允许被授权的挑战者(云租户)发起完整性度量请求,准确无误地接收云计算平台的

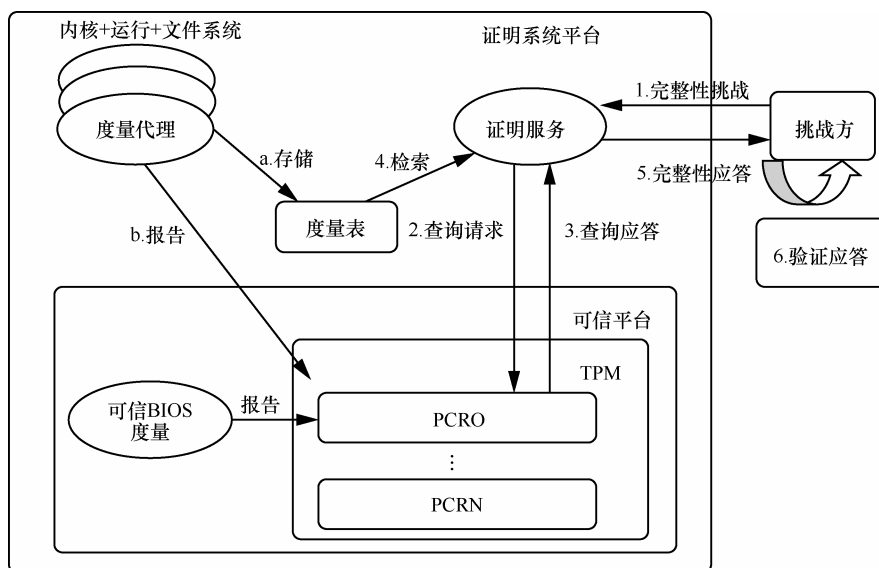


图4 IMA 远程证明

度量报告，并证明其完整性。

### 3) 完整性验证组件

该组件不仅能够证明反馈给挑战者的度量报告是完整的、无篡改的、实时的，而且证明测量报告中记录的云平台运行环境下的受信代码和配置文件均是有效的。

图4表明了该机制支持远程证明 (remote attestation) 的原理。度量代理初始化整个度量过程，并由它生成完整性度量报告，步骤a将完整性度量报告存入内核的度量队列里，步骤b将度量报告给TPM。完整性挑战机制允许远程挑战者发起完整性度量请求 (步骤1)。证明系统接收到完整性证明请求后，向TPM可信平台查询保存在RSA签名算法中私钥签名的PCR值，可信平台将查询结果反馈给证明系统 (步骤2和步骤3)。随后，内核也将度量报告返回给证明系统 (步骤4)。证明系统将度量报告及私钥签名一并发送给挑战方 (步骤5)。挑战方利用度量报告重新计算PCR值，然后与获得的PCR值比较，以此来证明平台的完整性是否遭到破坏 (步骤6)。

IMA是静态加载时的度量，但不能准确反映运行时的动态可变行为，易发生TOCTTOU (time of check to time of use) 一致性问题，而且IMA度量是在程序加载到内存时进行的，导致系统运行效率较低。对此，文献[9]提出可信动态度量模型，即PRIMA (policy-reduced integrity measurement architecture) 信息流度量。PRIMA度量

进程间的信息流，从本质上来说，PRIMA仅是IMA度量的改进，仍然是静态度量模型，并未解决TOXTTOU问题。

### 3.5 动态完整性度量

静态完整性度量一个显而易见的缺点是软件加载后便无法控制系统的完整性，这是因为它是在软件加载前进行完整性度量。与之相对应的是动态完整性度量，它是指在任意时刻都可以在对正在运行中的模块进行度量，在软件运行的整个生命周期内都可以控制系统的完整性。

文献[10]提出针对Linux内核的完整性监视器 (LKIM, Linux kernel integrity measurement)。该度量模型由度量对象、度量代理MA和决策体构成。LKIM利用基于上下文检测技术度量内核组件，不仅可以详细记录内核里与安全相关组件的状态，而且可以扩展到内核外组件的度量。此外，LKMI不仅是在系统启动的时候度量，而且可以响应来自IMS的度量请求和系统事件。度量数据以一种友好的方式存储，以便IMS随时查询原始数据。在系统安全政策的保护下，IMS不仅自身可以使用度量数据，而且可以根据指定度量脚本的要求将度量数据在任意节点间转移。

