基于等级保护基本要求的云计算安全研究

朱圣才
(上海市信息安全测评认证中心,上海 200011)

摘 要：随着云计算的进一步推进和发展,云计算面临的安全问题变得越来越突出,特别是在云计算安全中的用户数据机密性、完整性和可用性方面尤为突出，云计算安全已经成为云计算推进过程中的首要障碍和难题。从云计算应用安全和系统安全两个层面，提出了云计算安全中应用安全和系统安全的威胁所在以及相应的基本保护要求。

关键词：云计算;云安全;应用安全;系统安全;分类保护
中图分类号：TP309 **文献标识码**：A **文章编号**：1674-7720(2013)14-0003-04

Research of Cloud Computing Security based on classified protection

Zhu Shengcai
(Shanghai Information Security Testing Evaluation and Certification Center, Shanghai 200011, China)

Abstract: With further promotion and development of cloud computing, the security problems faced by cloud computing are becoming more and more prominent, especially in user data confidentiality, integrity and availability, Cloud Computing Security is more prominent, Cloud Computing Security is becoming the primary obstacle and problems in the promoting process of cloud computing. At the two levels of applications security and system security of Cloud Computing, this paper proposes the locality of threat to application security and system security and protection requirements to these threats.

Key words: Cloud Computing; Cloud Security; application security; system security; classified protection

云计算的目标是实现将各种共享的IT计算资源以服务的方式通过互联网交付给终端用户使用。云计算以其特有的优势逐步赢得了信息技术市场的认可,与此同时,云计算的出现也在不知不觉中掀起了一场IT技术革命。云计算的显著优势包括按需服务、高带宽网络接口、共享资源池、快速可伸缩性和服务可测量等特点[1-6]。

在传统的计算模式下,用户对数据的存储与计算拥有完全的控制权,由于传统信息系统的等级保护在等级保护基本要求中都有非常具体的体现,使得传统信息系统的整体安全性在一个可以控制的范围中;而在云计算模式下,用户数据与机器的管理将完全依赖于与计算服务提供商，终端用户仅仅保留对虚拟机的控制权限,使得信息系统的安全性出现了一些不可控的因素,在这种服务模式下,终端用户完全有可能不知道服务提供商的系统的物理地点和系统配置等详细内容。这种不可控因素的存在导致了云计算安全成为云计算推广过程的首要障碍和难题[7-10]。

本文从等级保护基本要求出发,结合云计算技术现状分析与研究,从等级保护基本要求的应用安全和系统安全两个层面，探讨如何在云计算平台下实施等级保护,为实现云计算平台下信息系统安全的可控性抛砖引玉,并且针对等级保护基本要求给出了具体的操作方式和解决方案。

1 云计算中的应用安全

本文从应用安全角度分析云计算中应用安全威胁,在等级保护基本要求框架下针对威胁给出具体的解决方法,为实现云用户安全目标提供技术支撑。

1.1 云计算中应用安全威胁

在大量研究CSA相关成果及CAM标准的基础上,结合上海市“云海”项目的研究,以及2013年7月微软将在上海部署微软云计算数据中心和OFFICE365项目的研究，给出云计算中应用安全主要面临的威胁及描述,如表1所示。

