

构建基于虚拟机的可信云计算平台

沈 松, 邢剑锋, 王鹏飞, 朱 飞

(海军蚌埠士官学校 信息技术系, 安徽 蚌埠 233012)

摘 要: 云计算结构能极大地降低计算成本, 但数据和计算的保密性和完整性目前还无法保证. 设计了一种可信赖云计算平台(trust cloud computing platform, TCCP), 可以为客户虚拟机安全执行提供封闭环境, 允许用户在执行虚拟机前先检验服务商, 能够确保服务安全.

关键词: 云计算; 信赖; 虚拟机

中图分类号: TP393. 08

文献标识码: A

文章编号: 1000-7180(2011)08-0191-04

Design of Trusted Cloud-platform Based on Virtual Machine

SHEN Song, XING Jian-feng, WANG Peng-fei, ZHU Fei

(Department of Information Technology, Bengbu Naval Petty Officer Academy, Bengbu 233012, China)

Abstract: Cloud computing infrastructures enable companies to cut costs. However, currently there is no means to verify the confidentiality and integrity of their data and computation. To address this problem we propose the design of a trusted cloud computing platform (TCCP). TCCP enables Infrastructure as a Service (IaaS) providers to provide a closed box execution environment that guarantees confidential execution of guest virtual machines. Moreover, it allows users to attest to the IaaS provider and determine whether or not the service is secure before they launch their virtual machines.

Key words: cloud compute; trust; virtual machine

1 引言

云计算服务能够大大节约存储和计算数据的成本, 但安全问题严重制约了云计算的发展. 企业最关心的是数据的安全性和失去数据控制权会对隐私带来什么样的危害, 而不仅仅是如何降低数据存储和处理的成本^[1]. 云服务商恶意和心怀不满的雇员很有可能篡改或者泄露用户数据, 甚至是公司的财务状况, 这会对用户会造成巨大危害.

本文提出一种可信赖云计算平台(TCCP), 可以确保外包给 IaaS 的计算的保密性和完整性. TCCP 为用户 VM 提供一个封闭的执行环境, 避免云服务商的特权用户窥视或者篡改内容, 在执行 VM 申请前, 用户可以远程判断服务后台运行的 TCCP 是否可信. 该方法拓展了整体服务验证的概念, 使用户能够预估计算执行安全性^[2].

2 相关知识

2.1 基础设施服务(IaaS)

当前众多云服务商提供不同的软件层级服务, 较低层级 IaaS 如 Amazon 等, 提供客户访问服务商控制的整个虚拟机, 客户和系统用户需要配备虚拟机上运行的软件. 较高层级的软件服务化(SaaS)系统如 Google Apps 等, 可以完全在线运行, 无需客户干预.

在高软件层级运行服务更难保证计算的保密性, 因为服务本身需要操作客户数据的软件(例如 Google Docs). 本文主要研究低层级 IaaS 云服务商, 其更容易保证客户虚拟机安全运行.

本文以 Eucalyptus^[3]为例, 这是一个开源 IaaS 平台, 界面与 EC2 类似, 系统包含一个或多个运行客户虚拟机的镜像(典型的如 Xen)的节点簇, 且拥

有一系列组件来管理这些簇. 简言之, 需要将所有这些组件集中到一个云管理者 (cloud manager, CM)^[3]. Eucalyptus 结构示意图 1.

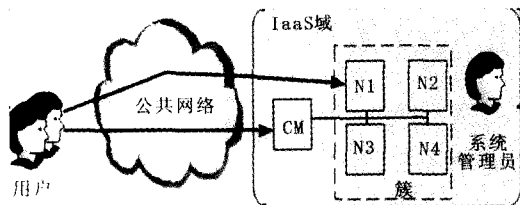


图 1 Eucalyptus 结构示意图

从客户角度, Eucalyptus 提供了一个可执行、可管理和可终止 VM 的 web 服务接口, 虚拟机镜像 VMI 运行 VM, 而 CM 负载 VMI. VM 启动以后, 用户可以利用普通工具登录, 如 ssh. 除了用户接口, CM 还提供管理服务, 如添加或删除 VMI 或用户. Xen 支持热迁移, 允许 VM 在执行时更换物理主机, 而过程对用户透明, 这种迁移对于簇内资源整合和负载均衡有重要意义.

2.2 攻击模型

云服务商的系统管理员拥有控制后台的特权, 可以实施多种攻击以访问客户虚拟机内存. 一旦拥有机器的根权限, 就可以安装执行实施攻击的任何软件. 另外在获取机器物理访问权后, 系统管理员可以执行更多精确攻击, 例如冷启动攻击, 甚至是毁坏硬件.

