



一种基于云—管—端的移动互联网恶意程序管控方案研究

李 俊

(中国移动通信集团江苏有限公司 南京 210023)

摘 要:为应对恶意程序给移动互联网安全带来的严峻挑战,提出了一种基于“云—管—端”模式的移动互联网恶意程序监测和管控方案,包括:建设云计算支撑平台,以实现手机恶意程序的集中分析、研判、策略分发与管理,在移动互联网网络侧实现手机恶意程序的监控和封堵,在终端侧实现手机恶意程序的查杀,从而构建安全、和谐、绿色的移动互联网环境。

关键词:移动互联网;智能终端;安全;恶意程序;云—管—端

doi: 10.3969/j.issn.1000-0801.2013.08.027

Research on a Mobile Malicious Code Management and Control Method Based on Cloud-Pipeline-Terminal

Li Jun

(China Mobile Group Jiangsu Co., Ltd., Nanjing 210023, China)

Abstract: In order to solve the increasingly serious security issues caused by malwares in mobile internet, a “cloud-pipeline-terminal” model was proposed to implement detection and killing of mobile internet malwares. The proposed model composes of a cloud computing platform to support the analysis and measurement of the malwares and to implement strategy distribution and management of the system, a monitoring and intercepting system on the side of mobile communication pipelines and a terminal security application to check and kill the malwares. The purpose is to build a safe and harmonious mobile internet environment.

Key words: mobile internet, intelligent terminal, security, malware, cloud-pipeline-terminal

1 引言

随着全球化和信息化的发展,移动互联网在传统互联网环境下得到了迅速发展和提升,移动互联网^[1]的发展进入高速行驶的快车道。2012年7月19日,中国互联网络信息中心(CNNIC)在北京发布《第30次中国互联网络发展状况统计报告》(以下简称《报告》)^[2]。《报告》显示,截至2012年6月底,中国网民数量达到5.38亿,增长速度更加趋于平稳;其中最引人注目的是,移动智能终端网民规模达到3.88亿,首次超越台式电脑成为第一大上网终端。移动智能终端的广泛使用,使其安全问题日益凸显。瞻博网

络全球威胁监控中心的数据显示,2009-2011年,针对智能手机的恶意软件数量增长了250%,对我国经济、社会发展带来了潜在威胁^[3]。因此,移动互联网恶意程序的检测和查杀成为安全防护技术研究的主要方向。

2 安全威胁与需求

移动互联网恶意程序按照行为特征可分为3类:资费损失类、隐私窃取类以及功能损坏类。

资费损失类安全事件主要有两种形式:一种是恶意扣费,另一种是资费消耗。恶意扣费类通过订购SP服务实现;资费消耗类则通过短信、彩信、上网流量实现。恶意订

购 SP 服务的扣费方式是一种主要的资费损失渠道,SP 通过这种方式可以赚取巨额利润。还有很多终端则直接内置恶意吸费软件,通过恶意代码从底层调用各类通信方式,包括发送短信、彩信、拨打声讯台和发起网络连接实现资费的消耗,如“手机骷髅”和“僵尸”病毒等。

隐私窃取类恶意软件在用户不知情的情况下读取用户隐私数据,包括电话本、短信和位置信息等,然后在后台启动数据连接或通过短信将相关信息发回给指定的手机、网站服务器;还有一些恶意软件可以在用户打电话时在后台启动电话录音,通过数据连接回传信息,或直接在打电话时启动三方通话,第三方的发话器静音,达到窃听用户通话的目的。

