

面向安全风险的云计算测试技术研究

刘云龙, 曾 晋, 刘法旺, 李 维

(工业和信息化部计算机与微电子发展研究中心, 北京 100048)

摘 要: 对云计算安全问题进行了分析, 构建了云计算安全风险框架, 并给出了云计算安全测试技术路线, 在此基础上, 针对云计算渗透测试和数据残留检测, 提出了两种解决方案, 并成功应用于实际工程项目中。

关键词: 云计算; 安全风险; 安全测试; 云安全渗透测试; 数据残留风险检测

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2013)06-0015-04

Test Technology Research for the Security Risks of Cloud Computing

LIU Yun-long, ZENG Jin, LIU Fa-wang, LI Wei

(Research Center for Computer and Microelectronics Industry Development, Beijing 100048, China)

Abstract: Security testing is an important means to ensure cloud computing security and is the key of the system security. This paper analyzed the security issues of cloud computing then proposed the framework of cloud computing security risk and the way of cloud computing security testing. Finally, the implementation plans of two new security testing tools was proposed, which are Cloud computing penetration testing tools and data residue detection tool. Both solutions are successfully applied to the actual project.

Key words: cloud computing; security risk; security testing; cloud security penetration; data residual risk testing

1 引言

云计算在整合 IT 资源、提高资源利用率、有效地隔离各用户与分离物理资源的同时, 其安全性问题已经成为产业界和学术界关注的焦点。目前学术界对云计算的安全性测试技术研究还处于初步阶段, King 等研究人员^[1]为云用户提供测试支持服务 (Test Support - as - a - Service), 提出了一种面向云应用的增强测试方法, 但是该方法只针对云计算系统内部引发的安全问题进行测试, 而不适用于云计算系统外部风险引发的安全问题的测试。Rings 等研究人员^[2]针对云基础设施的互操作性提出了一种测试方法, 但是该方法没有考虑到任何云计算安全方面的问题。Tsai 等研究人员^[3]针对云计算系统中 workflow 服务的组件化实现所导致的测试性能低的问题, 提出了一种并行测试技术, 但并没有考虑云服

务的安全性测试。

本文通过对云计算安全问题的分析, 提出了云计算安全风险框架, 给出了云计算安全测试技术路线, 针对云计算安全风险, 设计了云计算渗透测试和数据残留风险检测解决方案。

2 云计算安全问题分析

2.1 安全问题概述

云计算安全风险主要体现在以下几个方面^[4]:

恶意服务注入: 恶意软件可以导致关键数据泄露、敏感数据改写、完整功能的变化和阻塞。

非法数据恢复: 当用户任务完成时, 虚拟机以及其磁盘空间会被释放, 然而物理媒介可能不会被彻底擦除, 因此数据非法恢复风险被进一步放大。

篡改数据备份: 恶意用户可能通过技术手段掌控着云计算系统内部的一些备份进程, 导致数据备

收稿日期: 2012-08-11; 修回日期: 2012-09-22

基金项目: 2011 年国家发改委、工信部和财政部联合发布的云计算示范工程“云计算公共技术服务平台”项目; 2011 年电子发展基金“云计算关键支撑软件(平台安全软件)研发与产业化”项目

份安全风险提升。备份过程可能产生大量攻击数据或无效数据。

安全一致性差:云计算系统在进行资源动态调整时,很难保证安全水平的一致性。

跨虚拟机袭击:云计算系统通常使用虚拟机技术来实现多租户访问,以提高硬件的利用率,有效降低成本。虚拟机运行在“沙盒”环境下,因此虚拟机之间可以做到隔离,然而系统漏洞的存在可能使恶意用户可以逃脱沙盒环境,完全地控制物理主机,从而可以完全管控其它虚拟机,产生安全隐患。

分布式服务拒绝(DDoS):由于云计算中物理机可以虚拟化为多个逻辑主机,在遭遇 DDoS 时,多虚拟机可以迅速耗尽物理机的资源,因此放大了 DDoS 威胁。

2.2 安全风险框架

云计算安全问题的解决涵盖两方面内容,一是云计算安全保障技术,二是云计算安全测试技术。其中安全保障方面已经有了一些有效的工作,对于云计算安全测试技术而言,主要是通过检测、定位、分析云计算安全技术问题,支撑云计算安全保障技术的发展以及研发能力的提升,目前该领域的研究还很欠缺。

