doi:10.3969/j.issn.1001-893x.2014.05.021
引用格式:雷璟.安全桌面虚拟化信息系统设计与实现[J].电讯技术,2014,54(5):637-643.[LEI Jing. The Information System Design and Implementation Based on Security Desktop Virtualization Technology[J]. Telecommunication Engineering,2014,54(5):637-643.]

安全桌面虚拟化信息系统设计与实现*

雷 璟**

(中国电子科学研究院,北京 100041)

摘 要:通过对安全桌面虚拟化信息系统设计要求的分析,提出了"白名单"安全机制的安全虚拟化技术、优化设计的虚拟化层安全技术、资源和网络层隔离的虚拟机安全技术,在此基础上构建了安全桌面虚拟化信息系统的总体架构,给出了系统实现和典型应用场景。相关研究可为企业桌面云架构提供一个安全、易管理、低成本的解决方案,进而提高云计算安全核心技术水平,促进自主可控高安全云计算产品的研制。

关键词:信息系统;云计算;桌面虚拟化;白名单
中图分类号:TN918;TP393 **文献标志码**:A **文章编号**:1001-893X(2014)05-0637-07

Information System Design and Implementation Based on Security Desktop Virtualization Technology

LEI Jing

(China Academy of Electronics and Information Technology, Beijing 100041, China)

Abstract: Through analyzing the design requirement of security desktop virtualization information system, this paper presents safety virtualization technology of "white list" security mechanism, virtualization layer security technology of optimization design, and virtual machine security technology of resources and network layer isolation. On the basis, the overall architecture of security desktop virtualization information system is built, and also the system realization and typical application scenario are given. Research in this paper provides a safe, easy management, low cost solution of desktop cloud architecture for enterprise, improves the level of core technology on cloud computing security, and promotes the development of independent controllable high security cloud computing products.

Key words: information system; cloud computing; desktop virtualization; white list

1 引 言

"云计算"自从 2007 年被提出后,逐渐引起人们的关注和热捧,继个人计算机、互联网变革之后,作为第三次 IT 浪潮的代表正在向我们走来。云计算具有超大规模、虚拟化、高可靠性、通用性和资源复用率高等特点[1],它将带来人类生活、生产方式和商业模式的根本性改变,成为当前全社会关注的热点。

云计算是信息技术领域的重大进步。与传统软件架构相比,由于能够提供自助、动态可伸缩、可计量方式对共享资源实现按需访问,云计算在建设和运营成本、资源利用率、性能等方面具有显著优势。云计算将计算资源、存储资源、网络资源等各类资源集中起来可以带来资源整合统一管理、资源全局动态调度、应用请求智能分发和数据集中管理的使用价值。

* 收稿日期:2014-01-10;修回日期:2014-04-09 Received date:2014-01-10;Revised date:2014-04-09
** 通讯作者:leijanet@163.com **Corresponding author**: leijanet@163.com

桌面虚拟化是典型的云计算应用。随着企业的发展,企业对于桌面支持的需求大量增加,由各种管理问题带来的桌面安全隐患不断增多,这需要企业的 IT 部门投入巨大的精力加以解决[2]。另外,随着成本控制、可管理性、安全性以及业务连续性等方面压力的增加,传统 PC 桌面逐渐变得缺乏控制力,因此如何找到一种更好的桌面管理解决方案,搭建更高效的桌面基础架构,将桌面从传统的 PC 桌面模式中解脱出来,改善 IT 服务,降低 IT 基础设施的总体拥有成本,提高灵活性,成为当务之急。桌面虚拟化系统相对于传统桌面管理发生了非常重要的改变,它允许云终端通过瘦客户机或其他任何设备连接网络去访问跨平台应用和所有虚拟桌面[3]。

根据 2013 年云计算安全联盟(CSA)发布的云计算安全分析报告,报告中总结了 9 种威胁云计算安全的"罪魁祸首"。其中,数据泄漏、数据丢失和数据劫持三类威胁排名靠前,而桌面虚拟化同样也会面临这 9 种安全威胁。当前,国内外在云计算的相关领域方面还存在许多不足,尤其是在桌面虚拟化安全方面仅仅是某个单项产品解决某个特定问题,还没有形成一套包括用户的终端层面、边界层面、管理的运行环境层面的整体安全解决方案。

