DOI:10.19789/j.1004-9398.2015.04.005

云计算中虚拟化技术的安全问题及对策研究

王丽丽

(宝鸡职业技术学院电子信息工程系,陕西 宝鸡 721008)

摘 要

虚拟化技术在云计算中发挥着重要作用,云计算通过虚拟化技术提供灵活高效的应用服务.在分析云计算中虚拟化技术体系结构的基础上,本文分别从虚拟机硬件设备、虚拟机监控软件和虚拟化操作系统三个方面,阐述了虚拟化技术所面临的安全威胁,最后提出了相应的安全防护对策.

关键词:虚拟化技术,云计算,安全.
中图分类号:TP31

0 引 言

云计算以其低成本、灵活性、可伸缩性、可靠性、自适应性、多租户等特点已被广泛接受和应用.云计算通过软件、平台和基础设施三个层次服务等级,提供一个服务集合.软件即服务 SaaS(Software as a Service)是以互联网为载体,把各种软件和应用程序部署在云端,用户随时可用的一种软件服务模式.平台即服务 PaaS(Platform as a Service)依托基础设施即服务 IaaS(Infrastructure as a Service)平台,面向互联网应用开发者,把软件开发、测试、部署和运行环境提供给用户.IaaS 包括各种硬件和基础软件资源,以服务的形式为用户提供网络、处理、存储和基础计算资源.在云计算中,各种数据、服务和应用都存储在云中,云就好像是用户的"超级计算机".因此,云计算要求这个"超级计算机"能够统一管理所有的资源.但是,各种硬件设备之间的差异导致它们之间很难兼容,这为统一的资源管理提出了挑战[1].

虚拟化技术可将物理资源等底层架构进行抽象,使硬件设备之间的差异和兼容性对上层应用透明,从而实现云对底层各类资源的统一管理.虚拟化技术是一种调配计算资源的方法[2],它能将应用系统的不同层次(硬件、软件、数据、网络、存储等)进行隔离,从而打破数据中心、网络、服务器、数据、应用和存储中的物理设备之间的划分,实现统一管理和动态使用物理资源和虚拟资源,提高了系统结构的灵活性和弹性.

目前,关于云计算中虚拟化技术的安全问题已有很多的研究,如:美国国家标准与技术研究院[3]、支付行业数据安全标准[4]和云安全联盟[5]等都对其进行了相应研究,并提出了安全的云虚拟化环境.本文在分析云计算中虚拟化技术体系架构的基础上,分别从虚拟机硬件设备、虚拟机监控软件和虚拟化操作系统三个方面阐述了虚拟化技术面临的威胁,最后提出了相应的安全防护对策.

1 云计算中虚拟化技术面临的安全威胁

建立的云计算中虚拟化技术体系结构如图1所示,其中虚拟机监控软件 VMM(Virtual Machine Monitor)允许多个操作系统和应用共享硬件设备,是一种运行在底层虚拟机硬件设备和操作系统之间的中间软件层.

1.1 虚拟机硬件设备面临的安全威胁

云计算是将信息资源和数据计算交换分布在大量联网计算机上,用户通过按需访问存储系统和联网的计算机,从而获得信息交换和海量数据运算的功能.云计算的这种模式将原来局限在内部网络中的资源和数据暴露在公共网络中[6].如果攻击者物理接入云的硬件设备,通过执行恶意程序代码,修改虚拟机的源程序并改变其功能,达到攻击虚拟机的

收稿日期:2014-03-07

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

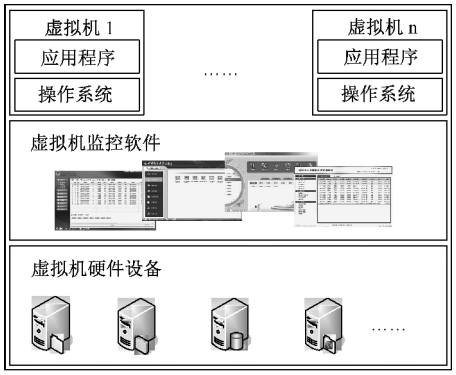


图 1　云计算中虚拟化技术体系结构

目的. 在网络层面上,云计算将面临域名服务 DNS(Domain Name Service) 攻击、拒绝服务 DoS(Denial of Service) 攻击、网络可达性攻击等多种安全威胁.

1.2　虚拟机监控软件面临的安全威胁

虚拟机监控软件 VMM (Virtual Machine Monitor) ,或称为 Hypervisor. 它可以访问服务器上的所有硬件设备. 当服务器启动并调用 Hypervisor 时,它会加载所有虚拟机客户端上的操作系统,同时给每个虚拟机分配适量的网络、CPU、磁盘和内存等物理资源. Hypervisor 负责协调这些硬件资源的访问,同时也在每个虚拟机之间施加安全防护.