功能损坏类恶意软件通常利用手机操作系统的漏洞,有的会破坏手机硬件,有的会破坏系统软件。

以上是移动互联网恶意程序的具体表现形式,为达到检测和查杀的最终目的,本文对恶意软件的植入方式进行分析并分类如下。

- 伪装成正常软件通过应用商店植入。恶意攻击者通过反编译直接得到源代码,将恶意代码插入正常的应用软件中,然后重新编译发布。许多恶意代码嵌入时下非常热门和流行的应用软件中,通过论坛和非官方的应用商店进行大范围传播。
- 固件植入。“越狱”后的手机由于没有权限限制,用户可以进行“刷机”操作。大多数用户“刷”的是经过修改、美化的第三方 Android 系统固件,恶意软件可能随着第三方 Android 系统固件植入用户的手机中。通过固件植入的恶意软件伪装成系统程序,隐蔽性更好,更不容易被用户察觉。
- 系统漏洞植入。同 PC 一样,智能终端的系统漏洞也可以被攻击者利用。攻击者可以通过系统漏洞在终端安装恶意程序窃取用户隐私或破坏用户数据。
- 手工植入。对于具有间谍软件性质的监控类软件,多是通过社会工程学等手段,手工植入用户手机中,如前文提到的家长控制工具“Kidlogger”,还有臭名昭著的“X 卧底”,早期版本也是运用手工植入的方式。
- 捆绑植入。应用软件安装包中包含原始的、不会被压缩的资源文件,攻击者将恶意软件直接捆绑到普通软件中,普通软件安装后,恶意软件安装包被释放,然后安装到用户手机中。如“绿色家园”应用软件安装包中的木马,正常应用程序安装后,会释放

出一个名为 Testnew.Apk 的木马子包,这个子包会自动安装到用户手机上,实施恶意行为。

- 诱骗下载。诱骗用户主动下载恶意软件的方式比较多,有的是通过给用户发送带有恶意软件下载链接的短信、彩信,并附上诱惑性的说明文字,诱导用户点击下载;或者打着热门应用软件的名号,欺骗用户,导致用户下载恶意软件;或者利用二维码,用户使用手机中的二维码识别软件扫描后得到恶意软件下载地址。
- 已安装恶意软件后台下载。有些恶意软件内部含有“下载器”,安装后还能在后台源源不断地下载其他恶意软件到用户的手机中。

对于运营商,移动互联网恶意程序造成不知情订购投诉事件频发、网络和业务质量缺乏安全保障,导致用户满意度指标面临挑战,影响企业形象和声誉,需要建立有效可行的移动互联网恶意程序管控方案。

现有的移动互联网恶意程序查杀软件主要实现终端操作系统的木马病毒查杀、恶意行为监控以及隐私保护等。基于以上分析可知,恶意程序不仅局限于在智能终端上实现恶意行为,需要实现一套终端查杀、传输管道侧监控和封堵以及云端分析处理的恶意程序管控方案,从而更加完整、有效地实现针对移动互联网恶意程序的安全控制和防护。

3 移动互联网云管端恶意程序查杀管控方案

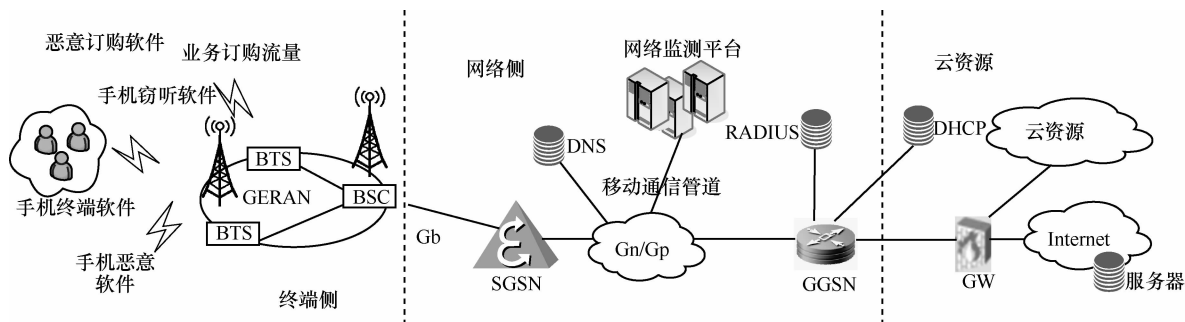
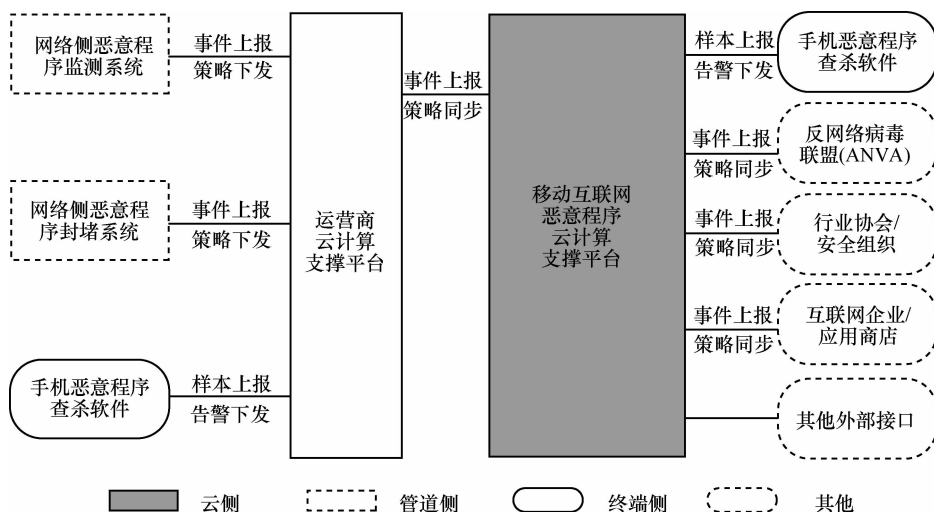
本文提出一种基于“云—管—端”的移动互联网恶意程序管控技术方案,需要分别建设云计算支撑平台、管道侧监控与封堵系统、终端侧查杀软件形成“云—管—端”多级架构,从而在多者之间形成联动,完成移动互联网恶意程序检测和查杀的功能闭环。方案的具体架构如图 1 所示。