本文分析了安全桌面虚拟化信息系统的设计要求,对安全桌面虚拟化的主要技术进行了分析研究,提出了安全桌面虚拟化信息系统的实现和应用场景,为我国安全云计算平台建设中的终端安全提供技术支撑,最终为国家关键和重要信息系统提供具有自主可控和高安全特色的桌面云计算平台产品。

2 安全桌面虚拟化信息系统设计要求

2.1 先进性要求

安全桌面虚拟化信息系统的设计实现需满足以下先进性要求:

(1)支持大规模应用网络的组网,提供集中、高效、快捷的管理方式;

(2)服务器端基于"服务器虚拟化"技术设计实现,通过一台或多台物理服务器构建成一个虚拟化环境,在这个虚拟化环境中虚拟出多个虚拟系统,每个虚拟系统对外提供一种或多种服务,各个系统之间相互独立[4]。服务器端采用基于 KVM 等虚拟化技术以提供对服务器物理资源的最大化利用和基础安全机制,用虚拟机代替现行系统中的 PC 机作为系统中工作人员的实际操作对象;

(3)云终端基于"桌面虚拟化"技术设计实现,云终端必须支持通过远程桌面协议连接服务器端的虚拟主机,并以与传统 PC 机相同的操作方式操作虚拟主机完成正常的业务流程操作。

2.2 安全性要求

安全桌面虚拟化信息系统的设计能够从底层架构上提供以下基础安全机制:

(1)桌面虚拟化管理平台需要具有三权分立的管理员权限划分;

(2)云终端产生的数据必须集中保存在服务端,云终端不得保存任何本地文件;

(3)封闭敏感数据从云终端泄漏的途径,防止数据以任何方式从工作人员的云终端桌面泄漏出去;

(4)桌面虚拟化管理平台的软、硬件通过自主研发实现,避免系统在软、硬件上存在先天的安全漏洞和隐患。

2.3 运维保障要求

安全桌面虚拟化信息系统的设计需满足以下运维保障要求:

(1)按照"闭环"模式设计,对运行需要的各项基础资源能够循环使用,并具备一定的容错功能;

(2)针对常见的故障提供对应的"故障排除"功能并易于操作;

(3)桌面虚拟化管理平台需要提供日常运维的监控表;

(4)提供整套系统的备份与恢复方案,在系统遇到重大故障时启动备用系统应急。

2.4 可扩展性要求

在安全桌面虚拟化信息系统设计时需要考虑桌面虚拟化系统在计算资源、存储资源及网络带宽等层面的扩展性,同时保证信息系统业务的连续性。

3 安全桌面虚拟化技术

目前,国内在安全桌面虚拟化技术方面仅限于不同云计算厂商提供的产品,尚未形成统一的云计算产品和技术标准,用来促进不同厂商之间的互联互通性,也没有一个厂商能够解决桌面虚拟化技术面临的所有安全问题,其市场还处于发展的初级阶段。安全桌面虚拟化技术的发展基础为虚拟化安全主体,虚拟化安全主体主要涉及安全虚拟化、虚拟化层安全、虚拟机安全。因此,安全桌面虚拟化的核心技术主要包括安全虚拟化技术、虚拟化层安全技术

以及虚拟机安全技术,以下将重点说明这三项关键技术的解决思路和方法。

3.1　安全虚拟化技术

虚拟化技术可以使我们设计出更具弹性和扩展性、更加灵活、也更加安全的架构[5]。安全虚拟化技术以密码技术为基础,采用“白名单”安全机制防范各种已知和未知攻击。白名单主动防御技术是进行动态行为判断的一种技术,通过文件指纹的校验和比对的方法从根源上节制了恶意软件的运行和传播[6],以基于用户身份的数据复制和传送安全控制机制保证内部敏感数据的安全,即使是内部合法人员也不能非法复制和盗取各种业务敏感信息;系统集中安全管控机制大大减少了系统安全运维复杂度,克服了软硬件配置差异带来的系统兼容性问题,最终提高安全管控运维的效率。