LKIM简化后的框架如图5所示。LKMI根据度量变量集合将度量程序分解为一系列独立的度量单元，并独立监测它们。LKMI的一个缺陷是不好把握监控粒度。如果度量单元划分的太细

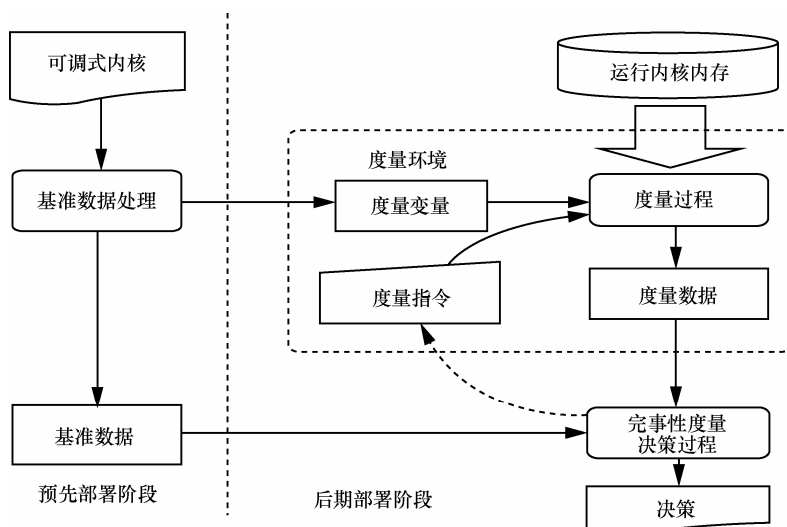


图5 LKIM简化框架

致，将影响系统的性能，监控起来也会很繁杂。反之，可能会无法捕捉到某些执行结果。虽然 LKMI 度量模型是在 Linux 内核下实现的，但其度量技术具有普适性，完全可以应用于需要被度量的其他类型的操作系统或复杂软件系统。

### 3.6 TOCTTOU 问题

为了解决 TOCTTOU 问题，文献[11]提出 HIMA (hypervisor-based integrity measurement agent)。HIMA 是基于 Hypervisor 的完整性度量代理，对用户虚拟机进行类似黑盒测试的综合性度量，度量对象包括虚拟机内核和用户程序。即使是在用户虚拟机内核被盗用的情况下，HIMA 不仅能保证用户程序静态完整性度量时的 TOCTTOU 一致性，也能保证度量程序的完整性。HIMA 主要使用以下 2 种技术来解决度量时可能发生的 TOCTTOU 一致性问题。

#### 1) 主动监控危险的用户事件

当用户创建新的线程或其他操作导致内存配置改变时，通过对加载到内存的代码和数据段进行散列计算来度量完整性。

#### 2) 用户内存保护

确保对用户任何程序的完整性度量不会被度量代理忽略。通过访问权限限制来保护用户内存，并使用测试虚拟域内存地址的散列方法来度量页映射中发生的安全问题。

HIMA 构架如图 6 所示，HIMA 将钩子程序植入 Hypervisor 代码，这样便可以拦截用户的以下操作：一些敏感服务器请求（如超级调用、VMExit 指令）、系统调用、硬件中断。为了方便远程证明，将生成的度量报告列表存储在管理员虚拟机中。HIMA 度量代理和 TOE 之间是完全隔离的，对于用户虚拟机来说完全透明，可以被移植于任何虚拟机监控平台。虽然可以通过虚拟化技术实现隔离，但度量技术绝不能依托于任何一个可以通过入侵易受攻击的客户就能将其破坏的组件或钩子程序。

文献[11]仅仅关注用户虚拟机静态部分的度量，没有考虑对动态生成的代码（如 Java JIT 编译器在堆上生成的可执行代码）的度量。然而，对动态数据完整性度量也是系统完整性度量的重要指标。此外，HIMA 仅仅是一个度量代理，需要依托于一个度量框架。

### 3.7 基于上下文语境的度量

在 Hypervisor 完整性度量方面，文献[12]提出 HyperSentry 度量模型，这是一个隐密的基于上下文语境的完整性度量模型，通过设计安全硬件增强 Hypervisor 完整性。

