网络出版时间：2016-03-18 15:31:52
网络出版地址：http://www.cnki.net/kcms/detail/42.1658.N.20160318.1531.020.html

DOI：10.13245/j.hust.160320

基于信任扩展的可信云执行环境

纪祥敏[1,2] 赵 波[1] 陈 璐[3] 向 骕[1]

(1 武汉大学计算机学院，湖北 武汉 430072；2 福建农林大学计算机与信息学院，福建 福州 350002；3 海军工程大学信息安全系，湖北 武汉 430033)

摘要 针对单点信任传递技术无法应对云环境多节点动态信任问题，提出云环境并行信任传递机制.该机制根据可信计算技术思路，结合云计算工作模式与新特点，将信任划分为静态信任和动态信任，分别给出静态信任根和动态信任根定义，将二者整合形成云执行环境的可信基，静态度量与动态度量有机结合，并行传递信任，将信任从可信基逐级扩展到用户应用资源.经过信任规则谓词逻辑形式化推理，证明了该机制信任扩展正确、有效.测试结果表明：上述机制可达到系统完整性保护目的，系统性能开销在可接受范围之内，不影响用户正常使用.

关键词 云计算；可信计算；可信基；动态信任；动态度量；谓词逻辑

中图分类号 TP391.41 **文献标志码** A **文章编号** 1671-4512(2016)03-0105-05

Trusted cloud execution environment based on trust extension

Ji Xiangmin[1,2] *Zhao Bo*[1] *Chen Lu*[3] *Xiang Shuang*[1]

(1 Computer School, Wuhan University, Wuhan 430072, China; 2 College of Computer and Information Sciences, Fujian Agriculture and Forestry University, Fuzhou 350002, China; 3 Department of Information Security, Naval University of Engineering, Wuhan 430033, China)

Abstract To solve the problem that single-node trust transfer technique could not be suitable for dynamic multi-nodes trust, parallel trust transfer mechanism was proposed in cloud environment. On the basis of new operating modes and features of cloud computing, the trust was divided into static trust and dynamic trust in terms of the idea of trusted computing technology. Meanwhile, the definitions of static trust root and dynamic trust root were respectively given to be integrated into the trust base for cloud execution environment. Combined with static measurement and dynamic measurement, trust was transferred from the trust base to applications in parallel. Predicate logic formal reasoning proves that the trust can be extended properly and effectively. Experimental results illustrate that the system integrity protection is achieved, and the performance overhead is restricted within an acceptable range, without affecting daily application.

Key words cloud computing; trusted computing; trust base; dynamic trust; dynamic measurement; predicate logic

云计算具有便捷易用与低成本特性，同时也带来了较传统模式更严重的安全威胁，引发了用户心理上的顾虑[1-3].云执行环境的安全可靠性是云系统成功应用的基础与关键[4-6].可信计算技术为解决云执行环境可信问题提供了新思路.

Berger 等[7]提出为每个虚拟域提供相应虚

收稿日期 2015-08-07.

作者简介 纪祥敏(1971-)，男，博士研究生；赵 波(通信作者)，教授，E-mail：zhaobowhu@163.com.

基金项目 国家重点基础研究发展计划资助项目(2014CB340600)；国家高技术研究发展计划资助项目(2015AA016002)；国家自然科学基金资助项目(61332019,61173138,61272452)；信息保障技术重点实验室开放基金资助项目(KJ-13-106).

拟信任根,作为每个虚拟域的静态信任起点.文献[8]基于虚拟机监控器(virtual machine monitor, VMM)动态度量框架,实现对虚拟机内部资源进行动态度量.文献[9]在此基础上,将网卡驱动写入统一可扩展固件接口(unified extensible firmware interface, UEFI),提升安全性.文献[10-11]将安全硬件作为信任根,实现可信虚拟化环境的构建.文献[12]基于扩展安全系统逻辑(logic of secure systems, LSS)对VMM动态度量进行形式化分析.这些研究主要基于传统PC单一可信硬件或虚拟信任根的单节点信任传递技术,在一定程度上加强了云执行环境安全性,然而云执行环境中存在多个操作系统,并发运行于同一物理平台,可能存在同一用户的资源运行于不同节点、不同虚拟域的情况,存在多节点动态交互新特点,明显有别于传统PC的工作特点[2,5].显然,要保证云执行环境的可信性,仅依靠传统意义上的静态信任起点远远不够,因此如何确定云计算新环境可信基范围是一个关键问题.