此外,安全虚拟化技术支持对移动设备的多因子身份认证、安全加密通信,并且不在移动设备上保存任何与业务相关的数据,即使移动设备丢失,也不会导致失泄密事件的发生。

安全虚拟化技术可以实现非法人员“进不来”、“看不到”、“拿不走”、“跑不掉”,帮助系统管理人员能够对系统“管得住”、“管得少”、“管得好”,不会影响办公业务人员的正常办公。

3.2　虚拟化层安全技术

从虚拟化的实现原理来看,所有的虚拟化系统都是基于虚拟化层实现的[4],我们采用优化的虚拟化层来运行虚拟机,控制物理服务器所使用的硬件,并调度虚拟机之间的硬件资源分配。优化设计的虚拟化层可提供内存强化安全、内存模块完整性和无代理防病毒的保护。

(1)内存强化安全

将内核、用户模式应用程序及可执行组件位于无法预测的随机内存地址中,将该功能与 CPU 的数据内存保护特性结合使用,可提供保护,使恶意代码很难通过内存漏洞来攻击主机系统。

(2)内存模块完整性

通过动态完整性度量等方法来确保由虚拟化层加载的模块、驱动程序及应用程序的完整性和真实性。模块签名允许虚拟化层识别驱动程序或应用程序的提供商以及它是否在虚拟化架构的白名单中。

(3)无代理防病毒

从有代理模式发展到无代理模式,开拓了一种虚拟化环境安全模式的新思路,是一种技术进步[7]。实现虚拟化系统后,在一台物理主机上同时安装多个虚拟机,每一个虚拟机上都需要安装防病毒软件,这样对物理服务器的资源占用率会很大。可采用建立无代理防病毒模块的方式,统一通过底层 hypervisor 层进行工作,既达到减少物理主机负载,提高整机性能的目标,又实现对虚拟化层整体的安全防护。

3.3　虚拟机安全技术

虚拟机是运行应用程序和云终端操作系统的容器。虚拟机安全设计技术要实现资源层和网络层两个层面的隔离。

(1)资源层面隔离

要求所有虚拟机在资源层面互相隔离,多个虚拟机可以在共享硬件的同时安全地运行,既确保能够访问硬件,又保证运行不受干扰。如果某个虚拟机上的云终端操作系统运行时发生故障,则虚拟机隔离技术将确保同一台物理主机上的其他虚拟机可以继续运行。某台云终端操作系统发生故障不会影响用户访问其他虚拟机的能力、正常运行的虚拟机访问其所需资源的能力以及其他虚拟机的性能。

(2)网络层面隔离

在网络环境中,虚拟机隔离可以根据场景要求实现主机内隔离、完全隔离和受控隔离 3 种方式。其中,主机内隔离是指虚拟机不与其他虚拟机共享虚拟交换机,该虚拟机与主机中的虚拟网络完全隔离;完全隔离是指虚拟机未配置物理网络适配器,与网络完全隔离;受控隔离是指虚拟机采用与物理主机相同的保护措施,如虚拟云防火墙和虚拟云杀毒软件,该虚拟机属于受控隔离。

4　安全桌面虚拟化信息系统实现

安全桌面虚拟化信息系统的实现首先需要构建相互隔离的桌面虚拟机并均运行在数据中心,然后采用桌面显示协议将操作系统桌面视图高效地传送到用户端设备上,用户使用低功耗的云终端设备登录并使用属于自己的虚拟桌面。桌面虚拟化管理平台提供了丰富的管理功能,管理员可实时查看桌面虚拟化管理平台的运行状况,根据需求动态调整后台服务器资源的分配,还可以对用户虚拟桌面进行维护,查询和统计用户虚拟桌面的使用情况。

