



面向融合网络的广电双向接入网入侵检测系统

邱 菡¹, 兰巨龙², 欧阳峰³, 张传浩², 王艳红⁴

(1. 信息工程大学 郑州 450002; 2. 国家数字交换系统工程技术研究中心 郑州 450002;

3. 国家新闻出版广电总局广播科学研究院 北京 100866;

4. 大连梯耐得网络技术有限公司 大连 116023)

摘 要: 针对广电接入网边界缺乏安全防护措施的现状, 提出一种面向融合网络的广电接入网入侵检测系统, 并实例化为 SunGnet703, 可检测并实时阻断进出接入网边界的各类网络攻击。系统具有“非配合”部署、高可靠性运行、“隐形”确保自身安全、全维数据分析 4 个特点, 可为广电接入网边界提供一种简便易行的安全防护方法和实际系统。

关键词: 广电双向接入网络; 入侵检测; 智能终端

doi: 10.11959/j.issn.1000-0801.2015149

Broadcasting Bidirectional Access Network Intrusion Detection System Facing Tri-Networks Integration

Qiu Han¹, Lan Julong², Ou Yangfeng³, Zhang Chuanhao², Wang Yanhong⁴

(1. The Information Engineering University, Zhengzhou 450002, China;

2. National Digital Switching System Engineering & Technology R&D Center, Zhengzhou 450002, China;

3. Academy of Broadcasting Science, SARFT, Beijing 100866, China;

4. Dalian Tnet Network Technology Co., Ltd., Dalian 116023, China)

Abstract: China's broadcasting bidirectional access network now rarely takes effective measures to protect its boarder safety. In view of this situation, a network intrusion detection system for the border safety was proposed and an example product called SunGnet703 was given. The system can detect network attacks passing through the border in real time with four notable features, non-aided deployment, high reliable operation, not able to be detected to ensure its own safety and full data collection, and hopefully it can give a simple and easy-to-accomplish solution to protect the border safety.

Key words: broadcasting bidirectional access network, intrusion detection, intelligence terminal

收稿日期: 2015-01-28; 修回日期: 2015-06-11

基金项目: 国家高技术研究发展计划(“863”计划)基金资助项目(No.2011AA01A103), 国家重点基础研究发展计划(“973”计划)基金资助项目(No.2012CB315900)

Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2011AA01A103), National Basic Research Program of China (973 Program) (No.2012CB315900)

论文引用格式: 邱菡, 兰巨龙, 欧阳峰等. 面向融合网络的广电双向接入网入侵检测系统. 电信科学, 2015149

Qiu H, Lan J L, Ouyang F, *et al.* Broadcasting bidirectional access network intrusion detection system facing tri-networks integration. Telecommunications Science, 2015149



1 引言

在三网融合政策以及数字化、网络化、智能化等技术的推动下,广播电视网络演变成了一个综合信息通信网络,既包括传统的单向信息广播网络也包括双向传输网,还可以接入互联网。广电机顶盒终端也从单向广播型向DVB(digital video broadcasting)+OTT(over the top)双向智能化演进,各地广电运营商还在发展融合型的家庭智能网关,以便用户所有智能终端都能随时随地收看数字直播等业务并能同时连接互联网,“电视设备网络化”趋势也逐渐模糊了个人电脑、个人通信终端和电视机的界限。

三网融合演进中,广电网原来安全的部分在新的融合形势下可能变得不再安全。双向改造为普通用户带来自主、个性化视频观看服务的同时,也为恶意攻击者提供了攻击路径,传统广电网络单向传播这一安全基石不复存在。终端智能化、电视网络化也为广电网带来新的安全隐患,智能化的机顶盒、电视机、家庭网关等终端运行在各种处理器平台基础上,安装有 Android 等操作系统,具备了连接外部网络的双向通信通道,也就可以成为恶意攻击者实施网络攻击的目标或者攻击跳板^[1]。

长久以来,广电网络围绕播出内容安全形成了体系化的内容安全保障技术,覆盖从广电前端网络到终端网络整个传播过程,采用了人工审查、回传监看、条件接收、DRM

(digital rights management)等技术,取得了很好的效果^[2]。相比内容安全保障技术,广电网的网络安全保障技术建设正经历从单向广播网络向综合信息网络演变的过程,还未能形成完备的网络安全保障体系。本文着眼于广电接入网的网络安全保障技术研究,提出一种面向融合网络的广电接入网入侵检测系统——SunGnet703,通过在 OLT(optical line terminal)上联链路中部署该系统,可检测针对广电智能终端的各类网络攻击,也可发现以智能终端为跳板对广电前端网络发起的攻击,从而大幅降低乃至防止攻击者通过接入网实施的以“致瘫”、“致乱”、“控制”为目的的网络攻击。