对于目前 IaaS 提供商, 没有哪个人拥有全部特权, 且服务商也部署了严格的安全设施和严格的访问权限策略, 能够阻止对机器物理访问的攻击. 但系统管理员还是需要簇内机器的访问特权来管理机器上运行的软件. 本文在攻击模型中假设系统管理员在任意时间都能以根权限远程访问任何机器, 他获取运行客户虚拟机的节点的物理访问权的唯一办法是将该虚拟机迁移到被他控制的、不在 IaaS 安全保护域内的机器上. 因此 TCCP 必须做到以下两点: (1) 确保虚拟机在安全保护域内运行; (2) 任何时候拥有根权限的系统管理员远程登录运行虚拟机的机器都不能访问虚拟机内存.

2.3 可信赖计算

可信赖计算群 (TCG)^[4] 提出了一系列的软硬件技术来构建可信赖平台, 而且给出了可信赖平台模块 (TPM) 集成的设计标准, 把硬件也考虑在内. TPM 支持私钥 (EK) 并将此作为身份识别的唯一标准, 还支持一些不可修改的加密方法, 不同厂商设备使用公钥识别集成模块.

可信赖平台^[2,5] 改进了 TPM 集成特性, 使其可以远程识别, 具体工作机制如下: 在启动时, 主机计算一个由启动软件序列哈希值组成的测度列表 ML, 启动软件即 BIOS、启动项、软件执行平台等, ML 安全载入主机 TPM, 为了验证平台, 远程一方利用当前 nU 挑战运行在主机平台, 平台调用 TPM 生成包含 ML 和 nU 的应答信息, 并用 TPM 的私钥加密, 主机将信息反馈给远程方, 远程方利用对应的 EK 公钥解密, 这样就完成了对主机的认证. 通过核验 ML 和 nU, 远程方可以鉴别主机上运行的平台是否可信赖.

假设传统可信赖平台能够保证单台主机上的计算安全性, 保证 IaaS 服务的最自然的想法就是在服务后台每个节点都部署平台 (图 1), 然而这样是不够的, 不论 VM 载入时 (通过操作 CM) 还是运行时 (通过迁移), 系统管理员都可以将客户 VM 转移到没有运行平台的节点上. 所以平台验证机制并不能保证远程方得到的测度列表 ML 就是 VM 运行 (或即将运行) 主机的真实信息. 因此 TCCP 需要设计远程验证方法, 保证后台平台资源持久安全.

3 可信赖云计算平台

本文提出一种可信赖云计算平台 (trust cloud computing platform, TCCP), 它将可信赖平台概念拓展到整个 IaaS 后台, 提供一个完全封闭的执行环境, 可以保证用户 VM 的保密性和完整性, 并允许用户预先判断 IaaS 是否实施了这些措施.

3.1 概述

TCCP 加强了 IaaS 后台, 使其可以在不改变结构的情况下提供封闭执行环境 (图 2). TCCP 可信赖计算的基础包含两个方面: 可信赖虚拟机映像 (TVMM) 和可信赖协调者 (TC).

后台每个节点运行掌控客户 VM 的 TVMM, 并防止特权用户窥视和篡改它们. TVMM 可以保护自身安全性并遵守 TCCP 协议, 节点被嵌入经验证的 TPM 并通过安全启动进程加载 TVMM. 版面限制不再描述详细的 TVMM 的设计过程, 有兴趣的读者可参考文献^[5], TVMM 的本质就是一个可抵抗恶意系统管理员的本地封闭环境.

TC 管理一系列可以安全运行客户 VM 的节点, 这些节点称为可信赖节点. 为了做到可信赖, 节点必须位于安全域内并运行 TVMM, 这要求 TC 保存节点位于安全域的记录, 并验证节点平台以判断该节点是否运行着可信赖 TVMM. TC 管理诸如簇中添加或

移除节点、由于维修或升级需临时关闭节点等事件。通过 TC 验证,用户可以判断 IaaS 是否安全。

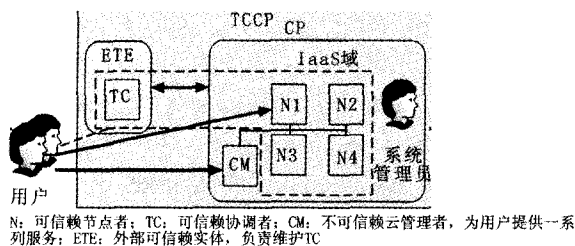


图2 可信赖云计算平台组成图

为了 VM 的安全,每个节点上运行的每个 TVMM 必须与 TC 相配合,目的是:(1)将 VM 限制在可信赖节点上,(2)在 VM 迁移时保证其状态不受窥视和篡改。这些保护措施关键在加载和迁移 VM 时的操作,为了保护这些操作,TCCP 制订了具体协议(见 3.2 节)。