4.1　安全云计算平台总体架构设计

安全云计算平台总体架构设计的最底层为资源层,包括实际的计算设备、网络设备和存储设备;在

此基础之上,采用安全虚拟化技术将硬件资源进行抽象,通过安全虚拟机技术将硬件资源提供给 IaaS 层进行管理;IaaS 层作为资源调度的中间层,一方面通过对管理员的权限控制,达到对资源的安全统一使用,另一方面向更上层的 PaaS、SaaS 提供资源使用接口;PaaS 层在采用充分隔离以及一系列安全加固后,提供给用户 API 级的资源服务;安全虚拟桌面基础设施使用虚拟化层的资源;安全云管理平台实现对整个安全云系统统一、全方位的管理;以上几个部分共同形成安全云计算平台的总体架构。安全云计算平台的总体架构设计如图 1 所示。

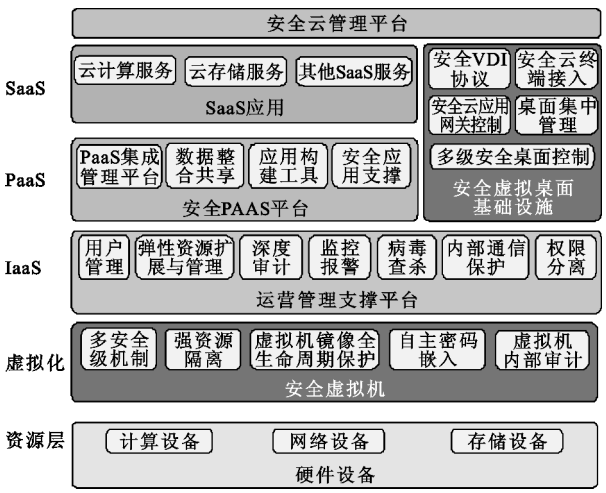


图 1 安全云计算平台总体架构设计图

Fig. 1 The overall framework design of security cloud computing platform

安全桌面虚拟化信息系统由安全云计算平台总体架构中的安全虚拟桌面基础设施和安全虚拟机构成。其中,安全虚拟桌面基础设施是指将桌面操作系统托管在一台运行在托管式的、集中化的或远程的服务器上的虚拟机内,用户可以在任何时候、任何地点采用任何设备对个人桌面进行访问[8]。

4.2 安全桌面虚拟化信息系统架构设计

数据中心是云计算中重要的、能够在数量和规模上快速扩展的基础设施的组成部分[9]。安全桌面虚拟化信息系统将传统模式下用户端的操作系统、应用程序和用户数据转移到数据中心进行运行和保存,用户利用各种云终端(含普通台式机、笔记本电脑、智能手机等),经安全虚拟桌面网关鉴权认证后通过安全桌面传输协议访问数据中心的应用服务器,本地终端不保留关键数据,实现用户桌面环境的集中存储、监控与管理。

安全桌面虚拟化信息系统的主要架构分为桌面虚拟化管理平台、安全虚拟桌面网关和云终端,如图 2 所示。

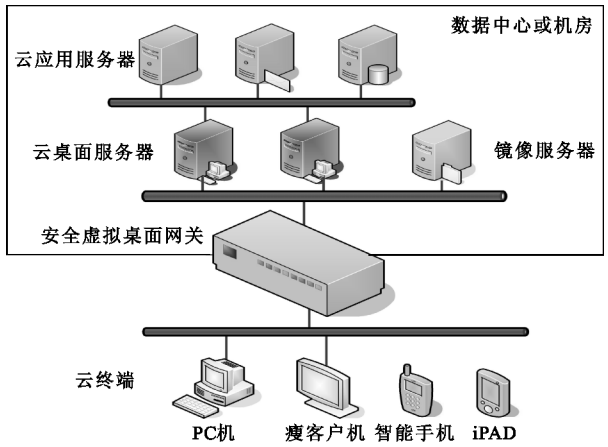


图 2 安全桌面虚拟系统架构图

Fig. 2 The system framework of security desktop virtual system

(1)桌面虚拟化管理平台:负责将计算资源和存储资源整合起来,统一分配资源,通过实时动态地管理虚拟机,分配给远程用户使用。同时,管理平台负责监控整个系统的运行状态、网络配置,并可以对资源进行动态调度。

