面向虚拟桌面内外部数据流的安全控制机制研究

邓霄霄[1] 路 川[1] 马 威[2]

(中国人民解放军装备学院 北京 101416)[1] (北京交通大学计算机与信息技术学院 北京 100044)[2]

摘 要 桌面虚拟化需要借助虚拟桌面协议来实现内部应用数据和外部操作平台的数据交互。然而该类协议中的数据流控制机制并不完善,存在数据非法交互的安全隐患。为解决该问题,基于网关模式提出了一种面向虚拟桌面内外部数据流的安全控制机制SCIED。它不仅能对协议中的虚拟通道进行全面管控,避免修改协议和大量的终端,还具有较高的兼容性、拓展性。将它部署于网关并用于防护边界攻击,能显著减少服务器端的负载和安全隐患。实验表明,该SCIED能够有效保证数据流的安全交互,并且对现有桌面会话的性能影响较小。

关键词 桌面虚拟化,虚拟桌面协议,安全控制机制,内外部数据流

中图法分类号 TP393.1 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.4.025

Secure Control Mechanism of Internal and External Data-flow Oriented to Virtual-desktop

DENG Xiao-xiao[1] LU Chuan[1] MA Wei[2]

(Academy of Equipment, Beijing 101416, China)[1]

(School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China)[2]

Abstract The data interaction of desktop virtualization between internal application data and external user operation platform are realized by virtual desktop protocol. Because of the deficiency of the data flow control mechanism in this kind of protocol, it may lead to the illegal interaction. In order to resolve this problem, based on gateway, this paper proposed a secure control mechanism of internal and external data-flow oriented to virtual-desktop. It not only has the overall control of virtual channel, avoiding modifying lots of transport protocols or terminals, but also has high compatibilities, expansibilities and usability. Deploying it at the gateway to protect from boundaries attack can reduce the server load and safety concerns significantly. Experiments prove that this mechanism can control the direction of data flow effectively. Meanwhile, it has little impact on existing desktop session.

Keywords Desktop virtualization, Virtual desktop protocol, Secure control mechanism, Internal and external dataflow

随着虚拟化技术的飞速发展,桌面虚拟化凭借其诸多优势,被广泛应用于云计算中。它不仅能实现虚拟桌面和应用数据的集中管控,还把数据安全问题转化为虚拟桌面与用户终端之间的数据交互问题[1,2]。虚拟桌面协议即实现虚拟桌面和用户终端之间数据交互的主要途径。对于不同的数据类型,协议需要为其建立特定的虚拟通道来传递数据,例如磁盘重定向通道、USB重定向通道。然而其在实际应用中却存在以下问题:1)虚拟桌面协议缺少单向控制机制,使远程虚拟机和本地物理机之间可以双向任意传输数据,存在一定泄密隐患;2)底层隔离机制对用户透明,其中的第三方通道不易被发现,存在恶意人员或程序利用隐蔽通道进行窃密的安全隐患。

因此,本文根据虚拟桌面底层架构的特点,采用软硬件相结合的方法,提出了一种基于网关模式的数据流控制方案——面向虚拟桌面内外部数据流的安全控制机制(A Secure Control mechanism of Internal and External Data-flow oriented to virtual-desktop, SCIED)。该机制能妥善解决虚拟桌面环境中内外部数据流的非法交互问题,实现虚拟通道的全面可控,有效提高系统中数据的安全性。

1 研究背景

对于虚拟桌面的数据流安全控制问题,国内外学者已有一些研究。目前主要有3种控制方式:1)在客户端控制;2)在服务器端控制;3)在客户端和服务器端之间进行控制。

(1)客户端控制:有通过设置防火墙并配合预定过滤规则实现数据流的控制[2],也有在终端内核层添加HOOK钩子或修改驱动来实现数据流的控制[3,4]。但是这些方法可能会有两个问题:1)由于移动办公的需求,客户端通常具有连接不确定性、平台多样性等特点,而此类方法大多需要修改或固定终端,十分不便,同时也会增加维护成本;2)因为客户端是由用户个人控制的,可能因为有意、无意的操作而绕过安全控制方案,导致数据控制失效。