假设由外部可信赖实体(ETE)来管理 TC,并为 TC 更新部署在 IaaS 域中一系列节点和可信赖配置的信息,最重要的是管理 IaaS 的系统管理员在 ETE 内部没有特权,因此不能篡改 TC。本文假设 ETE 由没有与 IaaS 服务商共谋动机的第三方维护,即如认证授权机构 VeriSign 一样的独立公司。

3.2 详细设计

本节详细介绍 TCCP 相关机制。在 3.2.1 节介绍可信赖平台上一系列节点的管理协议,3.2.2 节介绍 VM 安全管理协议,包括装载 VM 和迁移 VM。这些协议中用以下标记表示加密操作, $\langle K^p, K^p \rangle$ 表示私钥公钥对, $\{y\}K^x$ 表示经密钥 K^x 加密后的数据 y 。定义 EK_x 表示识别密钥, TK_x 表示可信赖密钥, K_x 表示会话密钥,随机数 n_x 由 x 产生,防止消息重放。

3.2.1 节点管理

通过保存包括安全域内节点、识别节点可信平台模块(TPM)的公开识别密钥 EK_N^p 和预期测度列表 ML_N 的目录,TC 可以动态管理一系列掌控 VM 的可信赖节点。ETE 保证 TC 部分参数安全公开可用,包括 EK_{TC}^p , ML_{TC} 和 TK_{TC}^p , ML_N 和 ML_{TC} 是远程方在识别节点 N 或 TC 上运行的平台时希望收到的值。

节点必须在 TC 注册,并遵守图 3 中描述的协议。前两步节点 N 验证 TC,节点 N 向 TC 发起挑战 n_N ,TC 返回经 EK_N^p 加密的 ML_{TC} ,如果 ML_{TC} 与预期相符,即表示 TC 是可信赖的。TC 在返回信息 2 中包含了对节点 N 的挑战 n_{TC} ,第三步节点 N 产生密钥对 (TK_N^p, TK_N^p) ,并将公钥随验证消息 3 发给 TC。如果 TC 成功验证节点 N 的身份,则发送消息 4 确认

节点是可信赖的。

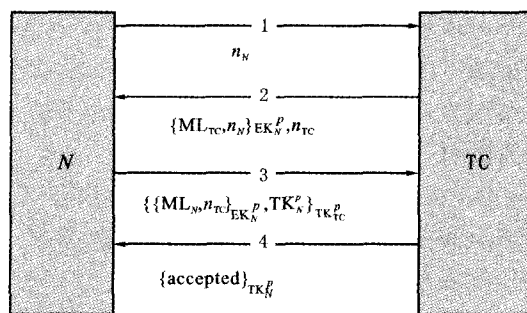


图3 节点迁移过程中的消息交换

可信赖节点重启时,TCCP 必须保证节点仍然是可信赖的,否则节点会威胁 TCCP 的安全性。为此若节点内存仅保存 TK_N^p ,机器重启密钥就会丢失,节点就会被 TCCP 阻止,因此节点必须重新注册。

3.2.2 虚拟机管理

下面介绍 TCCP 协议在 VM 加载和迁移操作的安全机制。加载 VM 时,TCCP 需要保证:(1)VM 加载到可信赖节点,(2)系统管理员无权窥视和篡改初始 VM 状态。VM 初始状态 α 包含虚拟机镜像 VMI 和用户公钥。注意,用户可以使用 IaaS 提供的 VMI。

参与 VM 装载的各方都必须遵守图 4 所示的协议。该协议制定的依据是在加载 VM 前,用户不知道 VM 将加载到哪个物理节点上,并且在服务的所有参与者中只有 TC 可信赖。首先用户生成会话密钥 K_{VM} ,发送消息 1 到 CM,消息包含 α 和 α 用会话密钥加密的哈希值以及用 TK_{TC}^p 加密的 K_{VM} 。用 TC 的公钥加密会话密钥,保证只有经 TC 授权的可信赖节点才能访问 α 。

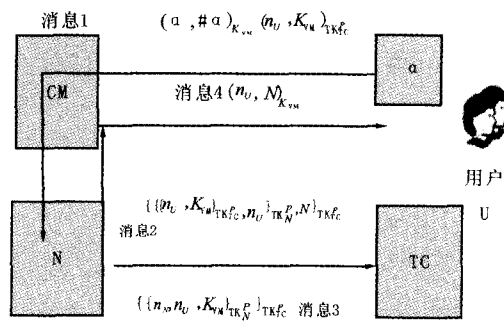


图4 装载 VM 过程中的消息交换

收到加载 VM 请求后,CM 指派簇中节点 N 加载 VM,并将请求转发给 N 。因为启动 VM 需要访问 α ,节点 N 向 TC 发送消息 2,TC 用私钥 TK_N^p 解密消息,验证 N 是否可信。如果 TC 信赖节点库中没有节点 N 的公钥,则拒绝该请求,这可能是由于 CM 将请

求转移到了恶意系统管理员控制的节点, 否则认为节点是可信赖的. TC 解密会话密钥, 并在消息 3 中发送给节点 N , 此时 N 就可以解密并启动 VM 了. 最后节点发送消息 4 给用户, 消息包含节点运行 VM 的证明.