2 广播电视网络接入网安全

2.1 广电网网络结构

如图 1 所示,广电网网络可分为外部网络和内部网络,其中内部网络分为前端网络、传输网络和终端网络三大部分。

- 外部网络:对应于广电网络之外的其他公共网络,如互联网。
- 前端网络:对应于广播业务前端网络、双向业务前端网络和广电办公网络,位于运营商网络的前部,完成日常办公和广播、双向业务的节目管理、节目发布、EPG (electronic program guide)、BOSS/SMS 等功能,在整个广电网络通信系统模型中可抽象成源端部分。

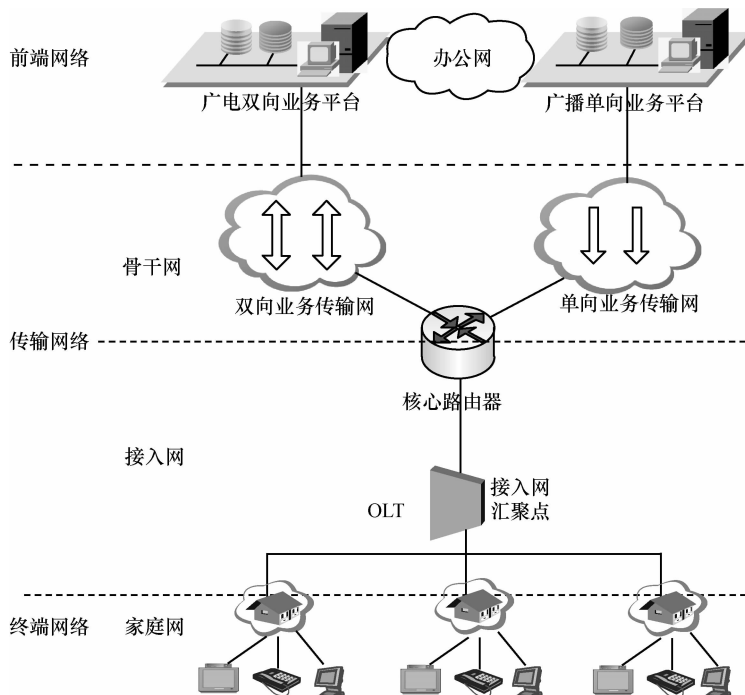


图 1 广电网络层次关系示意

- 传输网络:位于前端网络之后,在整个广电网络通信系统模型中可抽象成信道部分;包括单向广播传输网络和双向传输网络,从层次上还可分为骨干网络和接入网络,骨干网络由骨干路由器连接构成,接入网络通常采用 PON (passive optical network)+EOC(ethernet over coax)或其他接入方式。
- 终端网络:以新型机顶盒或家庭智能网关形成的家庭网络,在整个广电网络通信系统模型中可抽象成终端部分。

2.2 广电接入网边界网络安全

广电接入网边界网络包括外部网络与前端网络之间的区域边界、前端网络与传输网络的区域边界、传输网络与终端网络的边界。目前,广电网已在前端网络与外部网络边界、前端网络与传输网络边界加装了防火墙、IDS、IPS (intrusion prevention system)等常规安全防护设备,以防范攻击者从外部网络或办公网络对广电前端网络发起攻击,防范攻击者从双向传输网络或者终端网络对广电前端网络发起攻击。相比而言,在传输网络与终端网络的边界上至少有相应的网络安全保障技术提出和实施。广电网的网络安全建设需要对网络整体实施安全加固,忽视对传输网络与终端网络边界的安全防护可能会造成安全木桶的“短板”,即网络的整体安全并不是由安全性最强的那一部分决定,而往往由安全性最低的那部分确定。