(2)安全虚拟桌面网关:部署在虚拟的云桌面服务器和云终端(如用户 PC 机或瘦客户机)之间,负责系统的认证和权限管理、资源创建和分配管理、基于用户身份的信息流控制、镜像克隆管理、虚拟桌面白名单安全管理、各种终端的安全接入管理,为用户生产和办公信息系统提供有效和低成本的安全防护。

(3)云终端:负责连接和显示虚拟机的远程桌面,在硬件方面采用精简的计算机架构,硬件本身不需要很强的计算功能。

在安全桌面虚拟化系统中,数据安全主要通过以下方式进行防护:

(1)用户数据集中存放在统一存储设备中进行统一管理,云终端本地无硬盘,真正实现终端不留密;

(2)数据集中存放在统一存储设备中,虚拟机对数据盘的访问经过加密处理,防止管理员、非法用户非授权查看用户数据;

(3)用户在通过身份认证之后才可以访问数据盘,保证用户数据之间相互隔离;

(4)部署数据加密设备,对所有用户的数据进行加密存储;

(5)通过桌面虚拟化管理平台和主机监控与审计类产品对虚拟机的行为进行监控审计。

4.3　桌面虚拟化管理平台设计

使用安全桌面虚拟化技术构建的信息系统应以硬件虚拟化、安全隔离、集中管理和弹性资源调度等技术,将原本静态分布的 IT 基础设施抽象为可管理、易于调度、按需分配的资源,提供按需灵活使用各类 IT 资源服务。

使用安全桌面虚拟化技术的信息系统划分了多个集群,各个集群的资源池由桌面虚拟化管理平台统一管控。桌面虚拟化管理平台逻辑架构如图 3 所示。

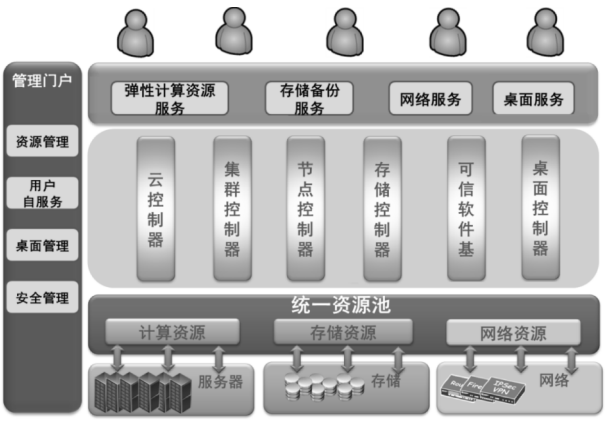


图 3　桌面虚拟化管理平台逻辑架构图

Fig. 3 The logic framework of desktop virtualization management platform

虚拟化管理平台可实现虚拟机管理功能,如创建、删除、重启等虚拟机操作,以及映像管理、监控告警等功能,从而实现轻量级的虚拟化管理[10]。桌面虚拟化管理平台还可以实现统一的计算资源管理、存储资源管理和网络资源管理。

(1)计算资源管理

计算资源指服务器上 CPU、内存等,使用桌面虚拟化理平台可以对整个信息系统进行资源整合统一管理、资源全局动态调度管理和资源弹性伸缩管理。

(2)存储资源管理

桌面虚拟化管理平台的存储资源池支持多种存储网络类型,实现存储资源的横向动态扩展,满足不同类型业务的应用需求。存储资源管理能够屏蔽不同品牌、不同类型设备物理资源的复杂性,实现逻辑资源与物理资源管理分离。