(2)服务器端控制:大多是修改底层架构,例如在虚拟机

到稿日期:2015-02-15 返修日期:2015-05-28 本文受中国铁路总公司科技研究开发计划重大课题(2013X010-A)资助。

邓霄霄(1990—),男,硕士,主要研究方向为信息安全,E-mail:turbock@126.com;路 川(1963—),男,硕士,教授,主要研究方向为数据库信息系统;马 威(1985—),男,博士,主要研究方向为信息安全、无干扰模型。

监控器(Virtual Monitor Machine,VMM)中设置钩子并进行分流处理[4],或在将各个数据流控制模块集成的同时并发调用[5]。但它们更偏向性能优化,对系统安全考虑得相对较少。也有研究通过修改驱动[6,7]、优化通信机制[8],或引入策略管理、访问控制模块(Access Control Module,ACM)[9-12]来进行信息流安全的控制,例如 Linux 安全模块、基于强制访问控制的虚拟机安全管理器架构(Secure Hypervisor,sHype)。在 sHype 中,ACM 模块位于 VMM 中,并根据特权虚拟机里的访问控制策略对服务器内数据流进行安全管控,如图 1 所示。但是它们都没有考虑内部应用数据和外部操作平台之间的数据流安全控制。同时,如果在服务器端进行内外部数据流的访问控制,一方面会增加服务器端的工作负荷,影响虚拟桌面的数量上限及其工作性能;另一方面,当客户端接入服务器并取得控制权后,可能会对服务器的设置进行篡改并导致安全控制失效。

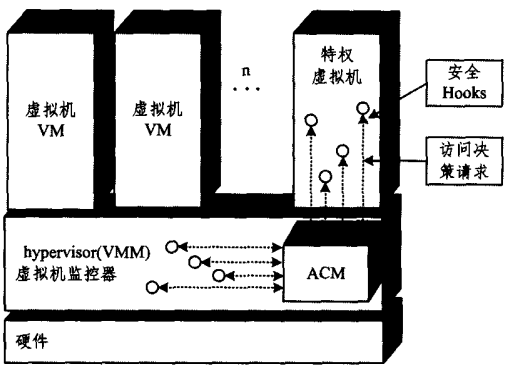

图 1 sHype 架构

(3)客户端和服务器端之间控制:最新的研究中,有的借助虚拟化技术进行多级域间数据流控制[13],增强不同安全级网络之间的安全隔离与信息交换;也有在云服务内部通过网关解决云服务信任及授权问题的解决方案[14];还有的借助软件定义网络(Software Define Network,SDN)和 OpenFlow 架构上的网络安全功能虚拟化(Network Security Function Virtualization,NSFV)来解决数据中心的安全挑战[15,16]。虽然它们均不能解决内外部数据流的安全控制问题,具有一定局限性,但 SDN 方案能够在不改动网络设备的基础上修改网络协议或拓扑架构进而控制数据流,具有较强的灵活性,值得借鉴。

综上所述,在客户端和服务器端之间进行虚拟桌面内外部数据流的安全控制具有以下优势:1)无需对大量的用户终端或多种服务器进行修改、维护和软件安装,能有效降低系统的维护成本;2)将安全风险控制在网关,可降低服务器的安全风险,减少工作负载;3)不改变用户的原有操作方式,能有效保证虚拟桌面的易用性和内部人员的正常工作效率。