接入网无边界防护可能带来许多安全隐患,具体如下。

- 攻击者可从终端网络发起对前端网络的上行攻击。从终端网络上,Wi-Fi 路由器已经被充分证明存在安全漏洞^[3,4],已引起人们警觉。相比 Wi-Fi 路由器,智能机顶盒潜藏的安全漏洞很少被关注,实际上,很多智能机顶盒由于升级困难,再加上人们对机顶盒安全的意识薄弱以及机顶盒本身的“静默”特性,使得机顶盒安全隐患的潜伏期更长,更容易被恶意攻击者大范围、大规模长期控制,可能造成更大的破坏后果。攻击者可利用各种终端漏洞从家庭网络发起攻击,在没有安全区域边界或者安全区域边界能力不够的情况下,入侵双向业务平台,控制服务器等设备,使应用系统瘫痪,或非法篡改替换各种数据、文字、图片、视频等,使得机顶盒等终端不能正常使用或显示播放非法信息。还可利用大规模机顶盒发动泛洪攻击等。

- 攻击者可从前端网络发起对终端网络的下行攻击。通过控制大量机顶盒酝酿大范围安全事故,利用机顶盒静默特性造成机顶盒下载存储非法应用,播放非法信息。
- 非法的终端可能以假冒的身份轻易进入网络,进行各种破坏活动;合法身份的终端在进入网络后,也可能越权访问各种网络资源。

有几种方法可以降低接入网边界无防护带来的安全隐患。一种是对智能终端及时更新操作系统补丁,安装病毒、恶意代码防范工具,增强身份鉴别登录,采用安全的远程管理。例如,可通过安装 TVOS^[5,6],在软件层植入安全模块增强终端安全性。这种方法能够较好地改善接入网安全环境,但需要用户或终端厂商“配合”,加载很多额外安全模块,增加了系统运行的成本,也不利于多厂商设备的互联互通。另外一种是利用已有网络设备的安全属性增强安全,例如,在接入路由器上设置访问控制列表增强安全性,限制非授权用户的访问。这种方式的问题是功能受限,只能进行简单的 ACL (access control list, 访问控制列表)控制,无法识别针对应用层的攻击。

3 广播电视接入网入侵检测系统

本文提出了一种面向融合网络的广电接入网入侵检测系统,通过在接入网汇聚点之上串接部署该系统,精确识别接入网汇聚流量中的各种融合业务成分,准确把握接入网流量中用户和终端的组成及变化规律,拦截经由该接入网汇聚点传播的不良信息,阻断恶意攻击,实现对接入网的“非配合”方式的网络边界安全防护。

3.1 接入网入侵检测系统组成及原理

广电接入网入侵检测系统的组成如图 2 所示,系统分为前端和后端两大部分。前端子系统串联/并联接入 OLT 上联链路,基于硬件化的深度分组检测(DPI)、深度流检测(DFI)技术,完成对汇聚流量的实时、智能识别,实现对汇聚流量的正确处理:对系统允许转发的视听流量进行转发;对不允许转发的节目内容进行阻断;对确知攻击特征的攻击流量进行清洗;对可疑流量或者后端系统需求的流量进行采集并传送给后端子系统深入分析。后端子系统对前端子系统筛选出的数据分组进行进一步的分析处理,一方面,通过对采集流量进行挖掘及分析,直观展现广电运营商的互动业务、互联网业务、直播业务及用户使用情况和收益情况,包括内容热点、各类型 URL 访问频度、频道

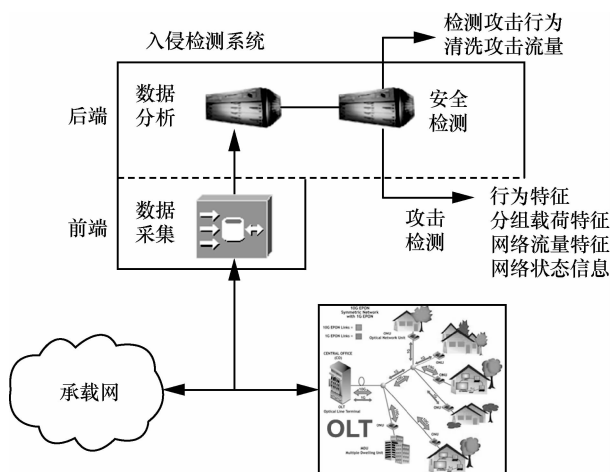


图2 广电接入网入侵检测系统组成示意

用户数、用户流量分析等；另一方面，系统中设置安全检测模块，当安全威胁到达后，该模块可根据安全威胁库对已知威胁特征的安全威胁进行比对检测，发现威胁后实时通知前端系统进行阻断等处理；而对于 0-day 攻击等需要后验知识才能确定的未知特征安全威胁，安全检测模块可基于前端子系统采集的全维数据，方便地利用大数据关联分析方法发现威胁^[7]，这也是目前主流的一种未知特征安全威胁检测方法。

