第 38 卷 第 3 期
Vol.38 No.3

计 算 机 工 程
Computer Engineering

2012 年 2 月
February 2012

• 工程应用技术与实现 • 文章编号：1000—3428(2012)03—0234—03 文献标识码：A 中图分类号：TP311.5

基于 Xen 的域间切换方法研究

施佳铁[1]，徐 宁[2]，刘文清[2]，杜丽霞[1]

(1. 兰州交通大学电子与信息工程学院，兰州 730070；2. 中标软件有限公司，上海 200030)

摘 要：为解决开源虚拟化系统的桌面切换问题，提出一种基于 Xen 的域间切换方法。利用 Xen 虚拟化支持 Intel VT-x 的硬件，使用 RFB 协议根据配置文件连接到 VNC Server 端，以显示虚拟机桌面，通过加密切换指令验证信息，从而完成域间切换。实验结果表明，该方法能实现 Windows 域和 Linux 域的桌面切换。

关键词：虚拟化；域间切换；信息验证；多域

Research on Xen-based Intra-domain Handoff Method

SHI Jia-tie[1], XU Ning[2], LIU Wen-qing[2], DU Li-xia[1]

(1. School of Electronic and Information Engineering, Lanzhou Jiaotong University, Lanzhou 730070, China;
2. China Standard Software Co., Ltd., Shanghai 200030, China)

【Abstract】Aiming at the desktop application of open-source virtualization system, a intra-domain handoff method Xen-based is proposed. It uses Xen to virtually support the hardware of Intel VT-x. It uses Remote Frame Buffer(RFB) protocol. According to the configuration file, it links to the VNC Server end, hence show the virtualization desktop. It makes use of encrypt instruction to complete the information authentication, and intra-domain handoff. Experimental results show that the method can implement the desktop handoff between Windows domain and Linux domain.

【Key words】virtualization; intra-domain handoff; information authentication; multi-domain

DOI: 10.3969/j.issn.1000-3428.2012.03.077

1 概述

对虚拟化技术的研究已有几十年历史，虚拟概念最早由 IBM 公司在六七十年代提出，将其用于 VM/370 系统中，以共享昂贵的大型机系统[1]。虚拟化可分为应用级和系统级，本文的虚拟化是指系统虚拟机[2]。近年来，随着多核技术的出现，计算机系统处理能力大幅度提升，其规模不断扩大，特别是云计算的提出，使得虚拟机化技术获得良好的发展基础，在这些因素的促进下，虚拟化技术又一次得到学术界和工业界的重视[3]。

Xen[4]作为一款基于 GPL 授权方式的开源虚拟机软件，起源于剑桥大学的一个研究项目，在设计之初，为追求高性能，采用泛虚拟化(Para-virtualization)技术。在 Intel 向外界发布硬件虚拟[5]之后，Xen 实现支持硬件虚拟化。

在 Xen 系统中，Xen 本身是底层管理系统，存在一个轻量级的软件层，即向运行在它之上的虚拟机提供虚拟硬件资源，同时，分配和管理这些资源，并保证虚拟机之间的相互隔离。随着硬件能力提升，以及将 Xen 的硬件虚拟化技术运用于多核 CPU，可有效改善虚拟机系统的运行效率和性能问题，且为双系统甚至多系统并行运行提供有力保障。但现有的虚拟化系统缺乏一种安全有效且反应迅速的桌面系统切换机制，使虚拟机系统的应用受到制约。为此，本文提出一种基于 Xen 的域间切换方法。

2 多域安全设计

针对上述不同系统不能实现桌面切换的缺点，本文提供一种安全有效、反应迅速且应用简便的虚拟机桌面系统切换方法。

在 Xen 系统中，假如每一个虚拟机称为一个域，那么多域指同时运行多个虚拟机。在本文方法中，域之间切换是安全有效的。

本文方法由 3 个部分子系统组成，即特权管理系统、通用桌面系统和安全 Linux 桌面系统。其中，特权管理系统为虚机系统的特权域系统，负责对后 2 个子系统进行资源分配和管理；通用系统和安全系统为主要使用的 2 个子系统；虚拟机系统默认引导是进入通用系统(如 Windows 系统)，当进入系统后，可保证能正常进行日常事务处理，如需处理一些涉及私密敏感信息时(如登录网上银行办理业务、安全办公存储等)，可通过切换方式直接转入安全系统进行操作。硬件需要 CPU 的虚拟化技术作为支持，并且在切换时需要对指令进行验证。