为此,针对PC环境单一可信硬件的单点信任传递技术无法解决云环境的多节点动态交互与信任扩展问题,从信任定义出发,分别给出云执行环信任根和可信基描述.同时,基于可信平台模块(trusted platform module, TPM)与UEFI,提出静态度量与动态度量相结合的并行信任传递机制,进行平台信任有效扩展,保证云执行环境的安全可靠性.

1 云执行环境可信基构建

1.1 静态信任与动态信任

根据云计算工作模式新特点,云执行环境信任可划分为静态信任和动态信任.其中,静态信任保障初始执行环境的安全是后续安全可靠的基础;动态信任确保平台执行过程安全,保障资源的运行时安全性.下面分别给出静态信任与动态信任的定义.

定义 1 对于任意程序,若从初始化到执行启动之前,该程序未受任何非法篡改或破坏,保持程序完整属性不变,输入与输出满足行为预期性,则称之为静态信任.程序行为的静态信任用 T_S 表示,具体描述为

$$T_S=\begin{cases}1 & (a\in A\mid\langle t_i,t_s\rangle);\\ 0 & (\text{其他}),\end{cases}$$

式中:a 为程序实体行为;A 为程序预期行为集合;t_i 和 t_s 分别为程序初始化时刻、执行启动时刻;T_S 为0时表示程序可信,为0时表示程序不可信.

定义 2 对于任意程序,若从执行启动到执行终止期间,该程序未受任何非法篡改或破坏,保持自身安全语义完整性不变,输入与输出执行过程没有违约、违规、超出安全权限或者范围,满足行为预期性,则称之为动态信任.程序行为的动态信任用 T_D 表示,具体描述为

$$T_D=\begin{cases}1 & (a\in A\mid\langle t_s,t_e\rangle);\\ 0 & (\text{其他}),\end{cases}$$

式中:t_e 为程序执行终止时刻;T_D 为1时表示程序可信,为0时表示程序不可信.

在程序初始化与执行启动之前,系统一旦发起信任度量,属于静态度量范畴;而程序在执行启动之后、执行终止期间,系统一旦发起信任度量,属于动态度量范畴.

1.2 静态信任根与动态信任根

信任根是可信计算的关键技术之一.在可信计算体系中,信任根作为信任的起点和发起者,负责建立最核心的信任节点,并将信任值传递下去,从而形成可信平台的安全环境.

基于定义1和定义2,云执行环境须以不同方式分别传递静态信任与动态信任.显然,在云执行环境中也应该存在静态信任根与动态信任根,分别作为静态信任和动态信任的起点.

定义 3 静态信任根是每台机器的初始执行环境传递静态信任的起点,在系统启动时以度量起点的方式存在.

在可信计算组织(trusted computing group, TCG)体系中,一般由TPM和BIOS共同构成系统的静态信任根.静态信任根只在系统启动建立静态信任时发挥作用.

定义 4 动态信任根是云执行环境中动态信任传递的起点,可以在平台运行后任意时刻发起度量,而不必在每次系统启动后发起度量.

由此可见:云执行环境中,由单一的静态信任根或者动态信任根构建的可信基难以满足多节点动态交互的实际需求,须要二者有机结合的方式构建可信基.

1.3 云执行环境可信基构建

可信基是整个可信计算系统的信任基点.可信基的安全性高于其余组件,并由硬件设备、安全技术和管理手段共同来保障.云执行环境可信基的安全假定条件为:**a.** 假定物理机器上的可信硬件安全,攻击者无法获取访问物理机器的权限;**b.** 可信硬件中的软件模块没有恶意的植入代码;

c. 云执行环境中不存在恶意管理员.

在以上安全假定的基础上，给出云执行环境可信基定义.