针对云计算安全技术问题,本文系统地提出了一个云计算安全技术问题框架。云计算体系架构分为三个层次:资源层、系统层、应用层。其中,资源层主要是指底层软硬件计算、存储、传感器、服务器设备以及在此基础之上运用虚拟化技术构建的虚拟化资源,该层可以提供基本的分布式资源服务,包括:灵活、高效、高强度的计算服务,可靠、安全、大容量、便捷的分布式存储服务,可靠、安全的网络通信服务。系统层主要是指通过虚拟化资源构建的网络存储系统、网络计算系统、任务调度系统、以及其上运行的任务、业务和监控系统。应用层主要是指部署于云计算系统中的应用软件、服务访问接口以及对外提供的服务。综合云计算体系架构,结合云计算安全风险的分析,将安全要求的实现落实到各个服务层次上,提出了云计算安全风险框架,如图 1 所示。

3 云计算安全测试技术路线

按照传统的安全测试思想,安全测试通过运行安全测试用例来发现信息系统中的安全漏洞,是一种确保系统安全性的有效方法^[5]。经典的安全测试方法包括形式化验证、渗透测试^[6]、静态代码扫描、反汇编、错误注入、随机测试(fuzzing testing)、变异

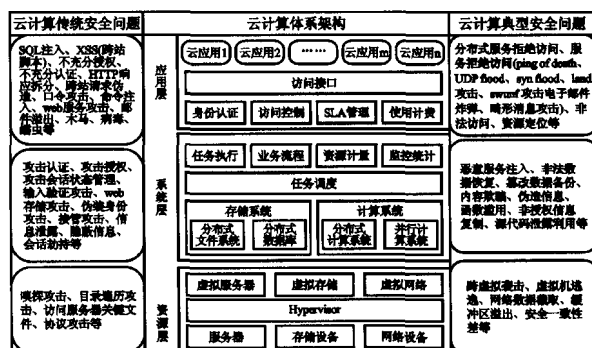


图1 云计算安全风险框架

分析等。

其中渗透测试则是当前使用的较多的验证型安全测试方法。尽管渗透测试存在测试用例实用性差、测试技巧依赖、缺乏测试标准等缺陷,但渗透测试仍然因其简单易行和在检验已知漏洞上的有效性成为了安全测试的一个重要组成部分。

通常安全性错误和漏洞的存在与安全保障措施无关,而是由于攻击者的异常行为而产生的,因此大部分信息系统的安全测试是负面因素的测试^[7],即模拟恶意攻击者的行为对系统发起攻击负面攻击以测试系统存在的安全问题。该测试方法更贴近于安全袭击的真实场景,因此测试结果更科学、合理。通过以上分析可知,渗透测试是面向系统负面因素进行的测试,即通过搜集、分析系统安全漏洞发起攻击,符合漏洞产生的条件,适用于面向风险的安全检测。因此相对于其他的测试方法,渗透测试较为适用于云计算的安全测试。同时,虚拟化机制是云计算最重要的特征之一,也使得安全风险剧增,有可能产生大量的安全漏洞。因此针对虚拟化安全问题,本文设计了云计算渗透测试方案,面向虚拟化的不同层次测试云计算的安全性。此外,就云计算数据存储安全而言,多租户在复用物理存储空间的同时,使得数据删除操作引入安全风险,如何测试数据删除的有效性变得十分重要。正面安全功能性测试^[7]较为适合测试这种具体的安全风险点。该方法可以简化测试流程、强化测试的针对性,即只针对系统安全功能的存在情况进行测试。因此,本文设计了数据残留风险检测方案,分析数据残留模式、恢复残留数据,检测云计算系统数据的非法恢复风险。

4 云计算安全测试解决方案

本文针对虚拟化风险、数据非法擦除风险,提出了两种云计算安全测试解决方案。云计算渗透测试以负面安全测试角度提出虚拟化安全检测的实现方

案,数据残留检测以正面功能性安全测试的角度解决如何判定系统存在非法数据恢复风险的问题。

4.1 云计算渗透测试

云计算渗透测试通过模拟一个未知恶意源发起的攻击,主动分析云网络安全强度,寻找由于系统错误配置,软硬件缺陷,或操作系统脆弱性等引起的潜在的漏洞,模拟现实世界黑客的攻击,找到绕过应用、系统和网络的安全措施的方法。通常该方法分为信息收集、网络扫描、漏洞识别、实施攻击几个阶段。一般地,渗透测试搜索漏洞的组合,以获得系统更多的权限。

