



虚拟化安全——公有云安全的核心关键问题

江家仁^{1,2}

- (1. 移动互联网系统与应用安全国家工程实验室 上海 201315;
2. 中国电信股份有限公司上海研究院 上海 200122)

摘要:在全球信息化的普及和信息技术蓬勃发展的背景下,使用面向社会与公众的云计算应用与服务已经成为企业发展的趋势和必然,并且公有云在企业发展中的作业也越来越巨大。对公有云的安全现状进行梳理,总结了目前公有云面临的主要安全技术问题,分析了每种技术的优缺点,指出了关键核心与安全前提是虚拟化安全,并对当前形势下公有云的安全防范策略提出建议。

关键词:公有云;虚拟化安全;数据安全

doi: 10.11959/j.issn.1000-0801.2015335

Virtualization Security, Key Issues of Public Cloud Computing Security

Jiang Jiaren^{1,2}

- (1. National Engineering Laboratory for Security of Mobile Internet System and Application, Shanghai 201315, China;
2. Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China)

Abstract: With the prosperous development of information technologies and popularity of information-based on a global basis, public application and service of cloud computing has become a trend and inevitable part of enterprise growth. Only an enterprise is speeding up the process, which is playing an increasingly important role in the enterprise growth. The security status of public cloud computing was firstly analyzed. Several important technologies were introduced, particularly concerning their dominant positions and inferior strengths. Finally, according to the in-depth research analysis and practical strategies, the protection measures for public cloud computing have been proposed.

Key words: public cloud, virtualization security, data security

1 引言

随着面向社会与公众的云计算应用与服务(以下简称公有云)的不断推广,公有云的安全逐渐成为社会企业及安全业界关注的重点,一方面由于公有云的计算与应用具有无边界性、流动性等特点,容易引发新的安全问题;另一

方面公有云的计算技术也对传统安全技术及应用产生了深远的影响。从完整意义上来说,公有云的安全应该包括两个方面的含义:一种是“云上的安全”,即公有云自身的计算与应用安全,如公有云系统平台及服务的安全、公有云的信息数据安全等;另一种是公有云的计算技术在安全领域的具体应用,即通过采用分布式计算技术来提升安全

收稿日期:2015-11-15;修回日期:2015-12-14

论文引用格式:江家仁. 虚拟化安全——公有云安全的核心关键问题. 电信科学, 2015335

Jiang J R. Virtualization security, key issues of public cloud computing security. Telecommunications Science, 2015335



系统的服务效能,如基于分布式计算的病毒防范技术、木马检测技术等。前者是公有云平台上各类业务应用可持续发展的基础,后者则是当前安全领域服务的技术热点。这里着重研究前者,并探讨公有云中与安全密切相关的核心关键问题。

在公有云环境中,用户不再拥有基础设施的硬件资源,软件都运行在云中,业务数据也存储在云中,公有云的安全性关系到对整个计算平台的系统级安全评价是否能够到达被业界接受的水平。公有云的安全技术研究主要包括虚拟化安全、管理安全、数据安全等几个方面,需要做到“云计算虚拟化环境可信,云计算数据的整个生命周期可控,安全管理体系可执行”,其中关键核心与安全前提是虚拟化安全,因为只有先解决了这一问题,公有云自身的环境特有的安全问题才能够逐步地、完整地得以解决,有效地改变现有的软件系统安全防护模式。

2 安全现状分析

公有云的虚拟化安全主要解决的是资源虚拟化过程中的虚拟机保护问题,尤其是对应网络、应用以及数据的安全隔离应作为本年度的重点工作来抓。以公有云为基础的虚拟化技术,如系统级虚拟机(包括VMware、Xen、Denali、KVM和User Mode Linux等),受到了越来越多的关注并得到越来越广泛的应用。与传统计算机系统相比,虚拟化技术具有许多优点,如提高了硬件利用率、更便于软件开发测试环境的部署以及通过隔离性提高了安全保障等。但它也带来了一些新的安全问题。用户通过操纵文件创建、复制、存储、读写、共享、移植和回滚运行状态,增强了使用的灵活性,但是却影响了传统系统的线性时间变化特征,从而也影响到它的安全策略和机制的有效性。目前,虚拟机在实际应用中已占相当大的比例,逐渐成为攻击者的目标。参考文献[1]中已出现的入侵或破坏虚拟化环境的案例几乎涉及所有知名的商业和开源虚拟化技术,如VMware、虚拟PC和Xen等。增强虚拟机技术的安全性和构建可信的虚拟化环境已经成为业界的迫切需求。虽然虚拟机具有良好的隔离性,但在很多应用上,必须进行虚拟机间的通信,而虚拟机间频繁的交互带来了新的安全问题。