定义 5　$B_{CT}=\{R_{ST},R_{DT}\}$为云执行环境可信基，且 $R_{ST}=\{TPM_0,TPM_1,\cdots,TPM_n\}$，$R_{DT}=\{STPM,UEFI_0,UEFI_1,\cdots,UEFI_n\}$，其中：$R_{ST}$和 R_{DT}分别为静态信任根与动态信任根；TPM_0，TPM_1，…，TPM_n 为云执行环境中每一个节点的 TPM；STPM 为云平台管理中心的安全管理模块软件 TPM（software trusted platform module，STPM）；$UEFI_0$，$UEFI_1$，…，$UEFI_n$ 为云执行环境中每一个安全节点的 UEFI.

如图 1 所示，云执行环境可信基 B_{CT} 由动态信任根 R_{DT} 与静态信任根 R_{ST} 构成，图中 N_0，N_1，…，N_n 分别为各节点. 云执行环境中的每个节点都有各自的 TPM 和 UEFI，其中各节点的 TPM 共同构成静态信任根，负责发起静态度量操作，保证节点启动过程中的安全性；安全管理模块 STPM 和每台机器的 UEFI 共同构成动态信任根，用户接入云平台后，云管理中心可以随时发起动态度量请求.

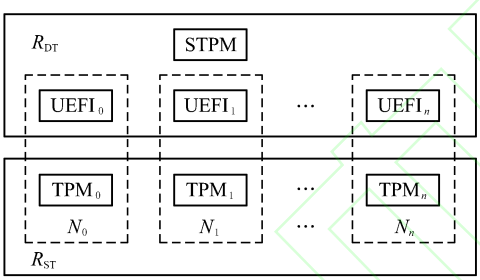

图 1　云执行环境可信基构成

在安全性方面，作为静态信任根的 TPM 为可信硬件，其安全性已经得到多年的理论和实践验证；同时，STPM 安全性由管理服务器的硬件 TPM 保证，UEFI 的安全设计和实现要求也保证了被篡改的可能性极低，因此将二者共同作为系统的动态信任根安全可靠.

2　云执行环境并行信任传递机制

针对现有基于单一可信硬件的单点信任传递技术无法满足动态多节点之间的信任传递需求，这里根据云计算工作模式新特点，按照信任扩展规则，提出云执行环境并行信任传递机制，静态度量与动态度量有机结合，并行传递信任，旨在将信任从可信基逐级扩展到用户应用资源，进而由信任规则谓词逻辑对该机制形式化推理，验证信任扩展的正确性.

2.1　信任扩展规则

通常，信任受到上下文、授权策略和认证路径长度等相关约束条件限制，在授权策略的引导下，资源节点被所辖的度量节点度量、认证；在认证路径中，认证路径越长，度量节点及相应资源节点可信程度损失越大.

为了实现云执行环境信任有效传递，利用信任扩展规则进行信任传递. 基于扩展谓词逻辑对认证规则、信任规则和信任扩展推理规则定义如下所示.

设 $\forall E_1,E_2\in E,p_1,p_2,p_3\subseteq P,l_1,l_2,l_3\in L$，其中：$E$ 为实体集合；P 为系统中存在的策略集合，表示系统中存在的所有策略；L 为路径约束集合.

定义 6　认证规则. 若实体 E_1 完成对实体 E_2 的认证，并信任 E_2，同时 E_2 已向 E_3 提供可信证明，当符合认证路径约束时，E_1 完成对 E_3 认证. 认证规则形式化表示为

$$A(E_1,E_2)\mid\langle p_1,l_1\rangle,T(E_1,E_2)\mid\langle p_2,l_2\rangle,C(E_2,E_3)\mid\langle p_3,l_3\rangle/[A(E_1,E_3)\mid\langle p_1\cap p_2\cap p_3,l_3\rangle],$$

式中：$A(E_1,E_2)$表示 E_1 完成对 E_2 认证；$T(E_1,E_2)$表示 E_1 信任 E_2；$C(E_2,E_3)$表示 E_2 向 E_3 提供可信证明.