(3)网络资源管理

使用安全桌面虚拟化技术的信息系统网络设计涉及到计算中心网络设计,可以支持多种网络模式。

4.4　安全虚拟桌面网关实现

安全虚拟桌面网关是一个独立的硬件设备,结构部署在基于虚拟化技术的应用系统与外部环境之间,主要实现以下几种功能。

(1)基于密码技术的病毒木马防范

基于密码技术,借鉴可信计算中信任链传递的机制来对桌面虚拟化中的可执行代码进行保护。实现应用系统内部可执行程序的“白名单”安全保护机制,保证应用终端和应用服务器的运行完整性。可执行代码“白名单”是一个安全可执行代码的 Hash 值的清单,它是系统预先根据桌面虚拟化系统中的任务要求制定和生成的,它为每个虚拟机都保存一份列表,该列表涵盖了该桌面虚拟化系统中所有被允许执行的代码文件。这种“白名单”安全保护机制能够对已知和未知的恶意代码进行有效防范。“白名单”安全机制克服了传统防病毒系统的防毒效果差、防毒性能低的问题。

(2)安全边界保护和数据流安全控制

安全虚拟桌面网关作为应用系统与外部环境之间的安全边界,依据相关网络协议对进出应用系统的信息流进行分析,依据管理员制定的规则和策略进行安全控制。在桌面虚拟化环境中,所有的应用数据均存储在“云”端,管理人员可以对应用系统与外部环境之间的通信进行安全隔离,并基于用户身份对其在应用系统内外环境之间的数据交换或信息流进行单向和双向控制,在保证应用系统安全性的同时降低系统安全建设成本,提高系统可靠性和运行性能。

(3)集中安全管理

安全虚拟桌面网关通过网络存储安全镜像克隆管理机制,实现对系统镜像的集中安全管理,支持软件快速部署和补丁升级,克服传统基于网络发布方式的系统升级维护带来的系统兼容性问题,并大幅度降低系统运维工作量,提高系统安全运维的效率和效果。

(4)安全通信和认证机制

安全虚拟桌面网关支持安全通信和基于数字证书的多因子认证技术,并支持各种移动设备的安全接入。用户可以在任何时候、任何地点均可以通过传统 PC 机、安全瘦客户机、iPAD 或 Android 平板电脑、智能手机等移动手持终端等设备安全地访问内网应用系统,并且不会导致应用系统数据外泄等安全问题。

4.5　系统典型应用场景

某单位信息系统内网对未知的病毒、木马难以有效防范;对内部人员的数据非法复制和盗取行为难以控制,数据安全得不到保证;系统运维人员除了

需要管理和维护各应用服务器外,还需要对用户终端进行安全维护和管理,工作量巨大,安全管理效果不尽人意。

对该单位安全桌面虚拟化解决方案的核心思想是以安全桌面虚拟化技术为基础,通过虚拟桌面信息流安全控制机制和基于密码技术的虚拟桌面的可执行代码保护机制,防范各种已知和未知的病毒木马,保护内部数据安全,其具体实现方式如图 4 所示。