入侵检测系统缺省部署方式是串行接入 OLT 上联链路，如图 3 所示。串接部署方式下，系统可检测安全威胁，实时检测并阻断、清洗恶意攻击流量。对前端子系统而言，由于其串接在汇聚点链路中，一旦发生故障造成线路中断，将引发严重后果。因此，在前端子系统发生故障时如何确保所串接的高速通信线路能不受影响地正常通信是系统设计必须考虑的一个核心问题，为此，系统设计并实现了线速串接光/电切换保护技术，在出现故障时能实时将链路切换到透明传输模式，自动实时避绕了故障点，保证

接入网正常不间断运行。

接入网络汇聚点的数据量大、业务类型多、内容复杂，接入网入侵检测系统需要识别多个层面的安全威胁。系统将采用分层功能模型，如图 4 所示，系统按照处理的复杂度由易及难、由已知特征到未知特征，逐层对数据量进行约减，综合运用多层面的分析处理及综合检测与控制技术，保证接入网安全。系统包括管理控制层、协议处理层、深度识别层和管控实施层。其中，管控实施层依据深度识别层的识别结果实施清洗、阻断等控制操作；深度识别层综合运用 DPI、DFI 等识别技术对报文进行分组级分析、流级别还原、内容级筛查，发现已知特征的安全威胁；协议处理层主要完成用户行为审计、数据关联分析、域间逻辑隔离和边界综合防护等的协议处理功能，发现未知特征安全威胁；管理控制层将集成策略维护、可视化展示、系统运维与联动等功能。这种分层的系统结构能够有效地集成高速接入网入侵检测系统的各种功能，同时又能将整个系统划分成多个功能独立的模块和分系统，便于各个模块及分系统的灵活组合与独立开发，具有良好的可扩展性和重构能力。

3.2 接入网入侵检测系统支撑技术

入侵检测系统以汇聚点上联链路为威胁检测与管控的对象，基于前端子系统线速采集、线速检测与管控功能和后端子系统数据关联检测安全威胁功能，可形成广电接入网入侵事件事前预警、事中阻断和事后追溯。以下将针对系统进行技术分析，指出其发展方向。

(1) 前端子系统深度数据检测与控制技术

前端系统以专用硬件实现 DPI、DFI 技术^[8]，可实现将已知的无威胁内容转发，将已知的安全威胁流量阻断功能。其中 DPI 负责对高速网络链路上的数据分组进行实时深度检测，服务于数据的一致性校验、安全威胁分组级特征的发现和控制；DFI 负责对高速网络链路上的数据流进