1.2 云计算中应用安全基本保护要求

根据《信息系统安全等级保护基本要求》(GB/T22239:2008)控制层面、控制点和控制项的框架,给出针对云计算中应用安全的基本要求,具体如表2所示。

2 云计算中的系统安全

云计算安全中系统安全很大程度依赖于云服务商的云服务能力和云服务架构,依据《信息系统安全等级

表 1 云计算中应用安全威胁分析表

编号	威胁名称	威胁描述
T1	云应用存在的安全漏洞	云服务商提供的云应用软件未进行安全性管理和技术防护，使得云应用本身的不成熟给用户带来的安全性威胁
T2	云应用操作数据时存在安全漏洞	用户通过云应用程序访问数据时，数据在内存处理中存在数据被窃取的威胁，使得用户在内存中操作数据存在不安全性
T3	特殊云应用和一般云应用混淆存在的安全漏洞	一般云应用程序的安全性要求比较低，如果在同一个虚拟机上运行，可能危害特殊云应用程序的正常运行和安全，导致信息安全事件的发生和用户数据的不安全性
T4	敏感数据和非敏感数据混淆存在的安全漏洞	非敏感数据的安全性要求比较低，如果在同一台虚拟机上或者同一台物理设备上存储，或者通过相同的协议和通道进行数据传输，可能会导致敏感数据的保密性、完整性、可用性等威胁
T5	云应用的密钥管理和证书安全	如果云应用的密码保管泄露或者证书失效以及篡改，将造成整个云应用不安全，给用户带来安全性威胁
T6	云应用日志泄露	多租户运行的平台，对各种云应用，是否只能各自管理自己的云应用日志，是否对云应用日志进行了分级管理和保护，是否对云服务商对日志的管理进行了监督，如果存在跨权访问或者不正常操作，可能造成敏感数据泄漏，导致用户损失
T7	云应用进行动态迁移时可用性和性能是否稳定	云应用在虚拟机系统上进行动态迁移时，该云应用的稳定性和性能是否能够达到正常要求，是否会对当前应用服务造成中断，进而造成用户损失
T8	云应用退出时，该应用是否进行数据销毁	当租户准备从云计算中退出服务时，如何保证租户撤出云服务的同时，存储在云服务中的应用和数据彻底销毁，如果缺少必要的技术和管理手段将导致用户数据存在安全性威胁

表 2 云计算中应用安全基本要求

编号	威胁编号	控制层面	控制点	云计算安全要求	云计算安全方法
R1	T1	应用安全	访问控制	对云应用的可用性和完整性进行验证，保证云应用程序的可持续使用	检查云服务商提供云服务应用程序的功能、性能测试报告，并对相应的内容进行验证
R2	T2	应用安全	数据保密性	保证数据在传输过程中和内存中的安全性和保密性	在传输层进行加密传输，对虚拟机进行隔离，对处理数据进行实时加解密，保证数据安全
R3	T3	物理安全	位置选择	云应用产生的敏感数据和非敏感数据应存放在不同的物理存储设备上	对数据中心、敏感数据服务器和非敏感数据服务器进行区分
R4		网络安全	结构安全	云应用产生的敏感数据和非敏感数据在网络结构上进行逻辑隔离，区分各自的传输通道	对云应用产生的数据传输，定义不同的传输通道级别，分配不同的通道进行传输处理，并进行加密和隔离操作
R5	T4	物理安全	位置选择	参见 T3 对应的云计算安全要求	参见 T3 对应的云计算安全方法
R6		网络安全	结构安全		
R7	T5	应用安全	访问控制	确保云应用密钥和证书管理安全和分级保护	将系统和云应用的密钥和证书分开管理，对密钥和证书管理使用密文管理与分级保护
R8	T6	应用安全	访问控制	要求实现应用程序日志管理的审计和监控管理，对日志访问控制有权限分级	云应用日志分级管理，并且不可以进行修改和删除，不可以进行越权访问，对敏感数据日志进行加密处理
R9	T7	应用安全	持续可用性	要求云应用进行动态迁移时保证该云应用的正常运行	检查云服务商提供的方案是否满足要求并测试
R10	T8	应用安全	剩余信息保护	保证云应用退出服务时所有数据彻底销毁	检查云服务商提供的销毁技术手段并测试

保护基本要求》，分析系统安全威胁弱点所在和基本要求是对云计算安全的基本保障。本章依据微软 Windows Azure 平台中分析的系统弱点和对应的基本要求进行总结分析，给出具体的威胁分析表和基本保护要求表。