3.1 方案网络结构

“云—管—端”恶意程序管控方案的网络结构如图 2 所示。云资源实现恶意程序的集中分析、研判、策略分发和管理;管道侧实现恶意程序的实时监测和封堵;终端侧实现恶意程序的确认和查杀。

3.2 云计算支撑平台

鉴于智能终端在计算和存储能力方面的局限性,恶意程序分析和研判操作会对智能终端的便携性、易用性带来挑战,从而严重影响用户体验,因此需要建立国家和运营商两



- 疑似样本分析: 汇总前端上报的疑似样本并入库; 完成疑似样本的相关统计工作; 汇总前端工作信息, 监测前端的工作状态; 提供病毒列表; 跟踪新发现病毒的增长趋势。
- 提供相关配置: 提供检测策略管理操作、配置策略管理操作以及黑白名单地址管理操作, 并向前端分发。
- 接收病毒库更新: 提供病毒特征库更新, 预留接收其他平台提交的特征信息、病毒信息的接口; 提供特征库管理操作。

3.2.2 云端特征库

平台建设的目的为建立一套完善的云平台特征库,从而更有效地实现恶意程序的检测和监控。如图3所示,特征库主要实现以下功能。

- 贡献样本:运营商、安全厂商和科研机构通过 Web 方式上报病毒样本。
- 样本审核:样本审核者可对病毒样本进行基本信息的查看和修改、样本体下载和样本审核。

- 贡献样本:运营商、安全厂商和科研机构通过 Web 方式上报病毒样本。
- 样本审核:样本审核者可对病毒样本进行基本信息的查看和修改、样本体下载和样本审核。

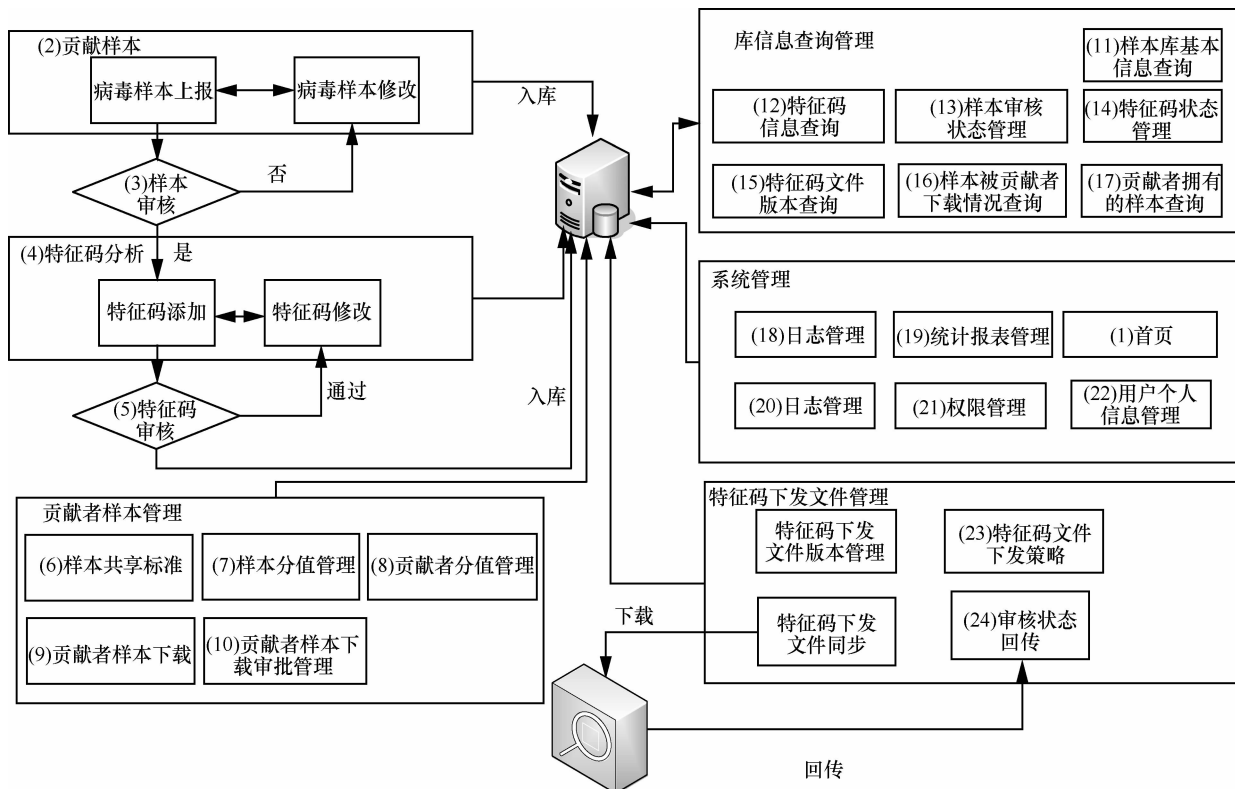