2.1 虚拟机显示

虚拟机显示通过 VNC(Virtual Network Computing)[6]实现，VNC 使用 RFB(Remote Frame Buffer)协议根据配置文件连接 VNC Server 端，然后显示虚拟机桌面。配置文件主要用来配置显示的一些选项，包括显示分辨率、显示地址、显示端口号。由于 VNC 协议在局域网内的显示效果是较满意的，更何况是在同一台电脑上，因此该显示不会造成明显的性能损耗，在虚拟机切换过程中也反应迅速。

基金项目：国家自然科学基金资助项目(61072047)；“核高基”重大专项(2010ZX01036-001-001)

作者简介：施佳铁(1986－)，男，硕士，主研方向：信息安全，虚拟机技术；徐 宁、刘文清，博士；杜丽霞，教授

收稿日期：2011-09-01 **E-mail：**shijiatie@163.com

2.2　信息的验证

需对切换指令进行加解密，以确定指令未被窜改，对切换指令进行加解密的过程如图 1 所示。其中，透明箭头是域内信息传递，填充箭头表示跨域信息传递。

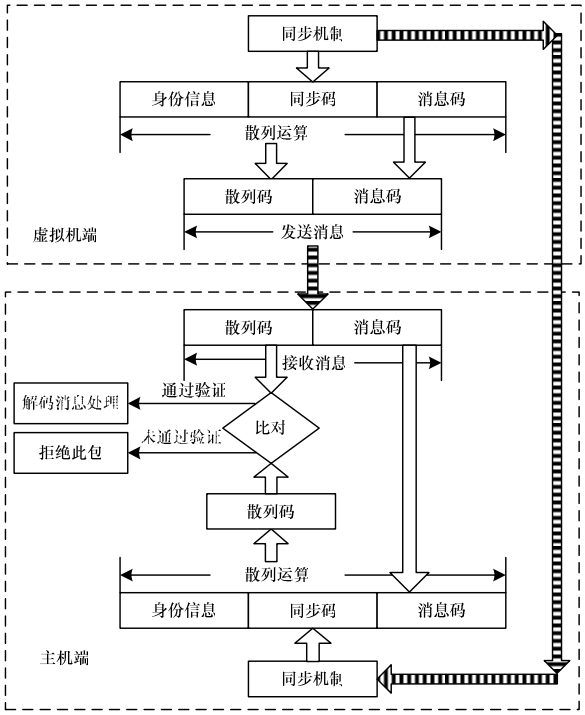

图 1　切换指令进行加解密过程

由图 1 可知，在该虚拟机桌面系统切换方法中，底层管理系统与桌面系统均具有相同的同步码，该同步码是单向离散函数验证码；桌面切换指令为经过同步码加密的消息包，该加密信息是将身份信息、同步码和指令码，在通过 Hash 计算后获得；底层管理系统接收相应的桌面切换指令，该指令来源可以是输入设备功能库获得的硬件触发信号，也可以是指定图标快捷方式。由于指令来源的不同，因此在实现方面也就表现为 2 种方式，即下文提到的硬切换和软切换；底层管理系统对接收的桌面切换指令进行验证，只有当验证通过时才允许切换。

2.3　域间切换

域间切换是从一个虚拟机切换到另一个虚拟机，除需要上述对切换指令进行加解密，以确保指令不被篡改以外，在切换指令顺利传达下来后，在虚拟机桌面系统切换方法中，桌面切换还包括 2 个步骤：(1)Xen 系统通过守护进程通知窗口管理器；(2)窗口管理器通过 VNC 协议切换显示桌面窗口。

在域间切换中，由于切换指令的来源不同，因此需要不同的实现方式，当切换指令来源于硬件触发信号时，则表现为硬中断切换；当切换指令来源于指定图标的快捷方式时，表现的切换为软件中断。

2.4　设计小结

虚拟机底层管理系统在接收到相应的桌面切换指令后，需要对指令进行验证。在验证成功后，才会执行所接收到的桌面切换指令。若验证不成功，则拒绝执行指令。上述过程使得该虚拟机桌面系统切换方法，能够通过该验证过程实现安全可靠的桌面系统切换。

该切换过程反应迅速，对虚拟机系统没有明显损耗，为用户提供更为良好的使用体验。同时，在切换的操作上设计 2 种不同的方式，即硬件触发或者指定图标的快捷方式，更符合现代操作习惯。

3　关键技术实现

本文方法的关键技术包括虚拟机显示、信息验证、域间切换，其中，域间切换包括硬件触发的“硬切换”和指定图标快捷方式的“软切换”。

实现部分如下：在裸机安装 Linux，然后构建 Xen 虚拟化环境，利用 Xen 对 Intel VT-x 技术的硬件实现虚拟化支持，并安装 Windows XP 虚拟机和 Linux 虚拟机，最后利用 VNC 显示 VM Windows 和 VM Linux。通过键盘上热键触发硬切换；利用指定图标实现软切换，该切换是安全有效、反应迅速的。