定义 7　信任规则. 若实体 E_1 向实体 E_2 提供了可信证明，则认为 E_1 信任 E_2. 信任规则形式化表示为

$$\frac{C(E_1,E_2)\mid\langle p_1,l_1\rangle,l_2\leqslant l_1}{T(E_1,E_2)\mid\langle p_2,l_2\rangle}.$$

定义 8　信任扩展规则. 若实体 E_1 信任实体 E_2，并且 E_2 信任 E_3，则 E_1 信任 E_3. 信任扩展规则形式化表示为

$$T(E_1,E_2)\mid\langle p_1,l_1\rangle,T(E_2,E_3)\mid\langle p_2,l_2\rangle/[T(E_1,E_3)\mid\langle p_1\cap p_2,l_3=(l_1,l_2)\rangle].$$

2.2　云执行环境并行信任传递机制

为了切实保证云执行环境中单个节点初始执行环境系统安全启动且执行过程中用户资源实时安全可靠，将静态信任传递和动态信任传递两部分并行执行. 云执行环境并行信任传递机制如图 2 所示.

静态信任传递方面，当云执行环境中各节点 N_0，N_1，…，N_n 启动时，以静态信任根 TPM_0，TPM_1，…，TPM_n 为起点，对各节点进行完整性度量，实现系统静态信任传递，保证各节点按照可信规范的方式安全启动，为云执行环境中各节点初始执行环境安全提供基础.

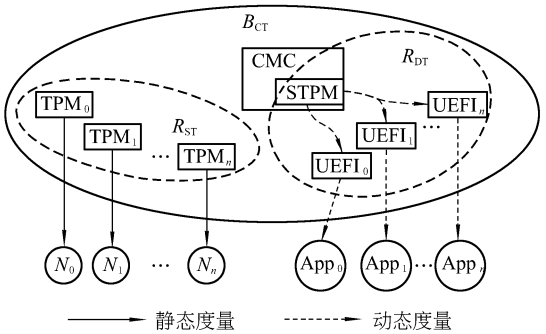

图 2 云执行环境并行信任传递机制

动态信任传递基本思路:当云执行环境用户应用一旦有安全需求时,由云管理中心(cloud management center, CMC)的动态信任根 STPM 结合各节点 UEFI,对执行环境或应用资源发起动态完整性度量,按照信任扩展规则构建动态信任链:STPM→UEFI→APP,防止恶意代码在云平台中运行.

根据定义 6~8,对云管理中心 CMC 到用户应用 APP 的动态信任传递规则进一步逻辑推导,给出如下定义.

定义 9 在云执行环境中,存在 E_{CMC}, E_{STPM}, E_{UEFI}, $E_{APP}\in E$, V_{CMC} 和 $\bar{V}_{CMC}$,其中:E_{CMC}, E_{STPM}, E_{UEFI} 和 E_{APP} 分别为云管理中心、STPM、UEFI 和用户应用实体;V_{CMC} 和 $\bar{V}_{CMC}$ 分别为云管理中心初始视图与经过逻辑推导后视图.

根据云执行环境各节点的信任关系,可定义

$$V_{CMC}=\{A(E_{CMC},E_{STPM})\mid\langle p_1,0\rangle, T(E_{CMC},E_{STPM})\mid\langle p_2,0\rangle, C(E_{STPM},E_{UEFI})\mid\langle p_3,0\rangle, C(E_{STPM},E_{APP})\mid\langle p_4,0\rangle\},$$

并且有如下定理

$$\bar{V}_{CMC}=V_{CMC}\cup\{T(E_{STPM},E_{UEFI})\mid\langle p_3,0\rangle, T(E_{CMC},E_{UEFI})\mid\langle p_2\cap p_3,0\rangle, A(E_{CMC},E_{UEFI})\mid\langle p_1\cap p_2\cap p_3,0\rangle, A(E_{CMC},E_{APP})\mid\langle p_1\cap p_2\cap p_3\cap p_4,0\rangle\}.$$

证明 根据定义 9,由定义 7 信任规则推理得 $C(E_{STPM},E_{UEFI})\mid\langle p_3,0\rangle/[T(E_{STPM},E_{UEFI})\mid\langle p_3,0\rangle]$,经过定义 8 信任扩展得

$$T(E_{CMC},E_{STPM})\mid\langle p_2,0\rangle, T(E_{STPM},E_{UEFI})\mid\langle p_3,0\rangle T(E_{STPM},E_{UEFI})\mid\langle p_3,0\rangle/[T(E_{CMC},E_{UEFI})\mid\langle p_2\cap p_3,0\rangle].$$