图3 云端特征库交互流程

- 特征码分析: 分析者下载已经审核通过的样本, 分析完成后, 上报病毒特征码。
- 特征码审核: 审核者下载样本和特征码或者只根据特征码, 进行特征码验证和审核。
- 样本基本信息查询: 查看正式入库的样本信息。
- 特征码信息查询: 查看正式入库的特征码信息。
- 样本审核状态管理: 查看样本审核过程中的状态信息, 如备注、审核状态, 不可以下载样本。
- 特征码审核状态管理: 查看特征码审核过程中的状态信息, 如备注、审核状态, 可以修改特征码的审核状态。
- 特征码文件版本查询: 查看特征码文件的版本信息, 显示出每个版本的<样本编号, 特征码编号>。
- 样本被下载情况查询: 输入样本名, 查出能下载该样本的贡献者的列表。
- 统计报表管理: 用来显示指定时间内“正式入库”的样本及特征码的趋势图以及指定时间内样本审核状态的饼图。

3.2.3 云端智能扫描引擎

云端智能扫描引擎为支撑平台的核心模块, 利用特征

码扫描、API 扫描以及动态沙箱技术, 实现对已知和未知恶意程序的检测以及恶意程序的行为分析等功能。

(1) 手机恶意程序特征码扫描引擎

手机恶意程序特征扫描引擎主要利用特征码扫描技术, 以手机文件特征检测手机病毒。文件特征扫描的核心原理是对手机文件格式解包后的每个文件进行 16 进制的快速特征定位。扫描过程中搭配恶意程序特征码序列数据库, 通过动态匹配库中的恶意程序特征码, 达到检测恶意程序的目的。