2 面向虚拟桌面数据流的安全控制机制

由上节可知,虚拟桌面内外部数据流的安全控制更适合在客户端和服务器端之间实施。桌面虚拟化需要借助 RDP、SPICE、ICA、PCoIP 等协议实现用户操作平台和虚拟桌面之间的数据交互,因此可以通过控制协议来完成它们之间的数据流安全控制。协议控制通常有两种方式:1)修改传输协议本身;2)采用网关模式进行控制。通过研究发现,修改协议不仅工作量大,还存在标准兼容性问题[17,18];而网关模式更实际可行,它不仅能避免兼容性问题,还能满足用户对易用性和拓展功能的需求。因此,本文在网关模式的基础上,提出了一种面向虚拟桌面内外部数据流的安全控制机制——SCIED。

2.1 SCIED 安全架构

网关模式的架构设计如图 2 所示。为保证数据流向符合安全级别规范,需要让所有客户端与服务器端的交互数据包均受到多级访问控制策略的约束,以防有意无意的绕过。因此在网络拓扑时采用双臂模式,借助其对数据包的转发功能,实现外部操作区和内部工作区之间的数据安全控制,从物理层确保一定的安全性。对于安全网关的架构设计,初步参考了访问控制通用框架[19](Generalized Framework for Acccess Control,GFAC)。它将访问控制分为策略决策模块和策略实施模块,以便随时更换策略而不改变控制实施部分,从而增强访问控制的灵活性和扩展性。当外部操作区发起低安全级会话时,则会根据控制策略,对发往低安全级主体的高安全级数据进行细粒度的访问控制。

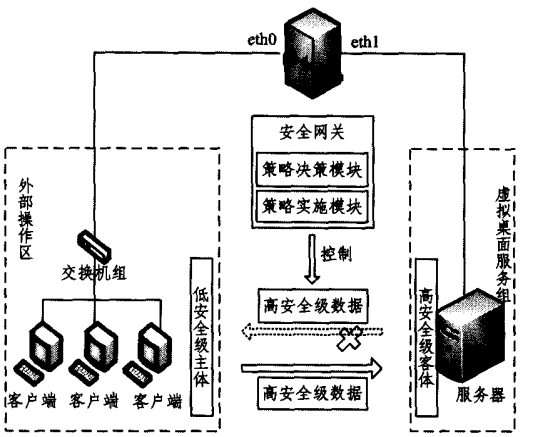

图 2 SCIED 网络基础架构

同时,安全网关需要满足以下几个预设条件:

(1)所有用户的桌面连接请求必须通过安全网关完成,即统一登录网关进行用户身份验证;

(2)安全网关掌握用户信息库,能够完成用户身份认证及虚拟桌面连接;

(3)用户身份认证成功后,可根据角色子集选择会话安全级,并正常接通预定连接的虚拟机;

(4)安全网关拥有策略信息库,可根据角色、客体和会话计算相应的细粒度访问控制策略;

(5)数据中心数据只能通过虚拟桌面协议与外部进行交互,以防绕过的非法数据操作。

2.2 SCIED 控制机制原理

SCIED 的核心思想是将信息分为多个安全级,根据虚拟桌面环境中的用户角色设置临时会话安全级,进而动态调整策略;当用户请求操作时,无论是哪种虚拟通道类型,仅对符合多级访问控制策略的数据包给予通过,而对不符合策略的数据包加以控制,最终实现虚拟通道的全面可控。实施中,SCIED 机制更侧重于数据流控制的实施,而对虚拟通道的具体控制策略不加以考虑,整个机制设计如图 3 所示。

在安全网关上，首先通过检测模块对接收数据包的协议类型进行判断。如果不是虚拟桌面协议，就将数据包转移至其他模块进行处理、转发；否则进行下一步的访问控制判断。通过通道约束和多级约束的计算匹配，对符合访问控制策略的数据包进行转发；对不符合的数据包则继续分析。接着判断数据包所属的虚拟通道类型，对无法识别的第三方通道数据包全部拦截；对可识别的，则根据具体通道的特点选择相应的访问控制方式。最终，对数据包进行修改、转发或拦截，进而避免隐蔽通道的泄密问题。