实现过程分为 3 个部分，即 Host 主机的守护进程，以及 VM Windows 上的 VM Windows Tools 和 VM Linux 上的 VM Linux Tools。其中，VM Windows 表示安装的 Windows XP 虚拟机；VM Linux 表示安装的 Linux 虚拟机；VM Windows Tools 表示 VM Windows 内的工具，其一直运行在该虚拟机内；VM Linux Tools 表示 VM Linux 内的工具，也是一直运行在该虚拟机内。

3.1　虚拟机显示

虚拟机显示由 VNC 协议负责。通过一段伪代码说明虚拟机显示(创建 VNC Server 的连接，创建和启动显示线程，以完成 VNC 显示的初始化过程)，具体如下：

```
url.setHost(VNC_Host);//设置主机地址
url.setPort(VNC_Port);//设置端口号
vncViewThread=new VNCViewThread(url)//创建连接
vncViewThread->Start();//启动显示线程
connect(SIGNAL(connected()));//绑定连接完成信号
connect(SIGNAL(changeSize()));//绑定改变大小信号
connect(SIGNAL(reinit_me()));//绑定重新连接信号
fullscreenEnabled=true;//全屏模式
view->setGrabAllKeys(true);//获取所有键盘事件
view->setFocus();//获取鼠标事件
```

3.2　信息验证

虚拟机的底层管理系统在接收相应的桌面切换指令后，对指令进行验证，在验证成功后，执行所接收到的桌面切换指令，若验证不成功，则拒绝执行指令。该指令是同步码加解密的消息包，加密过程的代码如下：

```
QString headsync(sync);//获取同步码
QString sendrawcmd=headsync+rawCmd;//获取要加密的命令
QString md5cmd=getMd5(sendrawcmd);//对命令进行 Md5 加密
QString sendCmd=”DomU/Host*”+md5cmd+”*”+sendrawcmd;
```

解密的过程与加密过程类似，是对接收到的命令进行截取，并与 MD5 码进行比对。

3.3　切换方式介绍

Host 主机的守护进程主要完成消息监听，以及在收到消息后对消息进行处理。VM Windows 上的 VM Windows Tools 与 VM Linux 上的 VM Linux Tools 主要完成将用户的操作信号通过虚拟设置驱动程序所控制的虚拟设备传递给 Host 主机上的守护进程。

切换可以是硬件触发信号，也可以是指定图标快捷方式，分别表示为硬切换和软切换，这 2 种切换方式分别利用的是“硬中断”和“软中断”。

3.3.1　硬中断

硬件中断是通过直接按键盘快捷键触发热键的方式实现桌面切换，如图 2 所示。

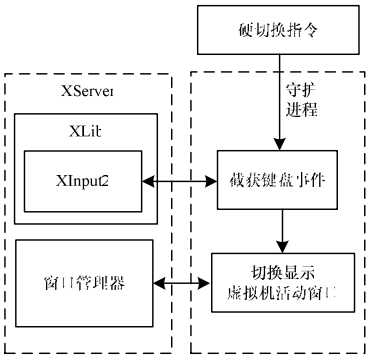

图 2 硬中断

由图 2 可知，在 Xen 系统上，所有键盘信号是被 Xen 截获的，但对于 I/O 设备的数据处理是由 Dom0 上的 Host 系统负责，因此，对于图形应用程序，I/O 设备数据均由 XServer 负责向上层应用程序分发，即 XServer 会首先收到键盘事件。XLib 和 XInput2 均为第三方库，供 XClient 端调用。具体实现方法为利用 XLib 的扩展功能 XInput2 功能库实现提取键盘事件。当提取到指定热键的键盘事件后，守护进程通知窗口管理器，切换通过 VNC 协议显示的另一桌面窗口，即达到桌面切换的目的。

3.3.2 软中断

软切换即让系统即时响应切换的请求事件，并向 Dom0 上 Host 系统发送切换桌面信号。VM Windows 在 Windows 操作系统看来所有的硬件都是真实的，而实际上硬件是 Xen 为 VM Windows 虚拟的设备。有 2 种方式向外界发送信号，即通过网络或者通过虚拟硬件。前者由于依托网络，因此，而存在巨大风险性。后者由于是软件虚拟的硬件，因此提供实现的可行性。为降低 Windows 软中断的开发难度，利用 Windows 操作系统可对虚拟硬件实现自识别与自驱动，在 Windows 上开发的切换程序通过 Windows WDM 直接调用内核驱动，再通过内核驱动向虚拟硬件发送消息，即可以实现 VM Windows 向 host 发送切换消息的目的。