(2) 未知手机恶意程序扫描引擎

未知手机恶意程序扫描引擎主要采用手机终端软件文件静态 API 扫描技术。通过对不同平台的手机文件格式分别进行解析提取病毒常调用的危险函数序号, 或者通过病毒分析人员的整理归纳出一个常见的病毒调用恶意函数的特征库, 在扫描程序运行过程中通过比对特征库的方式发现手机病毒的恶意行为。

(3) 动态沙箱建设

动态沙箱的本质是利用软件的环境模拟真实终端硬件环境运行目标程序。

Android 动态沙箱通过结合 Android 自身 SDK 接口在



不影响目标程序运行的前提下,对目标程序的运行行为进行跟踪和记录,并结合病毒特定恶意行为特征进行综合分析,从代码、文件、网络 3 个方面进行恶意行为总结,实现病毒恶意行为的全功能研判。

J2ME 动态沙箱主要建立在以 Java 为核心的平台之上,通过 Java 自身的成熟模拟器环境和特定接口,结合自身总结的一些病毒特定恶意行为特征,主要监控恶意程序的文件行为、网络套接字行为、联网行为、加密联网行为和短信收发等行为。

(4) 手机恶意程序爬虫系统

手机终端软件网络爬虫系统建设主要包含:URL 管理与处理模块、数据下载模块、数据解析模块、数据识别提取模块。

3.3 管道侧监控与封堵系统

移动互联网恶意程序需要发送恶意订购消息到非法 SP 实现恶意订购、上传隐私信息到攻击者的服务器等,或者下载和更新恶意程序组件等,因此需要在移动互联网通信管道(Gn 口)部署恶意程序安全检测和封堵平台,实现移动互联网恶意流量的监测和各类恶意程序的监控及封堵。

3.3.1 主要功能

移动通信管道侧的管控主要实现的功能如下:

- 在移动互联网管道的 Gn 口部署恶意程序检测和封堵系统,通过实时深度 DPI 技术,还原网络数据和行为,识别恶意程序并定位受感染的用户号码;
- 将恶意程序事件及疑似事件提交至云计算支撑平台,进行集中分析、研判和管理;
- 云计算支撑平台将确认的恶意程序下发给管道侧检测和封堵系统,实现全网恶意程序的封堵。

3.3.2 部署方案

管道侧监控与封堵系统网络结构如图 4 所示,系统部署于核心网内,主要提供如下两方面功能。

- 管道侧监控:通过对 Gn/PI 流量分光,实时采集分

组域流量通过对流量特征和关键字的监测,发现移动互联网恶意事件。

- 管道侧封堵:通过流控设备以及与现网其他网元(如短信网关、垃圾短监控系统)的联动,主动封堵恶意行为的传播。

3.3.3 功能实体

基于管道侧的网络系统结构和组网原则,需要采用分布式部署方式实现流量的采集和检测。分布式部署通过恶意软件检测代理和疑似样本及行为信息汇聚代理两个功能实体实现。

(1) 恶意软件检测代理

主要实现对已知恶意软件的检测和检测记录信息的上报,主要功能如下:接收云管理平台下发的特征库、配置策略,与管理平台保持同步;对 Gn 口分光数据流量进行还原,获得网络日志和样本文件;发现终端用户连接恶意软件主控 URL 的网络事件,汇总相关网络日志上报给管理平台;利用本地的非恶意软件文件样本 MD5 特征库对样本文件进行过滤,去除不可能是恶意软件的文件样本;利用本地恶意软件特征库对样本文件进行恶意软件特征匹配,检测恶意软件传播事件上报管理平台;将经过以上两类特征匹配检测之后剩余的疑似恶意软件样本及其相关网络日志上报给疑似样本及行为信息汇聚代理进行汇总去重处理。

(2) 疑似样本及行为信息汇聚代理

主要实现对疑似恶意软件行为信息的汇聚、疑似恶意行为日志的筛选和上报;支持对用户连接恶意软件的主控 URL 和下载 URL 的网络日志的检测,汇总后上报给管理平台;接收 Gn 口数据分析系统、Gi 口不良信息监测系统和恶意软件检测代理 3 种接口数据;接收管理平台下发的配置策略、疑似恶意软件网络行为筛选规则、已入库未研判疑似样本 MD5 特征库、全网恶意软件下载 URL 库、全网恶意软件主控 URL 库的更新,与管理平台保持同步;对得到的数据进行汇总和去重操作;对于恶意软件检测代理上报的疑似恶意软件样本文件及其相关的网络日志,进行过滤后上报给管理平台。