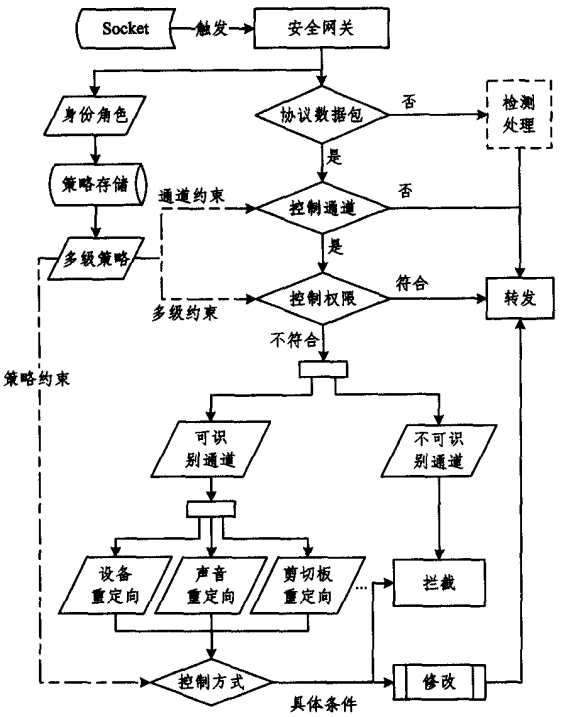

图 3　多级数据流向控制机制

2.3　SCIED 控制方式

根据一般用户登录系统的工作需求，假定几种控制方式：1)双向均不能传输；2)只能进行单向数据传输，例如只能从虚拟磁盘复制文件到虚拟桌面或从虚拟桌面复制文件到虚拟磁盘；3)可以进行双向传输。因此对通道控制的位置也略有不同，如表 1 所列。

表 1　数据流向控制策略

数据流向	c←!! →s 双向拦截	c→s 客户端 单向服务端	c←s 服务端 单向客户端	s←→c 双向通信
通信过程控制位置	1. 主通道连接初始化 2. 子通道建立与初始化 3. 通信转发(c、s)	3. 服务端接收包	3. 客户端接收包	1. 主通道连接初始化 2. 子通道建立与初始化

对于双向拦截的数据流，为减少其资源占用率，应在通道协商建立前就进行阻断。有两种控制方法，一种是在登录网关后进行桌面连接请求时控制，即在配置文件或虚拟桌面连接设置中进行相应修改以开启或禁止通道；另一种是在虚拟桌面连接时控制，对协议认证连接阶段的数据包进行修改，如表 1 中双向拦截控制的位置 1 和 2。在应用过程中，需要根据具体的使用情况选择控制方法。对于通道建立前就确定是否开启的通道，更适合采用第一种方式，进而减少通信资源消耗和开发成本。

对于单向数据流的控制，应根据具体协议及其通道特点进行数据包的接收、控制和转发。由于传输数据和虚拟桌面图像具有很强的关联性，对单向数据包或其中具体数据的修改或拦截将导致图像解析错误和接收端的挂起延迟错误，进而中断会话。因此，为不破坏原有通信机制并保证正常传输，需要对定位到具体通道的数据段标识符做修改、拦截操作。

3　实验评估

3.1　原型系统实现

在实验环境中，网关配置为主频 1.8GHz CPU，1000M WAN/LAN，系统采用 CentOS5.9。虚拟服务器的配置为双 Xeon X5650 CPU，千兆以太网卡，最多同时运行 40 个虚拟桌面，虚拟桌面系统采用 Windows XP；网络存储服务器为单核 Xeon X5650 CPU，千兆以太网卡。

SCIED 原型系统开发采用 QT 集成开发环境，并通过 Rdesktop 提供连接。在实验实现时，根据一般生产系统的工作要求，对原型系统进行了模块化处理，并增添了身份认证、访问控制等功能，其结构如图 4 所示。由于实验侧重虚拟通道中的数据流控制实施，因此仅采用了简单的身份认证方式及访问控制策略来进行 SCIED 机制的可行性验证。