在云计算服务中,资源是以虚拟、租用的模式提供给用户,这些虚拟资源根据实际需要与物理资源绑定. 在云计算中多个用户共享资源,多个虚拟资源很可能被绑定到相同的物理资源上. 如果云服务平台中的虚拟机监控软件存在安全漏洞,那么用户的数据就可能被其他用户访问.

在云虚拟环境中,大量的操作系统可以同时运行在同一个使用 Hypervisor 的主机服务器上,随着在同一个 Hypervisor 上运行的用户操作系统的数量不断增加,Hypervisor 所面临的威胁也就越大. 一旦攻击者控制了 Hypervisor,就能轻易地改变用户的操作系统,并且控制整个 Hypervisor 监控的资源.

1.3　虚拟化操作系统面临的安全威胁

虚拟化操作系统是在虚拟机监控软件层上采用虚拟化技术生成的操作系统. 除了和传统操作系统一样,受到病毒感染、系统漏洞等安全威胁外,虚拟机若从一个物理主机迁移至另一个主机后,原来主机的硬盘上仍保留有虚拟化操作系统的痕迹,即使将其从硬盘上删除或格式化,攻击者依然能通过恢复技术从该主机硬盘上获取有用的数据和信息.

2　云计算中虚拟化技术安全防护对策

基于虚拟化技术的云计算可能会带来多种安全威胁,通常采用以下几种安全防护对策来构建多层次的防范体系.

2.1　虚拟化硬件设备的安全防护对策

在硬件设备方面,应选用可信赖的安全模块 TPM(Trusted Platform Module) 的物理服务器,该模块在虚拟服务器启动时进行用户身份验证,若用户未通过身份验证,则不允许启动该虚拟服务器. 为保证服务器 CPU 之间的物理隔离,选择的 CPU 应支持硬件虚拟化技术,这样可减少许多安全隐患. 此外,在虚拟服务器的安装过程中,为每台虚拟服务器各划分一个独立的硬盘分区,实现从逻辑上隔离各虚拟服务器.

对物理主机的安全防护可采用传统的防护措施,如: 杀毒软件、防火墙、主机防御系统等. 为了避免被攻击后的某台虚拟服务器影响到物理主机,可以在物理主机上只运行虚拟服务软件,严格控制其运行的数量,同时禁止其它网络服务在该物理主机上运行. 通过虚拟专用网络 VPN[7] (Virtual Private Network) ,可以实现物理主机与虚拟服务器的连接或资源共享,并且可以采用加密的网络文件系统方式进行资源共享.

2.2　虚拟机监控软件的安全防护对策

虚拟机监控软件位于底层硬件设备和虚拟化操作系统之间,监控和管理虚拟化操作系统. 为确保该层的安全,严格审核访问用户的权限,任何未经授权的用户禁止访问虚拟化软件层,而对于有权限访问的用户,必须完整保存其对虚拟化软件层的访问记录,以便执行审计.

2.3　数据的安全防护对策

采用加密技术对存储在云中的数据进行加密处理,防止恶意的云“租户”和云服务提供商的滥用、保护数据的安全性. 传输数据时,应采用加密的协议,如: 安全复制协议 SCP(Secure Copy Protocol) 、安全超文本传输协议 HTTPS (Hypertext Transfer Protocol over Secure Socket Layer) 等,能够保护数据的机密性和完整性.

2.4　虚拟化操作系统的安全防护对策

一方面,当虚拟机迁移至另外的物理主机时,云管理员必须确保先前的物理主机硬盘上的数据被彻底擦除,或将硬盘物理销毁. 同时,为每个虚拟化操

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

作系统安装基于主机的杀毒软件、入侵检测和入侵防御系统、防火墙等. 此外,在使用虚拟机过程中,要对一些重要的虚拟机镜像文件进行加密处理,防止文件被窃取.

另一方面,建立镜像文件库,用于保存一些重要的虚拟机镜像文件和虚拟化操作系统的备份文件,以防止虚拟化操作系统的崩溃或被攻击造成的瘫痪. 对该镜像文件库进行访问控制,防止非法用户的访问和窃取[8]. 同时,要定期对镜像文件库进行病毒扫描和漏洞修复. 并建立镜像文件库信息记录表,如下表 1 所示,精确记录每个镜像文件的名称、发布人、访问人,访问内容和访问时间等信息,以便系统的安全跟踪. 在此基础上,建立镜像文件库的发布和访问机制,如下图 2 所示.