软中断是通过点击图标方式实现桌面切换的方式，具体如图 3 所示。

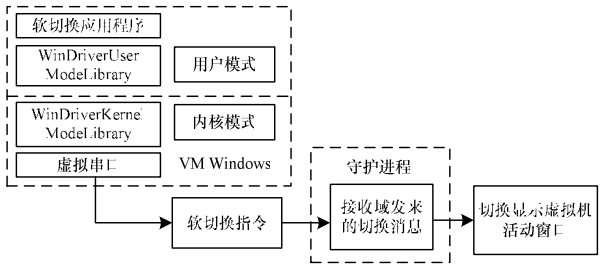

图 3 软中断

由图 3 可知，软切换程序主要由 VM Windows 上的切换程序和 Dom0 中运行的切换守护进程组成。VM Windows 上的切换程序通过 Windows 驱动编程 WDM 实现应用层调用 Windows 系统内核以达到直接驱动虚拟串口向外发送切换消息的目的。

4 相关工作

Xen 的诞生就是针对服务市场，故传统观点认为 Xen 能成功在服务器环境中实现虚拟化，但利用 Xen 的虚拟化同样可以很好解决终端桌面用户的安全问题，例如 Citrix 公司的 XenClient[7]、Virtual Computer 公司的 NxTop[8]、ITL[9]认为之所以现在的操作系统不安全是由于其不能很好地隔离，但是 Xen 虚拟机可以做到这点。XenClient 需要 Intel vPro 平台、C/S 模式，并且有一个 Server 端作为数据管理中心管理、备份和自助恢复的虚拟机。NxTop 是一个 C/S 模式的虚拟化解决方案，虽然不要求 Intel vPro 平台，但并非是个人用户的最好选择。

得益于 Xen 社区的努力，近期发布的 Linux kernel 3.1 完全支持 Xen 的 Dom0 和 DomU[10]，这再一次巩固了 Xen 在 Linux 世界的地位，并且方便 Xen 的安装和二次开发。

软件巨头 Oracle 在 2011 年 8 月推出基于 Xen 的虚拟机 VM 3[11]，这更奠定 Xen 在开源虚拟化中的地位。

5 结束语

本文提出基于 Xen 的域间切换方法。设计基于 Xen 的多域安全隔离方式，即在该设计方案中显示多个虚拟机，在多个虚拟机之间实现高效安全的自由切换，关键技术包括虚拟机显示、加解密信息、2 个虚拟机间的切换。实验结果表明，该设计能够安全有效、反应迅速地实现 Windows 域和 Linux 域的桌面切换，对虚拟化研究有参考意义。

参考文献

[1] Creasy R J. The Origin of the VM/370 Time-sharing System[J]. IBM Journal of Research and Development, 1981, 25(5): 483-490.

[2] James E, Smith R N. Virtual Machines: Versatile Platforms for System and Processes[M]. 安 虹, 张 昱, 吴俊敏, 译. 北京: 机械工业出版社, 2009.

[3] Goldberg R P. Survey of Virtual Machine Research[EB/OL]. (2010-11-20). http://elainetron.com/osprelim/summaries/survey_of_virtual_machine_research.html.

[4] Barham P, Dragovic B, Fraser K, et al. Xen and the Art of Virtualization[C]//Proc. of ACM Symposium on Operating Systems Principles. New York, USA: ACM Press, 2003.

[5] Intel Corporation. Intel Itanium Architecture Software Developer's Manual[EB/OL]. (2010-11-21). ftp://download.intel.com/design/Itanium/manuals/24531805.pdf.

[6] Richardson T, Quwntin J, Stafford F, et al. Virtual Network Computing[J]. IEEE Internet Computing, 1998, 2(1): 33-38.

[7] Citrix. A New Way of Computing from Citrix[EB/OL]. (2010-07-21). http://www.citrix.com.

[8] Virtual Computer. NxTop Intelligent Desktop Virtualization[EB/OL]. (2010-10-21). http://www.virtualcomputer.com/nxtop.

[9] Invisible Things Lab. Advanced Security Technologies[EB/OL]. (2010-12-21). http://invisiblethingslab.com/itl/Welcome.html.

[10] Xen Organizations Community Blog. Xen Celebrates Full Dom0 and DomU Support in Linux 3.0[EB/OL]. (2010-06-02). http://blog.xen.org/index.php/2011/06/02/xen-celebrates-full-dom0-and-domu support-in-linux-3-0.

[11] Oracle Corporation. Oracle VM 3: Architecture and Technical Overview[EB/OL]. (2010-08-21). http://destinationebooks.com/oracle-vm3-architecture-and-technical-overview.html.

编辑 刘 冰