2.1 云计算中系统安全威胁

针对 Windows Azure 云计算平台中系统安全，分析研究得出 Windows Azure 系统安全的威胁如表 3 所示。

2.2 云计算中系统安全基本保护要求

根据《信息系统安全等级保护基本要求》(GB/T22239：2008)控制层面、控制点和控制项的框架，给出针对 Windows Azure 云计算平台中系统安全的基本要求，具体如表 4 所示。

3 云安全

云计算等开放网络服务环境的安全问题成为企业是否采用云计算等开放网络服务的重要疑虑之一。关注基于云计算等开放网络服务的 IT 应用中的安全设计并去解决开放网络服务所引发的安全问题势在必行。其中重点需要解决的是可信问题，因为开放网络服务的模式改变了传统 IT 环境的可控性，使得针对传统信息系统构建模式的“等级保护”、“分级保护”等安全增强方法难以奏效。如何使各类云计算安全提供足够的可信度并能够提供用户足够的可控性是亟待解决的问题。

经过对云计算各类安全需求和机制的研究，总结出云计算安全防护机制的总体框架如图 1 所示。

图 1 是对云计算安全问题的归纳总结，并且创新地为每个安全问题划分了对应的层次，例如“数据安全”对应的层次是客户端到 IaaS，而“应用安全”对应的层次是客户端到 SaaS。

本文从信息系统等级保护基本要求研究云计算平台下如何实施传统可控的信息系统等级保护；另外，本文还结合了微软 OFFICE365 项目和微软 Azure 云计算平台，研究云计算中关于应用安全和系统安全两个具体关注点，给出两个层面的威胁点，并依据《信息系统安全等级保护基本要求》(GB/T22239：2008) 要求下给出威胁点的具体基本保护要求，从等级保护角度探索解决云计算安全的整体解决方案，进一步促进云计算安全走向成熟。

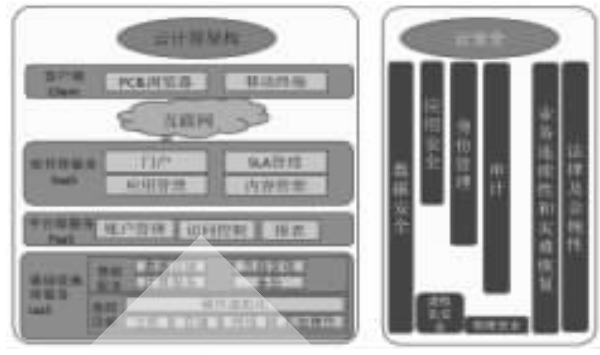

图 1 云计算安全机制框架

参考文献

[1] CSA.云计算关键领域安全指南 V2.1[Z]. 2010.

[2] 中华人民共和国国家标准《信息系统安全等级保护基本要求》(GB/T22239：2008)[S]. 2008.

[3] ENISA.云计算合同安全服务水平监测指南[Z].2012.

[4] JOHN R, JAMES R. Cloud computing: implementation, management, and security[M]. Beijing:China Machine Press, 2010.

[5] RINGS T, GRABOWSKI J, SCHULZ S. Grid and cloud computing: opportunities for integration with the next generation Network[J]. Grid Computing, 2009(7)：375-393.