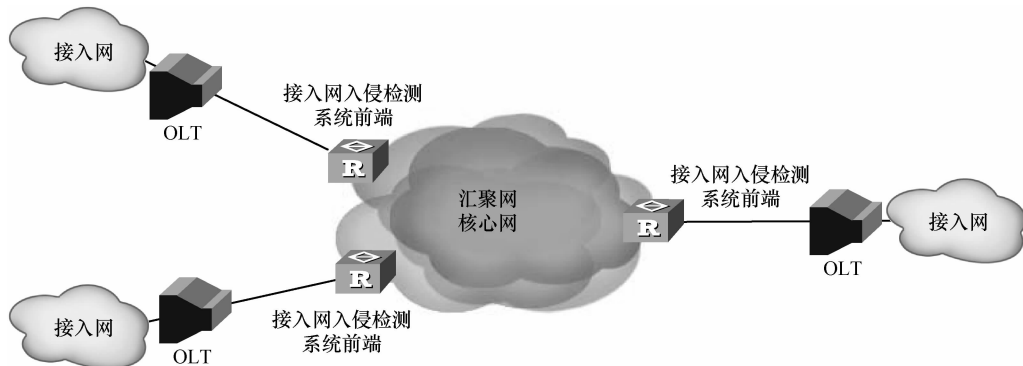


图3 接入网入侵检测系统前端的部署位置

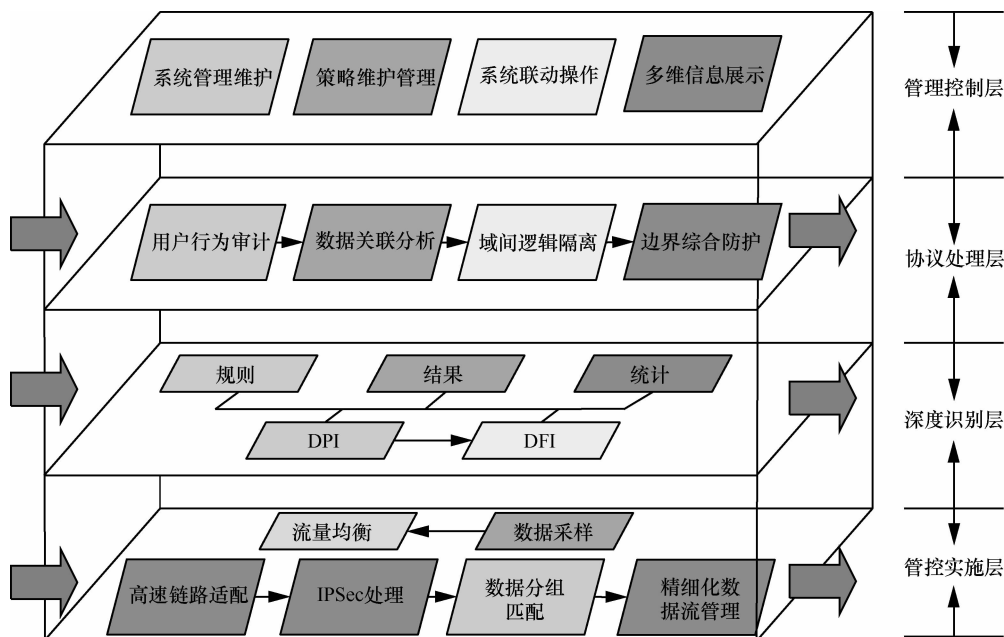


图4 接入网入侵检测系统的分层处理机制

行实时统计分析与认知,服务于业务识别和业务接入控制,安全威胁数据流级特征的发现与控制。此外,基于DFI技术,前端系统还可将可疑流量按“流”采集并传送给后端子系统。

(2)前端子系统光/电切换保护技术

光切换保护主要用于两路或多路光信号的备份切换,以在主光路通道出现故障时自动切换至备份通道,保证系统的正常不间断运行。光切换是物理层光通道切换,切换时间通常为毫秒级,切换过程造成分组丢失现象。与光切换相比,电切换可在链路层之上实现,其切换时间为纳秒级,切换过程可避免分组丢失,可有效避免传输和路由器的告警,用户无感。前端系统中需内置嵌入式自动监控系统,实时精确监控各路光信号输入功率,监控前端机物理层链路层解析、IP层/传输层报文头部分析、应用层解封装、特征提取、特征码匹配、结果综合处理、报文封装输出、在线管控等模块的工作状态,若发现某模块工作异常,可实时启动切换保护,确保无播出事故发生。

(3)后端子系统入侵检测技术

传统上,入侵检测技术是为保证计算机系统的安全而设计的一种能够及时发现并报告系统中未授权或异常现象的技术,广泛应用于互联网中。本系统的入侵检测与互联网中的入侵检测系统存在很大不同,一是输入待检测流量的大小不同,互联网入侵检测系统中,输入流量通常就是整个接入网流量,导致入侵检测系统检测速度常小于网