2.1 虚拟机隔离与管控问题

在服务器虚拟化环境中,在同一平台上会同时运行着来自于不同用户的虚拟机。无论是从保护用户隐私的角度还是保证平台虚拟环境安全的角度,都存在着隔离的需

求。例如,参考文献[2]VMware在vSphere4中推出了分布式虚拟交换机(vDS)。它的实现机制是分离了交换机的数据功能和控制功能。虽然数据功能还是由主机上的虚拟交换机来处理,但是控制功能都被集中起来移至主机之外,并将其安装在一个特制的虚拟机内。然而隔离所采用的方法并不是像传统方式那样采用网线、交换机或者防火墙等物理手段,只能依靠虚拟机监控器和一些软件模块来实现。这就要求管理者必须正确严格地划分虚拟区间,随时监控虚拟机状态。如果将不同安全级别(或信任级别)的应用放在了同一台物理机上,而没有加以隔离,就会产生数据泄露或系统全面瘫痪的严重后果。

虚拟机的隔离性使不同的客户能在互不干扰的情况下分享主机资源。然而,由于技术的限制和虚拟化软件的漏洞,最终往往并不一定能够达到理想的隔离效果。在某些情况下,客户虚拟机中运行的用户程序可以绕过底层,从而控制宿主机,导致虚拟机逃逸。并且,由于宿主机的特权地位,会使整个公有云的安全体系面临威胁。管理程序设计过程中的安全隐患会传染到同物理主机上的虚拟机,这种现象被称作“虚拟机溢出”。如果虚拟机能够从所在管理程序的独立环境中脱离出来,入侵者会有机可乘,进入控制虚拟机的管理程序,进而避开专门针对保护虚拟机而设计的安全控制系统。虚拟世界的安全问题正在试图脱离虚拟机的控制范围。

2.2 云平台中数据泄露的威胁

在公有云系统平台的安全中,攻击平台的存储系统是非法入侵的重要环节,也是在构建安全防护体系时需要着重考虑的环节。首先,平台对存储的需求主要体现在多种数据格式的适应能力。格式多样化是云平台数据的主要特征之一,这就要求平台存储管理系统能够适应对各种非结构化数据进行高效管理的需求。其次,为公有云平台的存储设计数据存储管理系统,开源的系统架构如Google BigTable和Hadoop HBase等非关系型数据库(NoSQL),通过使用“键-值(key-value)”结构、文件结构等非二维表的结构,能够适应非结构化数据多样化的特点。同时,面向分析型业务,以降低一致性为代价提升并发性能,并逐步把关系型数据库的操作便捷性特点和非关系型数据库灵活性的特点结合起来。但因此也带来新的安全威胁,主要包括以下几点。

(1)模型成熟度不够

目前的SQL技术标准具有严格的访问控制和权限管

理机制,而在 NoSQL 模式中,并没有这样的要求。事实上, NoSQL 无法沿用 SQL 的模式,需要重新为其新的属性定义安全策略。例如,与传统 SQL 数据存储相比,在 NoSQL 数据存储中,列和行级的安全性更为重要,修改行列属性应该得到约束,需重新设计保护策略。

(2) 系统成熟度不够

与关系型数据库系统相比, NoSQL 及其文件服务器系统的安全机制远未到达成熟期,系统容易产生漏洞,虽然 NoSQL 可以从传统的关系型数据库安全设计中学习经验并不断改进,但至少目前市面上很多 NoSQL 产品和应用程序仍然存在着各种漏洞。

(3) 数据冗余和分散性问题

公有云平台采用的非关系型数据库的优势是扩展简单、读写快速和成本低廉,但由于未提供对 SQL 的支持,缺乏强有力的数据库范式算法支撑,加之与关系型数据库数据存储位置相对集中不同,非关系型数据库数据分散在不同的地理位置、不同的服务器中,较难实现数据的完整性检验。

3 安全防范策略与建议措施

尽管没有哪家公司会允许安全问题通过管理程序技术的方式在虚拟主机间相互传播和蔓延,但这样的安全隐患还是存在的。因为入侵者或者安全漏洞会在虚拟机之间来回捣乱,这将成为开发者在开发过程中必须面对的问题。参考文献[1]中提到现在技术工程师通常采用隔离虚拟机的方式来保障虚拟环境的安全性。保障虚拟环境安全的传统方式是在数据库和应用程序层间设置防火墙。从网络上脱机保存虚拟化环境有助于缓解安全隐忧。这对于虚拟化环境来说是比较好的方法。

因此,公有云的安全应重点聚焦虚拟机管控与云平台数据安全,解决其中突出的安全问题,可以采用以下几种方法和安全软件一起来保护虚拟机。

3.1 加强硬件隔离,执行虚拟机严格管控

将虚拟机监控器从可信计算机中移除,通过硬件加强隔离^[3]。由于虚拟机监控器的代码量巨大且复杂,在进行漏洞检测和修改时的难度较大,虚拟机监控器很容易就会成为攻击者利用的对象。攻击者可以通过一台用户虚拟机潜入虚拟化环境,对虚拟机监控器进行攻击并将其俘虏,然后利用该不可信的虚拟机监控器对虚拟化平台上运行着的其他用户虚拟机进行攻击。因此,在进行虚拟化环境安