表 3 云计算中系统安全威胁分析表

编号	威胁名称	威胁描述
T1	虚拟机系统加固方案不是最佳	运行在 HOST OS 上的虚拟机，对虚拟机的加固方案是否达到预防安全漏洞的要求，对不同应用的不同虚拟机加固方案是否存在特殊的固定配置，如果虚拟机被恶意进入，则会导致用户数据被获取、泄漏
T2	对虚拟机系统的密钥管理和证书安全	如果虚拟机系统的密码保管泄露或者证书失效以及篡改，将造成整个虚拟机中的所有云应用不安全，导致用户应用与数据的泄漏，造成客户损失
T3	虚拟机系统日志泄露	多租户运行的平台，对于各自的虚拟机平台，是否只能各自管理自己的虚拟机系统日志，是否对云服务提供商对系统日志的监控进行了实时监控，如果存在跨权访问，或者云服务提供商随意访问，可能造成敏感数据泄漏
T4	云计算中 HTTP 协议安全漏洞	Azure 服务是否启用传输安全(TLS)利用安全的 HTTP 协议(HTTPS)来传输加密的请求，加固 HTTP 协议安全
T5	HOST OS 安全漏洞	HOST OS 管控所有的虚拟机系统，Host OS 配置与防护是否合理，如果 Host OS 被非法访问，可能导致重大的信息安全事件
T6	加载虚拟机系统的完整性和合规性检测	HOST OS 上运行的 Guest OS，Host OS 加载 Guest OS 时，是否存在完整性和合规性检查，防止非法用户加载非法虚拟机系统，进而导致数据泄漏和非法利用云服务资源
T7	虚拟机系统外部接口控制	虚拟机外部有哪些安全控制来保护暴露给用户的管理接口，如果接口被非法利用，则会导致数据不安全甚至泄漏
T8	应用压力导致内存耗尽	大量云应用程序的使用，导致内存资源耗尽，造成系统崩溃、业务中断、服务中断，导致用户损失

表 4 云计算中系统安全基本要求

编号	威胁编号	控制层面	控制点	云计算安全要求	云计算安全方法
R1	T1	系统安全	访问控制	虚拟机系统不会被恶意进入，有较好的防护措施	检查云服务商对虚拟机系统的管控措施是否满足监管效果
R2	T2	系统安全	访问控制	确保虚拟机密钥和证书管理安全和分级保护	对虚拟机系统密钥和证书管理使用密文管理
R3	T3	系统安全	访问控制	要求实现虚拟机系统日志管理的审计和监控管理，对日志访问控制有权限分级，对云服务商对系统日志的监控实行实时监控	系统日志分级管理，区分开与应用日志的存储，并且不可以进行修改和删除，不可以进行越权访问，对敏感数据日志进行加密处理
R4	T4	系统安全	系统结构	要求对 HTTP 协议进行加密传输	使用 HTTTPS 加密协议进行加密传输，保证系统安全
R5	T5	系统安全	访问控制	Host OS 不会被恶意进入，有较好的防护措施和验证机制	检查云服务商提供 Host OS 的管控措施是否对 Host OS 进行了实时监控和安全审计
R6			安全审计	Host OS 操作必须存在必要的安全审计策略，保证云计算大环境的安全	在 Host OS 操作层设置安全审计，可以追溯过去并对 Host OS 操作进行实时监控
R7	T6	系统安全	系统完整性	要求 Guest OS 必须经过云服务商的授权和认证，并且具完整性和合规性检查	检查云服务商提供的授权和认证方式是否安全，并试图安装自己的 Guest OS 进行测试
R8	T7	系统安全	访问控制	对虚拟机对外接口进行访问控制，授权和监控	检查云服务商提供的对外接口的安全管控技术
R9	T8	系统安全	资源控制	要求超负荷的情况下，云服务商不中断各种云服务	超负荷应用访问系统资源，检查监控资源状态和服务器状态

[6] Zhang Liangjie, Zhou Qun. CCOA: cloud computing open-architecture[C]. Proc of 2009 IEEE International Conference on Web Services, New Youk: IEEE Computer Society Press, 2009:607-616.

[7] YOUSEF L, BULRICO M, SILVA D. Toward a unified ontology of cloud computing[EB/OL].(2010-xx-xx)[2013-01-10]http://www.collabogce.org/gce08/images/7/76/Lamia Yousef.pdf.

[8] 冯登国，张敏，张妍，等.云计算安全研究[J]. 软件学报，2011，22(01)：71-83.

[9] 陈尚义.浅谈云计算安全问题[J].网络安全技术与应用，2009(10):20-22.

[10] 李玮.云计算安全问题研究与探讨[J].电信工程技术与标准化，2012(4)：44-48.

(收稿日期：2013-03-28)

作者简介：

朱圣才，男，1986 年生，硕士研究生，主要研究方向：信息安全、虚拟化与云计算。