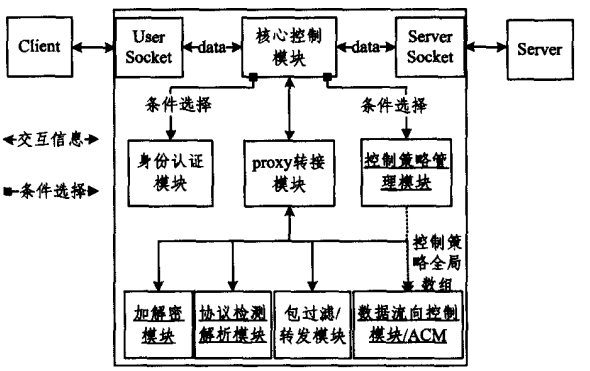

图 4　安全网关控制模块调用

在原型系统中每当有用户请求桌面连接时，安全网关就为其创建一个独立线程，同时将连接成功的客户端套接字 UserSocket 转交给此线程。然后根据用户身份和角色建立与服务器的 ServerSocket 连接，将动态申请的 IP、虚拟桌面与会话绑定。根据用户角色和会话安全级判断相应策略并传入到 proxy 转接模块。通过 select 函数选择线程中被触发的Socket，接收解析数据包并定位到预定控制的数据段。最后根据具体策略和条件采取相应的措施(如拦截、修改)，达到安全控制的目的。

3.2　基于 RDP 协议的数据流控制实验

为证明 SCIED 的可行性，本文以典型的虚拟桌面协议 RDP 为例展开了研究。在虚拟桌面连接时，当用户终端设备需要“映射”到服务器上时，RDP 要为其建立不同的虚拟通道来实现不同类型的数据交互。通过分析 RDP 的开源客户端 Rdesktop 可知，各种虚拟通道都有各自的通信机制，并通过不同 ID 号进行标识，例如默认情况下的设备重定向通道

1005。通过分析它们的数据包结构，可以确定其中各字段的含义，进而实现数据流控制。

以 RDP 剪切板通道为例，将其部分数据包的解密、定位、控制过程记录于日志并截图，如图 5 所示。其中标识＃319 为来自服务端剪切板通道的数据确认包，图中阴影“0x05 00 10 00”为数据确认标识符，右侧 ASCII 码“produce a hex-dump”为需要控制的数据。在定位到需要控制的数据通道类型时，程序根据控制策略“control policy is clipboard:c->s”，对该数据包特定标识符进行修改，并将传递数据段置空；最后通过剪切板通道的测试，证明了 SCIED 能够有效完成数据流的单向传输控制。

在安全性方面，由于只有剪切板通道才支持数据的剪切、复制和粘贴，用户很难绕过此通道来实现数据的拷贝，除非通过第三方通道。然而 SCIED 具有明显的白名单控制特征，即只有符合访问控制策略的数据流才被允许通过，进而将其他数据拷贝途径进行了拦截。

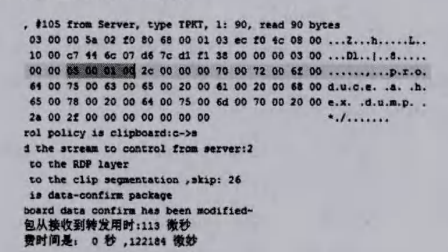

图 5　剪切板数据包的解析及控制

3.3　性能评估

从理论上定义原型系统的相关性能参数、概念和符号，表示如下：

1)设原型系统中不采用 SCIED 的运行状态集合为 $O=\{o_1,o_2,\cdots,o_n\}$，$o_1,o_2,\cdots,o_n$ 为具体的运行实例状态；仅采用 SCIED 中加解密模块的运行状态集合为 $C=\{c_1,c_2,\cdots,c_n\}$；完全采用 SCIED 的运行状态集合为 $S=\{s_1,s_2,\cdots,s_n\}$。它们的关系可用递进式 $O->C->S$ 形象地表达出来。