事实上，HyperSentry 并不关注于完整性度量本身，而是为完整性度量代理提供技术支持，使

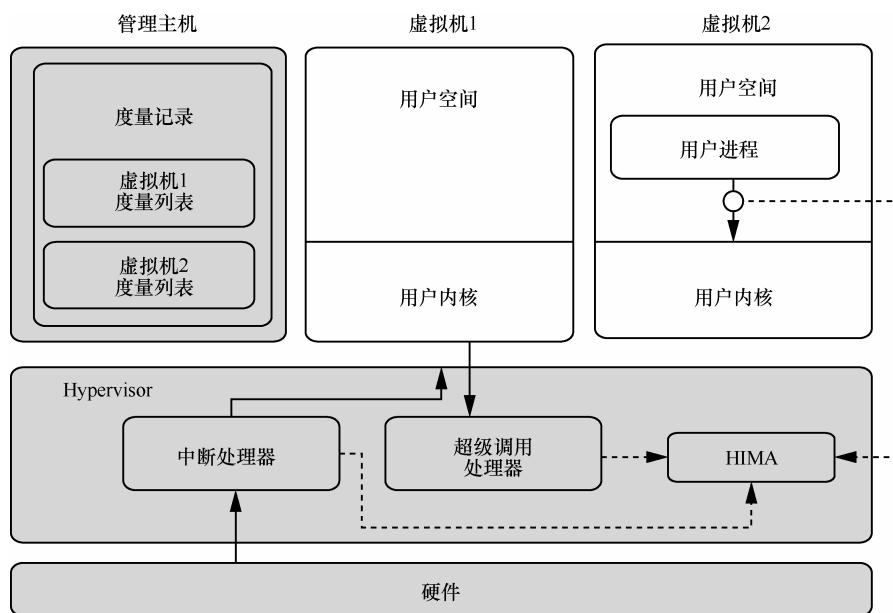


图 6 HIMA 架构（灰色区域为初始化信任组件）

其能够验证拥有最高权限软件的完整性。HyperSentry 并不是通过引入更高级权限的框架去度量拥有较高权限的软件,而是通过强化已经存在的硬件和提供固件支持的方式,引入一个与 Hypervisor 适当隔离的软件组件。或者说,HyperSentry 依赖于可信计算基 TCB 和一些其他固件。HyperSentry 度量模型由不受系统 CPU 控制的带外信道触发,即使系统屏蔽或重新规划信道,HyperSentry 仍能保持其隐密性。

HyperSentry 架构如图 7 所示。HyperSentry 由 SMI (系统管理终端处理器) 和内置于虚拟机监视器的度量代理组成。带外信道(本文指 IPMI)将 BMC (基板管理控制器)与远程证明方建立通信,而度量代理通过 SMI 间接与 BMC 建立通信。HyperSentry 通过带外信道触发隐密的完整性度量,使度量代理具有:1) 与虚拟机监视器相同的背景环境;2) 完全受保护的执行模式;3) 对其输出的证明。实践证明,HyperSentry 是一种适用于真实系统的低开销解决方案,但需要较大程度的硬件支持。

### 3.8 国内相关模型

国内对云服务可信度量的研究紧随国际潮流,如火如荼,成果斐然。刘孜文等和冯登国等在文献[13]与文献[14]中提出基于可信计算的操作系统动态度量架构(DIMA),实现了对系统中活动的进程与模块的细粒度度量,因此能有效解决 TOCTTOU 问题。林闯等在文献[15]中总结了针对不同云安全指标的形式化描述方法和不同类型的安全模型,并提出基于多队列多服务器的云安全模型与评价思路。周振吉等在文献[16]中提出一种虚拟机树形可信度量模型,该模型利用系

统调用截获和虚拟机内省技术构建度量原型,有效降低了虚拟机可信度量的复杂度。

## 4 结束语

本文度量模型基本解决度量中的一些难题,但一定程度上都有自己的缺陷。静态度量实时性和隐私保护性较差,而实时度量以牺牲系统运行性能为代价,基于内存代码监控的动态度量还存在控制监控粒度的问题。基于语义的度量需要较强硬件的支持。度量模型也面临自身安全的问题,只要可信度量根不被攻破,度量模型自身就是安全的。未来的研究方向是研究出兼顾可拓展性、实时性、隐私保护好、易移植且开销更小的度量模型。