3.4 终端侧查杀软件

终端侧查杀软件实现智能手机用户信息的安全存储、访问控制、软件恶意行为检测、异常数据流量监测等功能,并通过手机终端安装方式保护智能手机终端上的个人信息安全。同时,终端侧查杀软件需要与网络侧和云计算支

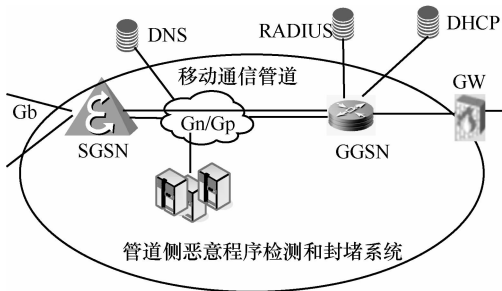


图 4 管道侧监控与封堵系统网络结构

撑平台实现联动,为“云—管—端”一体化安全防护服务体系提供必要的支撑。

终端侧恶意程序查杀软件界面如图 5 所示,软件功能结构设计如下。



图 5 终端侧恶意程序查杀软件

- 手机体检: 检查当前手机的防护及手机运行状态, 为用户提出优化建议。
- 病毒查杀: 对用户手机进行杀毒扫描, 并对用户手机进行监控, 保护用户手机安全。
- 主动防御: 主动拦截手机系统的敏感权限, 阻止软件窃取用户隐私。
- 流量监控: 监控用户手机上网时的流量使用情况, 包括 2G/3G 和 Wi-Fi 所使用的流量。
- 隐私保护: 对用户手机上的程序或文件进行加密处理, 保护用户隐私。
- 程序保护: 对用户手机上的应用程序进行加密。
- 手机防盗: 手机丢失后, 用来保护手机上数据信息的安全, 防止数据信息被他人窃取。
- 系统设置: 系统设置界面。
- 安全信息推送: 实时获取最新的安全防护信息, 了解安全防护动态及趋势, 丰富安防知识, 加强安防意识。

4 方案验证

本文提出的基于“云—管—端”的移动互联网恶意程序管控方案在某运营商进行试点, 表 1、表 2 分别显示了试点当月管控方案部署后, 检测和查杀的活跃病毒 top 10、恶意扣费病毒 top 10。试点结果证明, 本文提出的“云—管—端”管控方案可以完整、高效地检测和查杀移动互联网恶意程序。

表 1 活跃病毒 top 10

序号	病毒名称(中文)	病毒名称(英文)	属性主分类	感染用户数
1	伪视频病毒变种	Video.B	恶意扣费	4 271
2	疯狂短信	Smswish.A	隐私窃取	3 763
3	泄密超短裙病毒变种	Skirtup.b	隐私窃取	3 387
4	XVCI 病毒变种	XVCI.B	隐私窃取	3 119
5	系统设置吸费王	Smart.A	资费消耗	2 998
6	JazzMusic 病毒	JazzMusic.A	隐私窃取	2 792
7	FakeS60App 病毒	Fakes60App.a	恶意扣费	2 395
8	伪 OVI 客户端病毒	OVIClient.A	隐私窃取	2 336
9	毒媒手机木马	Dumusicplay.b	远程控制	2 204
10	伪视频病毒	Video.A	隐私窃取	2 194

表 2 恶意扣费病毒 top 10

序号	病毒名称(中文)	病毒名称(英文)	属性主分类
1	伪视频病毒变种	Video.b	恶意扣费
2	系统设置吸费王	Smart.a	资费消耗
3	FakeS60App 病毒	FakeS60App.a	恶意扣费
4	实习护士木马	nurse.a	恶意扣费
5	Gangstar 恶意扣费病毒	Gangstar.b	恶意扣费
6	扣费歪歪变种	sbyy.b	恶意扣费
7	伪安全杀毒病毒变种	SoftBox.d	恶意扣费
8	kfun 木马	kfun.a	恶意扣费
9	实习护士木马变种	Nurse.b	恶意扣费
10	柠檬听扣费木马	lemon.a	恶意扣费