表 1 镜像文件库信息记录表

镜像文件名称	文件发布人	文件访问人	访问内容	访问时间
VM	A	B	云计算资料	2014. 2. 3(10:02 – 11:20)
……	……	……	……	……

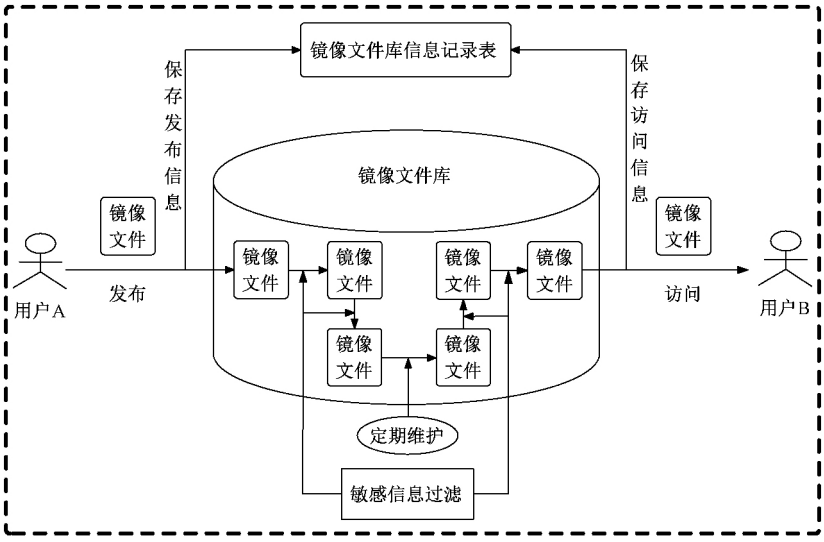


图 2 镜像文件库发布和访问机制

在虚拟化操作系统中,当用户 A 发布镜像文件或用户 B 访问镜像文件时,通过镜像文件敏感信息过滤,删除掉涉及用户隐私等的敏感信息. 每当用户发布和访问镜像文件时,操作系统将发布和访问的信息保存至镜像文件库信息记录表中,以便今后系统安全跟踪. 此外,要对镜像文件库进行定期的病毒扫描和维护,防止被病毒感染.

2.5 用户的安全防范对策

要提高云计算虚拟化技术的安全性,仅仅依靠以上几种对策还不够,还需要用户提高防范意识,尽量避免涉密或涉及个人隐私的资料存储在云端. 此外,对登录云服务的用户进行身份认证,严格验证程序,防止恶意人员的非法入侵.

随着云计算的快速发展,仅仅依靠云计算提供商的自觉性已无法从根本上解决云计算的安全问题. 除此之外,还应从法律法规角度对云计算进行安全防护,这就需要国家和政府或相关权威部门制定云计算安全环境的运行机制,对云计算服务提供商进行检查和监督,强制要求云计算提供商采取必要的安全措施,保证云服务的安全性.

3 结束语

虚拟化技术打开了云计算的“大门”,从本质上讲,云计算为我们提供的是虚拟化云服务. 虚拟化技术的成熟和广泛应用,推动了云计算的变革和发展,可以说,虚拟化技术是云计算发展的关键因素. 而云计算中虚拟化技术的安全问题也是制约云计算发展的重要问题,只有研究和解决好这些问题,才能不断完善和发展云计算.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

参 考 文 献

[1] 王庆波,何乐,赵阳等. 虚拟化与云计算[M]. 北京: 电子工业出版社, 2009: 132 – 133.

[2] 张为民,唐剑峰,罗治国等. 云计算深刻改变未来[M]. 北京: 科学出版社, 2010: 71.

[3] Sherif Sakr, Liu Anna, Batista Daniel M, etc. A Survey of Large Scale Data Management Approaches in Cloud Environments[J]. IEEE COMMUNICATIONS SURVEYS & TUTORIALS. 2011,13(3): 312.

[4] Jason Lackey. Virtualization and PCI DSS[OL]. [2010]. http://blogs.cisco.com/security/virtualization-and-pci-dss-1-2-1.

[5] Muhammad Kazim, Rahat Masood, Muhammad Awais Shibli, etc. Security Aspects of Virtualization in Cloud Computing[C]. Poland: [Computer Information Systems and Industrial Management], 2013.

[6] 熊家军,李强. 云计算及其军事应用[M]. 北京: 科学出版社. 2011: 150.

[7] Surya Nepal, Mukaddim Pathan. Security, Privacy and Trust in Cloud Systems[M]. Germany: Springer, 2013: 16.

[8] Chirag Modi, Dhiren Patel, Bhavesh Borisaniya etc. A survey on security issues and solutions at different layers of Cloud computing[M]. Germany: Springer, 2013: 580.

Research for Security Problems and Countermeasures of Virtualization Technology in Cloud Computing

Wang Lili

(Electronic Information Engineering Department, Baoji Professional Technology Institute, Baoji 721008)

Abstract

Virtualization technology plays an important role in cloud computing. Cloud computing provides flexible and efficient application services based on virtualization technology. Basing on the analysis of virtualization technology architecture in cloud computing, the security threat faced by the virtualization technology is described, from three aspects of virtual machine hardware equipment, virtual machine monitor and virtualized operating system. Finally, corresponding safety protection measures are proposed.

Key words: Virtualization Technology, Cloud Computing, Safety.

(C)1994-2020 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net