络传输速度,引发误报和漏报^[9],而本系统中入侵检测模块的输入流量远小于接入网流量,这主要是因为广电网中很多流量都是已知的合规视频节目流量,可不输入后端子系统入侵检测模块,减少了待检测流量,在同样入侵检测算法下能够更精确地检测入侵行为,降低误报和漏报。二是待检测流量的组成和特征不同,互联网包含海量应用信息,业务类型复杂且分布多样,相应的流量特征和行为特征各异,已有很多学者对其展开持续深入研究,很多研究成果已应用于互联网入侵检测系统中,形成比较稳定的异常检测模型和误用检测模型^[10];广电双向接入网链路中的混合流量成份与互联网流量组成有很大不同,其中既有广电运营商很多自有业务产生的流量成份原因,例如广播电视流量、VOD点播相关的控制信息和视频内容流量,远程医疗、远程教育等大量广电运营商自有业务产生的交互流量,还有很多广电运营商独特的运营交互信息原因,例如,大量机顶盒在约定的时间段会上传大量的数据记录信息给广电运营系统,以便分析收视率、点播率。本系统入侵检测模块综合运用模式匹配技术、协议分析和行为分析技术提高检测效率和准确性,其中模式匹配技术对已知安全威胁具有很好的检测效果;协议分析通过对数据分组进行结构化协议分析识别入侵行为;行为分析对采集数据进行关联分析,通过扩大被检测域,将基于单个时间点、单个攻击事件的实时检测转变为基于历史时间窗的检测来发现攻击,是发现未知特征安全威胁的一种有效方法^[11]。



3.3 广电接入网入侵检测实例系统——SunGnet703

SunGnet703 是广电接入网入侵检测的一种实例系统,是国家高技术研究发展计划(“863”计划)课题“高可信网络业务管控系统”直接技术突破的产业化成果^[12],包括前端子系统和后端分析子系统,前端子系统同样完成线速采集、线速检测与管控功能,后端子系统综合采集数据,对EOC终端及用户机顶盒上行IP分组的分析,实现互动业务的细致识别、分析与综合,为运营商提供互动节目点播率与直播节目收视率统计,用户开机率情况统计等服务,从而为高效运营提供有效的数据支撑。

图5是SunGnet703的系统外观和前端子系统硬件板卡,相比其他入侵检测方法,本系统具有4个技术特征。

- “非配合”的部署与工作方式。系统串联/并联在OLT上联链路后可独立运行,对已知安全流量进行实时转发,对已知特征的安全威胁进行实时阻断,对未知特征的可疑流量进行关联分析,判断其安全属性并进行相应处理,整个运行过程不需要普通用户和机顶盒等智能终端厂商的配合,也不需要运营商前端网络运营系统的配合。
- 运行的高可靠性。系统串联在OLT上联链路时,配备光/电切换保护模块,其内置的嵌入式自动监控系统可实时精确监控系统各模块工作状态,若发现工作异常,可实时启动切换保护,切换时间可达纳秒级,可做到用户无感,确保无播出事故发生。
- “隐形”功能确保系统自身安全。系统串联在OLT上联链路时,系统本身无外部可探测到的IP地址,类似于物理层的透明传输装置(类似一段光纤),因此具有天然的“隐形”特性,可免除攻击者对其进行探测,确保自身网络安全。
- 全维数据分析优势。系统可采集进出接入网的全维数据,包括运营信息、视听内容信息、控制信息、协议信息等,这比当前采用的定期采集机顶盒上传的用户收视记录信息更全面、更实时,相应地,系统可分析、展示给运营商的信息就更全面、更准确。



(a)外观



(b)硬件板卡

图5 SunGnet703的系统外观和前端子系统硬件板卡

4 结束语

在接入网边界部署IDS、IPS、UTM、防火墙等安全防护设备以确保内部网络安全已成为互联网安全防护的一种常态。广电网络中,机顶盒、电视机等终端智能化快速升级、加速发展,智能家居预期将变成现实。各种智能终端运行在Android等操作系统上,联通了双向通信通道,也就可以成为攻击者实施网络攻击的目标。终端智能化加速的同时带来终端安全漏洞的多样化,更严重的是,广电接入网边界目前还沿袭着单向业务传输网络时的做法,边界防护措施缺乏,这使得攻击者可无障碍地直达各个智能终端,控制终端进而渗透造成危害。在此情形下,本文提出了面向融合网络的广电接入网入侵检测系统,并实例化了该系统,具备了“非配合”工作方式、高可靠性、“隐形”确保自身安全、全维数据分析4个明显特点,预期可为广电接入网边界防护提供一种新的可行的安全防护方法和实际系统。