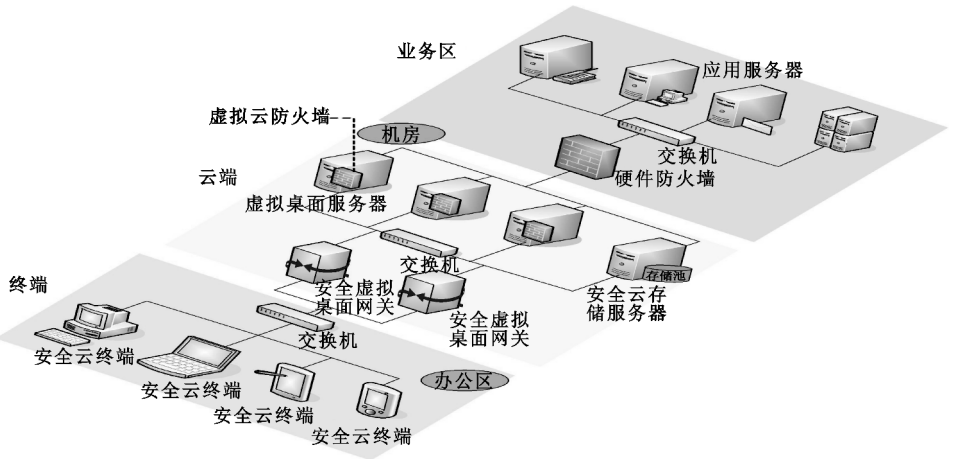


图 4 虚拟桌面安全防护结构示意图

Fig. 4 The sketch map of virtual desktop security protection structure

图 4 中,在机房中的业务区部署了 4 台应用服务器,云端部署了 3 台虚拟桌面服务器,每台虚拟桌面服务器上支持运行几十个虚拟桌面,每个虚拟桌面之间通过虚拟云防火墙进行安全隔离,办公人员通过安全云终端连接到虚拟桌面,进而访问相应的后台应用。安全桌面虚拟化信息系统的好处是它可以将用户操作终端与应用终端在物理上加以分离,实际的办公等应用软件和应用数据都在虚拟桌面上运行和处理,操作终端只是起到虚拟桌面的显示器和键盘鼠标输入作用,从而为数据安全提供了保护基础。

同时,为了加强对用户业务操作的集中管理,控制用户在虚拟桌面和操作终端之间的数据交换和文件复制行为,在虚拟桌面服务器和用户办公区的操作终端之间部署安全虚拟桌面网关。此外,为了提高系统安全机制的可靠性,根据需要部署 2 台安全虚拟桌面网关,实现双机安全热备功能。

针对安全桌面虚拟化系统实现方案,可以参考国际通用的云计算产品安全测试方法以及云计算安全性测试技术、基于桌面虚拟化平台的系统级安全评估技术来对检测及评估桌面虚拟化平台的设计和实现是否符合国家对云计算产品标准中相关安全性的要求。

4.6 设计特色总结

基于安全桌面虚拟化技术的信息系统在设计与实现过程中采取分层防护的思路,通过桌面虚拟化管理平台实现了从终端层、边界层、运行环境层在内的安全设计与实现,具体如下:

(1)终端层安全:利用安全虚拟化技术实现终端的多因子身份认证、安全加密通信,并且不在终端上保存任何与业务相关的数据,实现终端不留密,防止失泄密事件的发生;

(2)边界层安全:通过虚拟机安全技术并结合身份认证系统、虚拟化边界防护、虚拟化网络的逻辑隔离机制共同防护,来保证云终端接入运行环境的安全;

(3)运行环境层安全:通过虚拟化层安全技术对虚拟机的镜像及内存模块完整性进行保护,避免虚拟机操作系统以及内部的数据遭到篡改和非法访问。

5 结束语

随着政府机构、企业、各行业等单位对信息技术应用的不断深入,信息系统已成为办公、科研和处理日常业务的主要手段,在网络空间安全日趋激烈复杂的今天,安全保密工作的任务也越来越艰巨。相对于传统技术,桌面虚拟化技术具备高效、灵活、集中管控等一系列先天优势,因此越来越多的单位对建设基于安全桌面虚拟化技术的信息系统有迫切需求。

本文针对安全桌面虚拟化信息系统设计要求,通过对安全虚拟化技术、虚拟化层安全技术和虚拟

机安全技术的研究,提出了安全桌面虚拟化信息系统设计和实现方案,已经应用于某些政府、企业内网的桌面虚拟化试点建设工作,探索今后云计算环境下的安全保密风险及应对措施。未来目标用户包括国家党政机关、各行业企事业单位、军队等对下一代安全云计算环境有需求和对安全要求较高的用户。安全桌面虚拟化信息系统可以无缝部署在用户既有的应用环境中,不要求用户改变应用程序和操作习惯,满足各种用户应用需求。安全桌面虚拟化信息系统的解决方案能够显著提高系统安全水平,加强系统的集中安全管控能力,减少系统建设和运维成本,简化系统安全结构,减少安全产品数量,保证系统性能和运行可靠性。下一步的工作重点是加快安全桌面虚拟化的安全保密技术攻关和产品研发,有力支撑自主高安全云计算平台的研究与开发,进而提高云计算安全核心技术水平,促进自主可控云计算安全产品的研制。云计算作为网络空间发展中的新兴网络技术,它的安全将支撑网络空间技术验证和自主安全研发,最终将保障国家的网络空间安全,保卫国家的核心利益[11]。

参考文献:

[1] 张建. 云计算发展与虚拟化面临的安全挑战[J]. 信息安全与技术,2013(5):7-9.
ZHANG Jian. Safety Challenge of Cloud Computing's Development and Virtualization[J]. Information Security and Technology,2013(5):7-9. (in Chinese)

[2] 朱玉珩,李微巍. 企业桌面云计算应用浅析[J]. 中国管理信息化,2012,15(15):75-76.
ZHU Yu-heng, LI Wei-wei. Enterprise Desktop Cloud Computing Application Superficial Analysis[J]. China Management Informationization, 2012, 15(15): 75-76. (in Chinese)

[3] Zhou Yi-min, Guo Hui-hui. A Research of USB Device Redirection Mechanism over IP network in Desktop Cloud System[C]//Proceedings of 2012 National Conference on Information Technology and Computer Science. Lanzhou: IEEE,2012:197-200.

[4] 刁宇亮. 虚拟化安全建设研究[J]. 计算机安全,2012(1):65-68.
DIAO Yu-liang. Virtualization Security Construction Research[J]. Computer Security, 2012(1): 65-68. (in Chinese)

[5] 杜金秀,庄主,邹铭. 云计算平台中的虚拟化技术与安全机制[J]. 信息安全与技术,2013(3):41-43.
DU Jin-xiu, ZHUANG Zhu, ZOU Ming. Virtualization and Security Mechanisms in Cloud Computing[J]. Information Security and Technology,2013(3):41-43. (in Chinese)

[6] 汪锋,周大水. 白名单主动防御系统的设计与实现[J]. 计算机工程与设计,2011,32(7):2241-2244.
WANG Feng, ZHOU Da-shui. Design and implementation of active defense system based on white list[J]. Computer Engineering and Design, 2011, 32(7): 2241-2244. (in Chinese)

[7] 于锋. 无代理安全防护模式——虚拟化安全的必然趋势[J]. 信息安全与技术,2012(12):58-61.
YU Feng. Through Higher Vocational Professional Skills Competitions to Analyze the Advantages of Enterprises High-quality Teaching Resources[J]. Information Security and Technology,2012(12):58-61. (in Chinese)

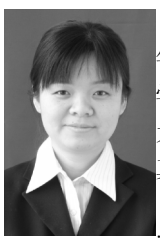
[8] 孙宇,陈煜欣. 桌面虚拟化及其安全技术研究[J]. 信息安全与通信保密,2012(6):87-92.
SUN Yu, CHEN Yu-xin. Research on Desktop Virtualization and Its Security[J]. Information Security and Communications Privacy,2012(6):87-92. (in Chinese)

[9] Tian Yuan, Lin Chuang, Chen Zhen, et al. Performance Evaluation and Dynamic Optimization of Speed Scaling on Web Servers in Cloud Computing[J]. Tsinghua Science and Technology,2013,18(3):298-307.

[10] 茅秋吟,张春芳. 轻量级 POWER 虚拟化管理平台 PowerDirector[J]. 微型机与应用,2013,32(6):11-14.
MAO Qiu-yin, ZHANG Chun-fang. Lightweight POWER virtualization management platform PowerDirector[J]. Microcomputer & Its Applications,2013,32(6):11-14. (in Chinese)

[11] 雷璟. 网络空间攻防对抗技术及其系统实现方案[J]. 电讯技术,2013,53(11):1494-1499.
LEI Jing. Cyberspace Attack and Defense confrontation Technology and System Realization Scheme[J]. Telecommunication Engineering,2013,53(11):1494-1499. (in Chinese)

作者简介:



雷　璟(1977—),女,湖北武汉人,2003 年于华中科技大学获计算机应用技术专业工学硕士学位,现为高级工程师,主要研究方向为信息安全、信息网络安全建设、网络安全仿真评估。

LEI Jing was born in Wuhan, Hubei Province, in 1977. She received the M. S. degree form Huazhong University of Science and Technology in 2003. She is now a senior engineer. Her research interests include information security, information network security construction, network security simulation and evaluation.

Email: leijanet@163.com