最后,由定义 6 认证规则得

$$A(E_{CMC},E_{STPM})\mid\langle p_1,0\rangle, T(E_{CMC},E_{STPM})\mid\langle p_2,0\rangle, C(E_{STPM},E_{UEFI})\mid\langle p_3,0\rangle/[A(E_{CMC},E_{UEFI})\mid\langle p_1\cap p_2\cap p_3,0\rangle],$$

以及

$$A(E_{CMC},E_{UEFI})\mid\langle p_1\cap p_2\cap p_3,0\rangle, T(E_{CMC},E_{UEFI})\mid\langle p_2\cap p_3,0\rangle, C(E_{UEFI},E_{APP})\mid\langle p_4,0\rangle/[A(E_{CMC},E_{APP})\mid\langle p_1\cap p_2\cap p_3\cap p_4,0\rangle].$$

由此定理得证.

综上所述:多个信任根共同形成云执行环境的可信基,静态度量与动态度量有机结合,从整体上将信任从云执行环境中的可信基逐级扩展到用户应用资源,并且信任传递正确、扩展有效.

3 系统实现与测试分析

在已有理论研究与实践中,静态度量机制已经得到充分验证,因此这里仅对云执行环境动态信任传递机制进行设计. 以 Openstack 作为云执行环境基础管理平台,以 Xen 作为虚拟机监控器层的管理软件,构建可信执行环境动态度量原型系统,并对信任传递机制的有效性、度量开销指标进行测试.

3.1 系统实现

使用 3 台华为服务器搭建一个云执行环境,采用 OpenStack H-3 作为云管理平台,构建可信执行环境动态度量原型系统,进行有效性与度量开销测试分析. 在测试环境所用到的其他软硬件环境如下:CPU 为 Intel 至强 5 650×2, 2.0 GHz;64 GB 内存;西部数据 4 TB 企业级硬盘;国民技术 TPM2.0 芯片(Z32H320TC);VMM 为 Xen 4.0;SUSE Linux Enterprise Server 11 SP3 64 bit 操作系统.

构建的云执行环境动态度量原型如图 3 所

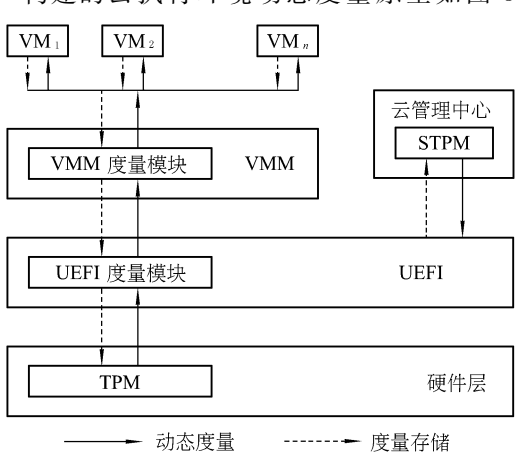

图 3 云执行环境动态度量框架

示,在每个节点的 UEFI 和 VMM 中分别设置了一个度量模块,此外包含一个云管理中心,协同负责对虚拟域以及其内的组件发起动态度量、度量结果反馈功能.

动态度量过程:当系统启动时,云管理中心获

得控制权，以动态信任根 STPM 为起点，系统发送度量指令，验证 UEFI 模块的完整性，验证通过后，信任控制权转移到 UEFI 模块；接着由 UEFI 模块中的度量代码验证 VMM 的完整性，验证通过后，信任控制权转移到 VMM 度量模块；最后由 VMM 度量模块验证虚拟机(virtual machine，VM)及应用软件的完整性，由此建立从 STPM 到上层应用的动态信任链.

3.2　有效性测试

为了测试云执行环境信任传递机制的有效性，实验中首先测试节点的抗篡改攻击能力. 具体方法为：平台首次启动时，进行平台初始化操作，按照动态信任结构构建信任关系；首次初始化完毕后，修改内核部分代码，若再次启动发现不能进入系统，则系统的完整性得以保障.