2)将各个状态 O、C、S 下的单数据包总时延表示为 $T_t=T_s+T_b+T_d+T_q$，其中 T_s 为发送时延，T_b 为传播时延，T_d 为处理时延，T_q 为排队时延。用 $T_d(O)=\{t_d(o_1),t_d(o_2),\cdots,t_d(o_n)\}$ 表示状态 O 中各实例的处理时延集合；同理有 $T_d(C)=\{t_d(c_1),t_d(c_2),\cdots,t_d(c_n)\}$ 和 $T_d(S)=\{t_d(s_1),t_d(s_2),\cdots,t_d(s_n)\}$。

3)设 $\bar{T}_{wn}$ 为用户可感受到的时延均值，属于模糊指标。根据二八定律，假定正常情况下有 $T_t<80\%\times\bar{T}_{wn}$，表示用户工作没有受到影响；当 $80\%\times\bar{T}_{wn}\leqslant T_t\leqslant\bar{T}_{wn}$ 时，时延对用户操作影响很小；当 $T_t>\bar{T}_{wn}$ 时，则用户体验会受到影响。相关研究表明，一般的 $\bar{T}_{wn}$ 指标在 100ms 左右。

4)$\bar{T}_t(O)=\sum_{i=1}^{n}t_t(o_i)/n$ 为状态 O 的处理时延平均值；同理有状态 C 和 S 的处理时延均值 $\bar{T}_t(C)$ 和 $\bar{T}_t(S)$。根据 2)中公式，也有状态 O 下的 $\bar{T}_s(O)$、$\bar{T}_b(O)$、$\bar{T}_d(O)$、$\bar{T}_q(O)$。

5)在状态中 O、C 和 S 中，发送时延、传播时延和排队时延基本没有差别，而主要不同都集中在处理时延 $\bar{T}_d$ 上。因此有公式 $\Delta T_t(OC)\approx\bar{T}_d(C)-\bar{T}_d(O)=\Delta T_d(OC)$，表示状态 C 和状态 O 之间的平均总时延差值约为网关代理上进行额外操作（C 增添了加解密功能）所增加的时延；同理也有 $\Delta T_t(CS)\approx\Delta T_d(CS)$，$\Delta T_t(OS)\approx\Delta T_d(OS)$。

·理论分析

正常情况下都有 $\bar{T}_t(O)\leqslant 80\%\times\bar{T}_{wn}$，为了满足 $\bar{T}_t(S)\leqslant\bar{T}_{wn}$，$\Delta T_d(OS)$ 就成为影响用户体验的关键因素。假设状态 O 的最坏情况下，有时延 $\bar{T}_t(O)=80\%\times\bar{T}_{wn}=80$ms，使用户工作稍微受到影响。所以 SCIED 原型系统至少应该满足 $\Delta T_d(OS)\leqslant 20\%\times\bar{T}_{wn}\approx 20$ms，才可以保证不影响用户体验。

从原型系统结构分析，其中策略管理模块、身份认证模块以及 proxy 转接模块属于同级调用，可以并行处理。proxy 转接模块主要负责各个虚拟桌面会话的数据包接收转发和安全控制工作，需要处理大量的数据包。而策略管理模块和身份认证模块从核心函数接收到少量参数后即完成相应计算，此过程中时间损耗极小，相对于 proxy 转接模块可忽略不计。对于 proxy 转接模块，需要考虑的时间消耗主要是在虚拟通道数据包的加解密、控制通道中特定标识符的定位/匹配和数据包修改/拦截上。由于原型系统需要对数据包进行解密和加密还原，可能会对性能造成一定影响，因此设定了参数 $T_t(C)$ 和 $\Delta T_t(OC)$。同时在标识符定位/匹配和数据包修改/拦截方面，由于数据包结构相对固定，属于有序结构段，其匹配样本空间很小，修改数据段或拦截数据包的耗时理论上极小，即 $\Delta T_d(CS)\approx 0$。所以综上分析，可认为网关代理原型系统的总时延关系为 $\bar{T}_t(O)<\bar{T}_t(C)\approx\bar{T}_t(S)$。