云渗透测试分为两个部分:渗透测试管理系统和渗透测试执行单元,如图2所示。由管理系统控制分布在云计算中心各处的执行单元进行渗透测试。管理系统作为一个总控单元,可以控制若干渗透执行单元模拟黑客行为进行信息收集和渗透测试。

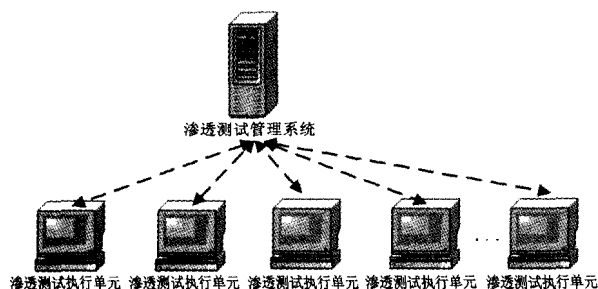


图2 云渗透测试体系架构

渗透测试管理系统的功能包括:接收用户或其他应用程序制定的渗透测试任务,根据任务进行相应的配置,监控执行工具的状态。渗透测试执行单元的功能包括:获取并解释测试脚本,接收管理者的命令调用相应的黑客工具进行攻击,返回攻击结果信息给管理工具。云渗透检测方案可供云服务提供商(CSP, Cloud Service Provider)使用,包括 IaaS、PaaS、SaaS 服务提供商。该方案可以实现云计算中心内部的定期渗透测试。

云渗透检测流程分为:准备阶段、测试部署阶段、信息收集阶段、场景建构阶段、攻击阶段、交付阶段。准备阶段确定测试的范围和时间期限等;部署阶段在云计算中心部署一个渗透测试管理工具和多个执行工具;发现阶段运行 Whois, Nslookup, Traceroute, VisualRoute, SmartWhois, SamSpade 等工具,收集目标信息,进行漏洞分析;场景构建根据分析结果,构造测试步骤,比如测试图,测试树,测试序列等;攻击阶段根据测试步骤进行攻击以验证漏洞是否存在;交付阶段根据场景构建阶段和攻击阶

段的信息进行分析,提供分析报告。云计算渗透测试流程如图3所示。

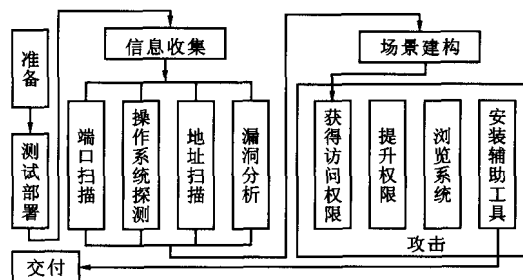


图3 云渗透测试流程图

云渗透测试主要针对以下几个层面进行渗透测试,一是 guest VM 的漏洞,但不感染 hypervisor 或 host 操作系统;二是感染虚拟化系统本身的漏洞,整个虚拟化环境都受影响,此类漏洞不是由 guest VM 引起的;三是由 guest VM 的漏洞引起的 hypervisor 漏洞,影响其他 VM 或者 hypervisor 本身;四是 Web 应用的漏洞,这类漏洞感染运行客户端浏览器的系统;五是 Web 服务器漏洞,影响 Web 应用。

4.2 数据残留风险检测

云计算应用模式下,数据集中在云计算系统中,用户对自身的数据只有使用权,而无物理上的控制权,无论使用何种云计算的服务模式(SaaS/PaaS/IaaS),用户数据的安全至关重要,云计算产业能否良性发展,很大程度上取决于用户数据的安全性否得到有效地保障。数据残留是数据在被擦除后所残留的物理表现,存储介质被擦除后可能留有一些物理特性使数据能够被重建,在云计算 IaaS 应用模式下,数据残留可能会无意泄露敏感信息,因此需要确保释放后的存储空间在分配给其他云用户前完全清除。