其次，实验还对虚拟域内一个受保护软件的抗篡改攻击能力进行测试，选取一个浏览器验证 STPM 对于软件的完整性保护效果. 浏览器选用 Google Chrome 46.0，其可执行代码的文件名为 Chrome，大小为 42.311 KB. 实验中预先修改了浏览器一个帮助文件的二进制字符串字段，该文件本身不会影响程序执行；之后再次执行程序，若发现保护过的 Chrome 不能执行，则达到了对软件的完整性保护.

3.3　度量开销测试

在 VMM 内实现了一个度量模块，对一个选定的程序发起度量，并记录了度量过程中系统的时间开销. 在测试过程中，除了计算应用程序的 hash 值之外，还须要向硬盘中写入一些软件的身份信息. 选取的程序大小为 380 KB，一共进行了 6 次试验. 实验中 6 次度量时间分别为 19.37，19.03，19.56，19.96，19.71 和 19.53 s，平均时间开销为 19.53 s，每 100 KB 代码度量时间为 5.13 s，在用户可接受范围之内.

在 CPU 占用率测试实验中，依次运行 1，5 和 10 台 VM，分别记录系统正常运行与动态度量执行时的 CPU 占用率. 如表 1 所示，在 VM 数量相同情况下，与系统正常运行时 CPU 占用率相比，动态度量执行 CPU 占用率增加较小.

表 1　系统正常与动态度量执行时 CPU 占用率　%

执行方式	VM 数量		
	1	5	10
正常运行	20.1	56.0	92.3
度量执行	23.9	59.1	97.6

基于扩展谓词逻辑信任扩展推理证明与测试结果表明：静态度量与动态度量有机结合的并行信任传递机制达到了系统完整性保护目的，系统开销在用户可接受范围之内.

参　考　文　献

[1] Ali M, Khan S U, Vasilakos A V. Security in cloud computing: opportunities and challenges[J]. Information Sciences, 2015, 305: 357-383.

[2] Xu P, Chen H, Zou D, et al. Fine-grained and heterogeneous proxy re-encryption for secure cloud storage [J]. Chinese Science Bulletin, 2014, 59(32): 4201-4209.

[3] Zou D, Zhang W, Qiang W, et al. Design and implementation of a trusted monitoring framework for cloud platforms[J]. Future Generation Computer Systems, 2013, 29(8): 2092-2102.

[4] 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.

[5] Xiang S, Zhao B, Yang A, et al. Dynamic measurement protocol in infrastructure as a service[J]. Tsinghua Science and Technology, 2014, 19(5): 470-477.

[6] Yu F, Zhang H, Zhao B, et al. A formal analysis of trusted platform module 2.0 hash-based message authentication code authorization under digital rights management scenario[J]. Security and Communication Networks, 2015, 8: 2462-2476.

[7] Berger S, Cáceres R, Goldman K A, et al. vTPM: virtualizing the trusted platform module[J]. Usenix Security, 2006, 15: 305-320.

[8] IBM. Tpod[EB/OL]. [2015-07-12]. http://domino.research.ibm.com/comm/research_people.nsf/pages/taiga.reports.html/$FILE/RT0564.pdf.

[9] Zhang F, Wang J, Sun K, et al. HyperCheck: a hardware-assisted integrity monitor[J]. Dependable and Secure Computing IEEE Transactions on, 2013, 11(4): 332-344.

[10] Seol J, Jin S, Lee D, et al. A trusted IaaS environment with hardware security module [J]. IEEE Trans on Services Computing, 2015(1): 1-14.

[11] Jaeger T, Sailer R, Shankar U. PRIMA: policy-reduced integrity measurement architecture[C]// Proceedings of the 11th ACM Symposium on Access Control Models and Technologies. LakeTahoe: Computer Science, 2006: 19-28.

[12] 纪祥敏，赵波，向骕，等. 基于扩展 LS^2 的 VMM 动态度量形式化分析[J]. 山东大学学报：理学版，2014，9(9)：1-8.