在实时迁移^[6]中, 运行中的 VM 的状态信息在两个节点间迁移: 源节点 N_s 和目标节点 N_d . 为保证操作的安全性, 两个节点必须互信, 且 VM 状态必须可信并且在完成迁移前是不可修改的. 图 5 所示为参与 VM 安全迁移的消息队列, 首先 N_s 请求 TC 检验 N_d 是否可信, 消息 3 中, N_s 向 N_d 发起 VM 迁移申请并附加会话密钥 K_s . N_d 验证 N_s 是否可信 (第 4、5 步). 如果两个节点都认证成功, N_d 通知 N_s 接受 K_s (第 6 步), 在消息 7 中 N_s 最终将 VM 状态哈希值加密发送给 N_d , VM 迁移成功.

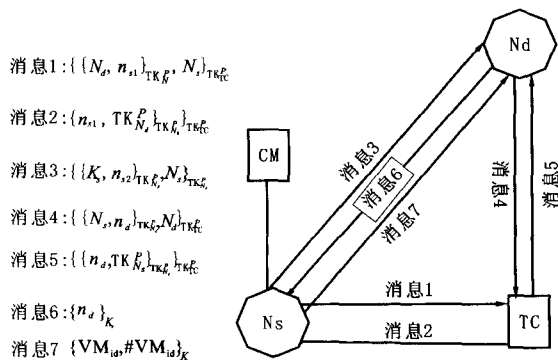


图 5 VM 迁移过程中的消息交换

4 结束语

企业普遍应用云计算的主要阻力源自对数据和计算的保密性和完整性的担心, 本文提出一种可信云计算平台 TCCP, 它可以为 IaaS 服务提供一个封闭执行环境, 保证了客户 VM 执行的机密性, 允许

用户验证 IaaS 提供商并在装载其虚拟机前先判断服务是否安全.

参考文献:

- [1] Berger S, Caceres R, Goldman K A. vTPM: virtualizing the trusted platform module[C]// Proc of USENIX-SS'06, Berkeley, CA, USA: IEEE, 2006.
- [2] Survey: cloud computing no hype, but dear of security and control slowing adoption[EB/OL]. [2010-10-15]. http://www.circleid.com/posts/20090226_cloud_computing_hype_security/.
- [3] Clark C, Fraser K, Hand S. Live migration of virtual machines[C]// Proc of NSDI'05. Berkeley, CA, USA: IEEE, 2005: 273-286.
- [4] Murray D G, Milos G. Improving xen security through disaggregation[C]// Proc of VEE'08. New York, NY, USA: IEEE, 2008.
- [5] Nurmi D, Wolski R, Grzegorzczak C. Eucalyptus: a technical report on an elastic utility computing architecture linking your programs to useful systems. Technical Report 2008-10[R]. Santa Barbara California UCSB Computer Science, 2008.
- [6] TCG. [EB/OL]. [2010-10-15]. <https://www.trustedcomputinggroup.org>.

作者简介:

沈松男, (1973-), 副教授. 研究方向为网络安全和云计算.

邢剑锋男, (1981-), 硕士, 讲师. 研究方向为 P2P 和云计算.

王鹏飞男, (1984-), 硕士, 讲师. 研究方向为网络安全和光纤通信.

朱飞男, (1979-), 讲师. 研究方向为网络安全和云计算.

(上接第 190 页)

(2) 对文中的办法用更多的实际系统进行验证, 发现问题, 改进方法.

参考文献:

- [1] 木村隆洋, 中村匡秀, 井垣宏, 松本健一, “データ依存解析に基づくレガシーソフトウェアからのサービス提取法,” 信学技報 ソフトウェアサイエンス研究会[J]. 2005(45): 13-18.
- [2] Papazoglou M P, Georgakopoulos D. Service Oriented Computing[J]. Communications of the ACM, 2003, 46(10): 25-28.

[3] 牧野友紀. ビジネス環境と実装システムを繋ぐ BPM と SOA[J]. 情報処理, 2005, 46(1): 60-63.

[4] 田中 秀一郎. サービス指向に基づくビジネスプロセス分析方法論[D]. 日本: 日本南山大学, 2006.

作者简介:

车战斌男, (1964-), 博士, 副教授. 研究方向为分布式系统、分布式数据库.

韩玉民男, (1963-), 本科, 高级工程师. 研究方向为软件开发技术、软件技术教育.

邢颖女, (1985-), 硕士, 助教. 研究方向为网格计算与云计算.