·实验分析

为量化相关性能指标，以剪切板通道为例对其进行了实验测试。对比类型为 3 组，分别是状态 O、状态 C 和状态 S，且对每组实验都进行 10 次测试；每次测试都采取相同的操作，即 2 次双向的“复制”和“粘贴”，并确保操作的数据相同，数据容量为 1000Byte。在网关代理上通过编程将每个数据包从开始接收到发送完成的处理时长记录于日志文档。对于每次测试，从第一个剪切板包开始连续采集，直至最后一个剪切板数据包，并将此数据包以前的所有处理时长进行加和求均值。得到单次实验均值后，再在各组内求 10 次测试的均值，结果如表 2 所列。

表 2　剪切板流向控制实验时延测试

采样及测试	状态 O	状态 C	状态 S
采样包平均处理总时长 $\bar{T}_{dl0}$	138380μs	146718μs	151304μs
采样数据包平均量 N_{l0}	547	529	523
每个采样包平均处理时长 $\bar{T}_{dl0}=\bar{T}d/N$	252.98μs	277.35μs	289.33μs
剪切板包处理总时长 $\bar{T}_{dl0c}$	1699μs	2750μs	3211μs
剪切板包采样量 N_{l0c}	15	15	17
剪切板包平均处理时长 $\bar{T}_{dl0c}=\bar{T}_{dl0c}/N_{l0c}$	113.27μs	184.34μs	194.76μs

因为发送时延、传播时延和排队时延基本一样，从表中 $\bar{T}_{d10}(O)=113.27\mu s$、$\bar{T}_{d10}(C)=184.34\mu s$ 和 $T_{d10}(S)=194.76\mu s$可看出，得到的处理时延均值$\bar{T}_d(O)<\bar{T}_d(C)\approx\bar{T}_d(S)$与原型程序的理论分析基本吻合，即 SCIED 产生的时间消耗主要在数据包的加解密上。在状态 O 转变为状态 S 的过程中，平均每个数据包增加的时延为 $\Delta T_d(OS)=289.3-252.98=36.32\mu s$，该值远小于理论分析中用户体验的最低要求 20ms，进一步从实验上证实了它能够很好地满足用户时延需求。综上所述，尽管实验评估中的样本容量不大，但实验结果较为明显，可以证明 SCIED 对原有桌面会话的性能影响较小。

结束语 针对虚拟桌面环境中内外部数据流的非法交互问题，提出了一个基于网关模式的数据流安全控制机制 SCIED。它具有单向控制功能，能够兼容多种虚拟桌面协议；对不符合多级访问控制策略的数据流均加以控制，以防隐蔽通道泄密。最后通过实验证实了它的安全可行性，并通过建模和分组实验对其性能进行了评估，结果表明它对原有虚拟桌面系统的影响很小。

与当前主流的虚拟化安全架构 sHype 相比，本文设计的 SCIED 及其实现方案不仅增添了内外部数据流的访问控制；还把该功能定位于网关，将外部边界的攻击控制在服务器之外，减少了服务器端的负载和安全隐患。下一步将对该方案进行压力测试分析，使其能够适应数量庞大的虚拟桌面应用场景，进而提高 SCIED 的可用性和实用价值。

参 考 文 献

[1] The Greaves Group. Virtualization in education [M]. USA: IBM, October 2007

[2] Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v3.0[EB/OL]. 2014-11. http://www.cloudsecurityalliance.org/csaguide.pdf

[3] Zheng Xing-yan. The Design and Implementation of Security Virtual Desktop System[D]. Beijing: Beijing Jiaotong University, 2012(in Chinese)
郑兴艳. 安全虚拟桌面系统的设计与实现[D]. 北京：北京交通大学，2012