5 结束语

本文提出的技术方案可以实现手机恶意程序的集中分析、研判、策略分发与管理, 在移动互联网网络侧实现手机恶意程序的监控和封堵, 在终端侧实现手机恶意程序的

(下转第 167 页)

- 位置通道(cursor channel),指示设备的位置、可视性和光标形状;
- 音频播放通道(playback channel),指示来自服务器待由客户端播放的音频;
- 音频捕捉频道(record channel),指示客户端捕捉的音频。

7 结束语

SPICE 协议实现了通用接口的定义,可以直接对接口进行调用,而将平台相关的实现置于对等目录中。编程过程中,较容易实现屏幕绘图和通道信息的传输。SPICE 协议已经显现了 6 个通道的定义,基本满足云桌面远程连接和桌面展现的需求,而且新通道的定义也较容易实现,经过后期开发,也能实现应用程序数据的传输。

目前笔者已经实现基于 SPICE 协议的云桌面原型系统开发,实现的功能包括多终端统一接入、云桌面用户和桌面管理以及自服务门户,具体介绍如下。

- 多终端接入功能,包括支持 PC、瘦终端、Android 终端、iOS 终端接入云桌面。
- 云桌面用户管理功能,包括用户创建、编辑、分组等。
- 桌面管理功能,包括桌面的创建、修改、克隆、删除和分配等。
- 自服务门户,用户可以通过自服务门户提交性能扩容申请,包括对云桌面进行启动、关闭、重启等。

该云桌面原型系统在公司内部进行了一年左右的试点,效果较好,平台未出现性能问题和功能故障。

总的来看,基于 SPICE 开源协议,在功能上,能实现行

业内优秀的云桌面产品的功能。开源 SPICE 协议的云桌面将是未来云桌面领域的一匹“黑马”,为国内云桌面产品的应用推广推波助澜。

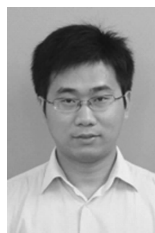
参考文献

- 1 龚德志, 闻剑峰. 虚拟化技术在电信服务器资源整合中的应用研究. 电信科学, 2009, 25(9)
- 2 石屹嵘, 段勇. 云计算在电信 IT 领域的应用探讨. 电信科学, 2009, 25(9)
- 3 闻剑峰, 龚德志. 虚拟化技术在电信灾难恢复计划中的应用研究. 电信科学, 2009, 25(9)
- 4 成静静. 基于虚拟化的云桌面技术方案研究与设计. 广东通信技术, 2011, 31(6)

[作者简介]



石屹嵘,男,中国电信股份有限公司上海研究院高级工程师、信息技术部主任工程师,长期从事系统架构、云计算、系统审计和信息安全等方面的研究工作。



龚德志,男,中国电信股份有限公司上海研究院工程师、中国电信企业信息化验证实验室主管,主要研究方向为云计算、大数据、信息系统评测和容灾。

(收稿日期:2013-03-05)

(上接第 161 页)

查杀。本技术方案实施后,将为移动通信网络提供优质的风险评估、安全防护符合性评测和安全咨询等专业服务,在保障移动通信网络的安全稳定运行、人民群众安全通信和减少国家经济损失方面具有重要意义。

参考文献

- 1 李钧. 移动互联网的安全之思. 网络与信息, 2011(10):61~63
- 2 <http://www.cnnic.net.cn/dtygg/dtgg/201207/W020120719405405832029.pdf>
- 3 王勇斌. 移动互联网网络安全探析. 现代电信科技, 2008, 39(8):

28~30

- 4 <http://www.cert.org.cn/publish/main/upload/File/201208282mobile.pdf>
- 5 潘娟, 史德年, 马鑫等. 移动互联网形势下智能终端安全研究. 移动通信, 2012, 3(5): 48~51

[作者简介]

李俊,男,中国移动通信集团江苏有限公司网络部工程师、部门副总经理(资深),主要研究方向为通信网络网管支撑系统、网络安全与信息安全。

(收稿日期:2013-07-25)