数据残留风险检测通过三个过程实现对残留数据的分析和检测,首先对数据文件系统进行分析,利用 raid 磁盘阵列或其它存储方式的特点,对分区表、MBR、DBR 等存储引导进行扫描和重构;然后再根据存储方式特点,选择相应数据恢复策略,对数据区文件数据进行重建,恢复残留数据;最后根据数据的恢复情况,分析可能存在的非法数据恢复隐患。根据以上三个过程,该方案包括四个部分,分别为存储模式分析、恢复方案管理、残留数据恢复和风险分析,如图4所示。

存储模式分析模块将根据被选择的云存储空间,获得相应磁盘内存储的各项基本信息,如:自

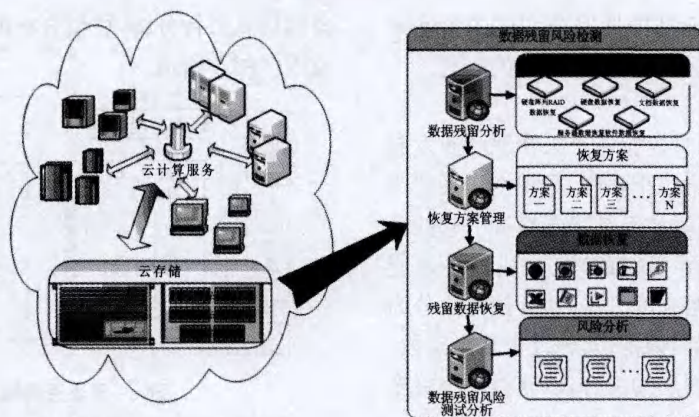


图4 数据残留检测模块

动进行 raid 磁盘阵列的磁盘次序、块大小和旋转方向等参数的分析,确定磁盘存储的数据结构中主引导记录、DOS 引导记录、文件分配表、硬盘分区表等数据完整程度。恢复方案模块负责保存和管理针对不同存储模式的数据恢复策略,并不断完善和更新。当根据上一模块完成存储模式和数据信息完整情况分析后,本模块可根据相应信息提供策略选择,自动分析生成残留数据部分原始文件位置、数据大小、类型等信息。数据恢复模块,根据选择的策略从云存储目标区域读取磁盘数据区数据,对文件进行重建还原,并对缺失部分数据进行估算,生成原文件,恢复残留数据。风险分析模块通过数据恢复模块恢复的残留数据情况,分析云存储可能存在的不同级别、不同层面非法数据恢复隐患。

5 结束语

本文对云计算安全风险进行了系统的分析,形成了安全问题框架,通过传统安全测试技术的分析,基于负面安全因素测试与正面安全功能性测试的理念,提出了云计算渗透测试、数据残留风险检测的设计方法及实现方案。两种测试技术方案在云计算示范工程“云计算公共技术服务平台”和电子发展基金“云计算关键支撑软件(平台安全软件)研发与产业化”项目中得到了验证,并成功应用于实际工程。随着项目的推进,相关研究工作将进一步拓展和深化。

参考文献:

- [1] Jay H, Mark N. Assessing the security risks of cloud computing[R]. Gartner, 2008;G00157782.
- [2] King T M, Ganti A S. Migrating autonomic Self-testing to the cloud [C]// Software Testing Verification

and Validation Workshop, IEEE International Conference on, 2010. France: Paris, 2010: 438 - 443.

- [3] Rings T, Grabowski J, Schulz S. On the standardization of a testing framework for application deployment on grid and cloud infrastructures [C]// The Second International Conference on Advances in System Testing and Validation Lifecycle. France, Nice, IEEE, 2010: 99 - 107.
- [4] Wei - Tek T, Peide Z, Balasooriya J, et al. An approach for service composition and testing for cloud computing [C]// Autonomous Decentralized Systems (ISADS), 2011 10th International Symposium on. Japan: Tokyo, 2011: 631 - 636.
- [5] Chris W, Lucas N, Dino D Z, et al. The art of software security testing: identifying software security flaws [M]. Symantec Press, Boston, MA; Addison - Wesley Professional, 2006.
- [6] Linde R P. Operating system penetration [C]// AFIPS National Computer Conference. USA: Anaheim, 1975: 361 - 368.
- [7] Zech P, Risk-based security testing in cloud computing environments [C]// software testing, verification and validation (ICST), 2011 IEEE fourth international conference on. Germany: Berlin, 2011: 411-414.

作者简介:



刘云龙 男,博士,工程师。研究方向为分布式计算、电子系统可靠性、信息安全、数字信号处理等。