参考文献

- 1 王欣,陈德林,孙岳等.广电智能终端操作系统安全模型及实现.自动化与仪器仪表,2014(8):121~123
Wang X, Chen D L, Sun Y, *et al.* Radio intelligent terminal operating system security model and technology. Automation & Instrumentation, 2014(8):121~123
- 2 欧阳峰,朱里越,牛妍华等.面向下一代广播电视网的安全保障技术机制研究.网络新媒体技术,2012,1(4):6~9
Ouyang F, Zhu L Y, Niu Y H, *et al.* Security management architecture research next generation broadcasting. Network New Media, 2012,1(4):6~9
- 3 Viehbock S. Brute forcing Wi-Fi protected setup. http://www.coyotus.com/repo/pdf/hacking/viehboeck_wps.pdf, 2011
- 4 Cutlip Z. SQL injection to MIPS overflows: rooting SOHO routers. Proceedings in Black Hat, Vegas, USA, 2012
- 5 腾讯科技.广电总局发布首款电视操作系统TVOS1.0. <http://news.mydrivers.com/1/307/307478.htm>, 2014
Tencent Technology. Radio release operating system TVOS1.0. <http://news.mydrivers.com/1/307/307478.htm>, 2014
- 6 巫英坚,张恩阳,展华益.电视操作系统(TVOS)研发及产业化.网络新媒体技术,2012,1(1):1~3
Wu Y J, Zhang E Y, Zhan H Y. TV operating system(TVOS) R&D and industrialization. Journal of Network New Media, 2012,1(1):1~3
- 7 Security meets big data: RSA's new security analytics system. <http://www.emc.com/collateral/solution-overview/h13361-sb-rsa-sa-and-big-data.pdf>, 2015

8 Cascarano N, Ciminiera L, Risso F. Optimizing deep packet inspection for high-speed traffic analysis. *Journal of Network and Systems Management*, 2011, 19(1): 7~31

9 赵彬,王亚弟,李立新等. 利用关联和风险评估方法减少误报和漏报. *计算机应用研究*, 2008, 25(10):3105~3107

Zhao B, Wang Y D, Li L X, *et al.* Reducing false positive and false negative by correlation and risk assessment. *Application Research of Computers*, 2008, 25(10):3105~3107

10 张玲,白中英,罗守山等. 基于粗糙集和人工免疫的集成入侵检测模型. *通信学报*, 2013,34(9):166~176

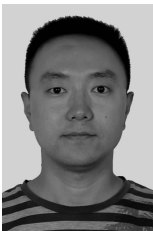
Zhang L, Bai Z Y, Luo S S, *et al.* Integrated intrusion detection model based on rough set and artificial immune. *Journal on Communications*, 2013, 34(9):166~176

11 Virvilis N, Gritzalis D. Trusted computing VS advanced persistent threats: can a defender win this game. *Proceedings of the 10th IEEE International Conference on Autonomous and Trusted Computing*, IEEE Press, Italy, 2013

12 SunGnet703. http://www.dltnet.com.cn/chanpinfuwu/SunGnet703_wangluoyichangliuliangjieyigongjifan/index.html, 2015



兰巨龙,男,博士,国家数字交换系统工程技术研究中心教授、总工程师,主要研究方向为高速宽带信息网络。



欧阳峰,男,国家新闻出版广电总局广播科学研究院高级工程师,主要研究方向为有线网络传输技术和网络安全技术。



张传浩,男,博士,国家数字交换系统工程技术研究中心信息与通信工程博士后流动站在站博士后,主要研究方向为融合网络信息安全。

[作者简介]



邱茜,女,博士,信息工程大学讲师,主要研究方向为网络安全模拟与评估等。



王艳红,女,大连梯耐德网络技术有限公司总经理,主要研究方向为广电网业务识别与分析。

2015149-7

2015 年 4 月通信业主要指标完成情况(二)

指标名称	单位	本月末到达	比上年末净增	本月净增
固定电话用户合计	万户	24 388.6	-554.4	-153.4
城市电话用户	万户	17 705.7	77.8	-169.6
农村电话用户	万户	6 682.9	-632.2	16.2
移动电话用户合计	万户	129 295.9	686.2	-101.2
其中:3G 用户	万户	46 630.3	-1 895.2	-959.8
4G 用户	万户	17 795.8	8 067.4	1 603.9
互联网宽带接入用户	万户	20 472.8	424.4	83.1
其中:xDSL 用户	万户	7 965.9	-972.7	-288.2
FTTH/O 用户	万户	8 196.3	1 364.8	357.3
移动互联网用户	万户	88 997.5	1 475.3	-986.0
固定电话普及率	部/百人	17.9		
移动电话普及率	部/百人	94.6		

(来源:工业和信息化部运行监测协调局)