[4] Wu Jie-wei, Wang Jia-jun, Qi Zheng-wei, et al. SRIDesk: A Streaming based Remote Interactivity Architecture for Desktop Virtualization System[C]// IEEE Symposium on Computers and Communications (ISCC). 2013: 281-286

[5] Zhang Yu-meng, Ren Feng-yuan. Congestion Integrated Control in Virtualized Cloud[C]// International Conference on Progress in Informatics and Computing (PIC). 2014: 486-492

[6] Liu Su-na. Research and Implementation of BLP Based Network Accesss Control Mechanism on Virtualization Platform [D]. Shanghai: Shanghai Jiaotong University, 2011(in Chinese)
刘苏娜. 虚拟化平台下基于 BLP 的网络访问控制机制研究与实现[D]. 上海：上海交通大学，2011

[7] Lai Ying-xu, Hu Shao-long, Yang Zhen. Research of security technology based on virtualization[J]. Journal of University of Science and Technology of China, 2014, 41(10): 907-914(in Chinese)
赖英旭，胡少龙，杨震. 基于虚拟机的安全技术研究[J]. 中国科学技术大学学报，2011，41(10)：907-914

[8] Wang Xiao-rui, Wang Qing-xian, Guo Yu-dong. Design of Information Flow in Collaborative-VMM[C]// 4th IEEE International Conference on Software Engineering and Service Science (ICSESS). 2013: 124-129

[9] Wu Yue, Liu Xiao-dong, Duan Yi-zhen. Design and implementation of secure access control architecture of desktop virtualization[J]. Computer Engineering and Design, 2014, 35(5): 1572-1577(in Chinese)
武越，刘向东，段翼真. 桌面虚拟化安全访问控制架构的设计与实现[J]. 计算机工程与设计，2014，35(5)：1572-1577

[10] Cokder G. Xen Security Modules(XSM)[C]// The Xen Summit of 2007. New York, 2007

[11] Sailer R, Valdez E, Jaeger T, et al. sHype: Secure Hypervisor Approach to Trusted Virtualized Systems: RC23511(W0502-006)[R]. IBM, 2005

[12] Bellovin S M. Virtual machines, virtual security[J]. Communications of the ACM, 2006, 49(10): 104-106

[13] Chen Da, Ma Wei, Li Xiao-yong. One-way Communication Mechanism for Network Security Isolation and Information Exchange[J]. Netinfo Security, 2014, 6(6): 48-52(in Chinese)
陈达，马威，李晓勇. 一种单向安全隔离与信息交换机制[J]. 信息网络安全，2014，6(6)：48-52

[14] Bhatkalkar B J, Ramegowda. A unidirectional data-flow model for cloud data security with user involvement during data transit [C]// International Conference on Communications and Signal Processing (ICCSP). 2014: 458-462

[15] Luo Xuan, Ma Sai, Jin Yao-hui. HADES: A compatible SDN based network virtualization architecture [C]// International Conference on Optical Internet 2014 (COIN). 2014: 1-2

[16] Battula L R. Network Security Function Virtualization(NSFV) towards Cloud computing with NFV Over Openflow infrastructure Challenges and novel approaches[C]// International Conference on Advances in Computing, Communications and Informatics (ICACCI). 2014: 1622-1628

[17] Cen Zhi-song. Research and application design of RDP protocol [D]. Guangzhou: South China University of Technology, 2004 (in Chinese)
岑志松. RDP 协议的研究及其应用设计[D]. 广州：华南理工大学，2004

[18] Red Hat. Spice remote computing protocol definition v1.0 [EB/EL]. 2014-12. http://www.spice-space.org/docs/spice_protocol.pdf. 2009

[19] Abrams M, LaPadula L, Eggers K. A generalized framework for access control[C]// The 13th National Computer Security Conf. 1990: 36-42