全性保护的过程中,将虚拟机监控器排除在可信计算机之外是很有必要的。采用软件的方式进行隔离,并不能达到有效的物理强隔离效果。攻击者仍然可以通过各种手段来破解基于纯软件的隔离机制,非法访问或截获宿主机内存、用户虚拟机内存。因此,纯软件的解决方案不足以充分保护虚拟化环境的安全,想要达到理想的强隔离效果,只有利用硬件资源来实现对宿主系统、虚拟机监控器和用户虚拟机的有效物理隔离。

通过访问控制与身份认证,加强虚拟机管控。通过禁止对用户虚拟机进行非授权的访问,可以在一定程度上保护虚拟化环境的安全性。为了保护用户的虚拟机内存不被非法访问,可以对用户的虚拟机内存进行访问控制。除了通过虚拟机监控器以外,不允许其他任何形式的对虚拟机内存的访问。对虚拟机内存进行访问控制在一定程度上防止了虚拟机内存的数据泄露,但是仍然存在一种可能性会危害到系统的安全性。这就是攻击者可能会利用虚拟机监控器的漏洞将其俘虏,然后利用虚拟机监控器在虚拟化环境中的最高特权,对运行在同一主机上的用户虚拟机进行攻击或查看用户虚拟机的内存,破坏虚拟化环境的安全性。控制所有用户对资源池管理工具的访问,只有被信任的用户才被授予权限来访问资源池组件,例如物理服务器、虚拟化管理程序、虚拟网络、共享存储等。向未被认证的用户开放资源池管理工具的访问权限,就等同于向那些恶意操作开放了系统。控制对虚拟机文件的访问,通过合理的认证机制和访问控制来确保所有包含了虚拟机的文件夹以及虚拟机所在压缩文件的安全。所有的虚拟机文件,无论是打开的还是关闭的,都必须获得严格的管理和控制。

3.2 公有云平台的数据安全机制

公有云的安全关键在于数据分析和利用,因此不可避免地增加了平台上数据的安全风险,应重点考虑 Hadoop 的非关系型数据库安全机制的运用。

建议在公有云系统平台中采用 Hadoop HBase,能够为 NoSQL 提供一些安全方面的支持,包括基于 ACL 的服务级权限控制、基于令牌的认证机制、基于 HDFS 云存储的完整性验证等。通过 ACL 的服务级权限控制, Hadoop 能够保证 HBase 数据库底层 HDFS 的服务级安全访问,并且通过用户和组的限制,防止攻击者对数据进行操作。文件的权限主要由 NameNode 管理,通过令牌认证机制保证私密性, NameNode 周期性地更新 masterKey 来产生新的授权令牌, HDFS 集群启动时从 NameNode 中获得密钥(key)来实



现认证。数据完整性方面的保障通过 HDFS 的云存储完整性验证来实现,主要技术手段是通过核心类 DataBlockScanner 实现,它能够在 DataNode 的后台执行一个独立的扫描线程,周期性地对数据进行 CRC 校验和检查,确保 HDFS 中云存储的完整与安全。此外,运用 HDFS 优化副本保存和备份的机制,尤其对于核心数据启用远程容灾备份和其他额外的数据备份与恢复,能够提高数据的可靠性和可用性,实现数据的可靠保护。

4 结束语

在全球信息化的普及和信息技术蓬勃发展的背景下,使用公有云的应用与服务已经成为企业发展的趋势和必然。许多企业都通过使用公有云平台来加快信息化的进程,从而在激烈竞争的市场中占据一席之地,并且公有云在企业发展中的作业也越来越巨大,同时市场也要求公有云能够达到以虚拟化安全为关键核心,实现虚拟化环境可信、数据的整个生命周期可控、安全管理体系可执行等一系列安全要求。虽然公有云面临着复杂的安全挑战,但用户可以充分利用多处理器、多核体系结构和虚拟化软件提供安全机制对其进行防护。此外,现

在和将来都可以通过采用由诸如 Vshield API 在虚拟化平台中的不断演化来实现安全性增强策略,从而保护虚拟化 IT 资源。

参考文献

- 1 Erl T, Mahmood Z, Puttin R. Cloud Computing Concepts, Technology & Architecture. Upper Saddle River: Prentice Hall Press, 2013
- 2 吴朱华. 云计算核心技术剖析. 北京: 人民邮电出版社, 2011
Wu Z H. Cloud Computing Core Technology Analysis. Beijing: Posts & Telecom Press, 2011
- 3 Vic W. Cloud computing: virtual cloud security concerns. Microsoft Technet Magazine, 2012, 32(13)

[作者简介]



江家仁,男,移动互联网系统与应用安全国家工程实验室、中国电信股份有限公司上海研究院高级工程师,主要从事移动互联网安全技术及安全产品攻防技术方面的研究工作。