### 参考文献:

- [1] 陈康, 郑伟民. 云计算:系统实例与研究现状[J]. 软件学报, 2009, 20(5):1337-1348.  
CHEN K, ZHENG WM. Cloud computing: system instances and current research[J]. Journal of Software, 2009, 20(5):1337-1348.
- [2] Common criteria for information technology security evaluation part 2: security functional requirement, version 2.2[S].2004.
- [3] Common criteria for information technology security evaluation part 3: security assurance requirements; version 2.2[S].2004.
- [4] NIELSEN F. Approaches to security metrics[C]//CSSPAB Workshop on Approaches to Measuring Security. c2000.
- [5] Cloud Security Alliance(CSA). Security guidance for critical areas of focus in cloud computing V3.0[EB/OL]. <https://cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf>.
- [6] AVIZIENIS A, LAPRIE J C, RANDELL B, et al. Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Transactions on Dependable & Secure Computing, 2004, 1(1):11-33.
- [7] TCG Group. TCG specification architecture overview[J]. TCG Specification Revision, 2007, 1: 1-24.
- [8] SAILER R, ZHANG X, JAEGER T, et al. Design and implementa-

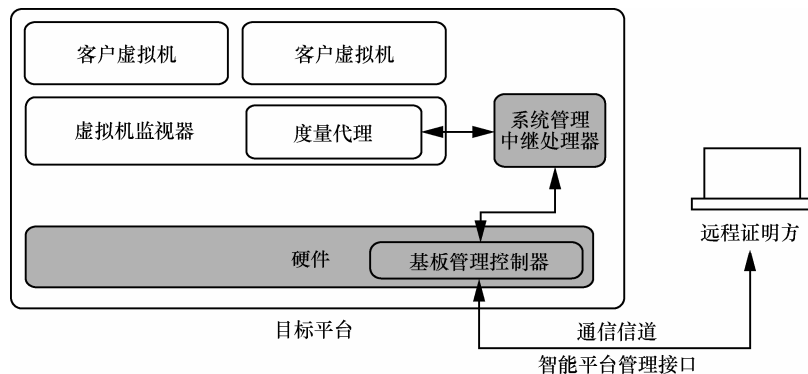


图7 HyperSentry 架构 (灰色区域为受信任的组件)

- tion of a TCG-based integrity measurement architecture[C]//Usenix Security Symposium. c2004:16-16.
- [9] JAEGER T, SAILER R, SHANKAR U. PRIMA: policy-reduced integrity measurement architecture[C]//The 11th ACM Symposium on Access Control Models and Technologies. c2006:19-28.
- [10] LOSCOCCO P A, WILSON P W, PENDERGRASS J A, et al. Linux kernel integrity measurement using contextual inspection[C]//ACM Workshop on Scalable Trusted Computing. c2007:21-29.
- [11] AZAB A M, NING P, SEZER E C, et al. HIMA: a hypervisor-based integrity measurement agent[C]// IEEE Computer Security Applications Conference. c2009:461-470.
- [12] AZAB A M, NING P, WANG Z, et al. HyperSentry: enabling stealthy in-context measurement of hypervisor integrity[C]//ACM Conference on Computer and Communications Security(CCS). c2010:38-49.
- [13] 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 and Information Technology, 2010, 32(4):875-879.
- [14] 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.
- FENG D G, QIN Y, WANG D, et al. Research on trusted computing technology[J]. Journal of Computer Research and Development, 2011, 48(8):1332-1349.
- [15] 林闯, 苏文博, 孟坤, 等. 云计算安全:架构、机制与模型评价[J]. 计算机学报, 2013, 36(9):1765-1784.
- LIN C, SU W B, MENG K, et al. Cloud computing security: architecture, mechanism and modeling[J]. Chinese Journal of Computers, 2013, 36(9):1765-1784.
- [16] 周振吉, 吴礼发, 洪征, 等. 云计算环境下的虚拟机可信度量模型[J]. 东南大学学报(自然科学版), 2014(1):45-50.
- ZHOU Z J, WU L F, HONG Z, et al. Trustworthiness measurement model of virtual machine for cloud computing[J]. Journal of Southeast University(Natural Science Edition), 2014(1):45-50.

#### 作者简介:



陆月明(1969-), 男, 江苏苏州人, 北京邮电大学教授、博士生导师, 主要研究方向为分布式计算、信息安全。



张志辉(1991-), 男, 安徽桐城人, 北京邮电大学硕士生, 主要研究方向为分布式计算与信息安全。