



面向运营商移动网络的流量安全审计关键技术

薛立宏¹, 梁晓江²

(1. 中国电信股份有限公司上海研究院 上海 200122;

2. 中国电信股份有限公司湖北分公司 武汉 430023)

摘要: 基于现有运营商移动网络拓扑结构, 结合网络信息安全服务需求, 通过对海量数据相关汇聚分流、安全审计、用户关联分析等关键技术的研究, 提出面向运营商移动网络的流量安全审计总体技术架构, 并给出平台部署建议。

关键词: 网络流量; 安全审计; 汇聚分流

doi: 10.11959/j.issn.1000-0801.2015337

Key Technology About Security Audit of Mobile Network Traffic for Telecom Operator

Xue Lihong¹, Liang Xiaojiang²

(1. Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200122, China;

2. Hubei Branch of China Telecom Co., Ltd., Wuhan 430023, China)

Abstract: Based on the telecom operator mobile network topology, whereas the requirements of secure service for network information security, the key technologies such as convergence diversion, security audit, user association analysis, etc, were analyzed. The architecture of audit analysis platform was described, and some advice for the constructing of audit analysis service platform was given.

Key words: network traffic, security audit, convergence diversion

1 引言

近年来, 随着运营商在 LTE 建设方面投入的加大及 3G 网络的成熟, 移动互联网应用日趋普及。但由此带来的基于移动应用的网络信息安全形势也日益严峻, 智能终端成为新的攻击入口^[1], 移动网络信息安全已经成为各国关注的焦点, 不仅关系到用户的信息和资产安全, 也关系到国家安全和社会稳定, 已成为热门研究和技术发展的新领

域。针对移动网络的信息安全, 不仅需要在法律、管理、道德各方面采取切实可行的有效措施, 也迫切需要运营商采取相应的技术措施以确保移动通信网络建设与应用“又好又快”地健康有序发展。

随着移动互联网应用的信息安全进入高风险期, 运营商基于管道布局移动应用安全防护正当其时。根据工业和信息化部保[2012]247 号文要求, 对基础电信企业网络运营商制定了信息安全考核要求^[2], 其中移动通信网络的

收稿日期: 2015-11-18; 修回日期: 2015-12-15

论文引用格式: 薛立宏, 梁晓江. 面向运营商移动网络的流量安全审计关键技术. 电信科学, 2015337

Xue L H, Liang X J. Key technology about security audit of mobile network traffic for telecom operator. Telecommunications Science, 2015337



信息安全是保障要求之一。面向运营商移动网络的流量安全审计,目标就是加强和规范移动互联网安全技术防范工作,保障网络安全和信息安全,促进移动互联网健康、有序发展,维护国家安全、社会秩序和公共利益。

基于通信网络流量的安全审计^[3](audit)是指按照一定的安全策略,利用记录系统活动和用户活动等信息,检查、审查和检验操作事件的环境及活动,从而发现系统漏洞、入侵行为或改善系统性能的过程,也是审查评估系统安全风险并采取相应措施的一个过程。在不至于混淆的情况下,简称为安全审计,实际是记录与审查用户操作通信终端及网络系统活动的过程,是提高系统安全性的重要举措。系统活动包括操作系统活动和应用程序进程的活动。用户活动包括用户在操作系统和应用程序中的活动,如用户所使用的资源、使用时间、执行的操作等。

本文基于现有运营商网络拓扑结构,结合网络信息安全服务需求,通过对大数据流量相关汇聚分流、安全审计、用户关联分析等关键技术的研究,提出面向通信网络中大数据网络流量的实时监测分析技术架构,提升运营商对大数据网络流量的信息安全审计分析能力。

2 移动网络流量安全审计技术现状

2.1 流量安全审计服务需求

基于通信网络流量的安全审计是网络安全领域里的新型产品形态,平台是针对网络中最不稳定的因素——人以及人与网络发生的一系列内容交互行为——进行技术上的安全防范和应对的。然而人是个性化的,并且会不断变化,其与网络的交互方式和交互内容也会不断改变,这也决定了审计分析系统的技术设计要与时俱进、因需而变。目前,基于运营商通信网络的流量安全审计系统主要服务于运营商自身和行业用户。

(1) 运营商的网络信息安全审计需求

- 相关互联网产业基地的安全运营合规需求;
- 用户上网行为分析及内容安全审计;
- 峰值流量预测与异常流量的拦截。

(2) 行业用户的信息安全审计需求

- 新型移动应用的内容深度分析与安全审计;
- 异常移动应用网络行为识别、实时跟踪;
- 海量用户的上网日志留存,安全追溯。

2.2 流量安全审计分析技术现状

基于运营商承载网络或骨干链路中的数据流量进行

安全审计分析,审计平台的性能将直接影响到运营系统的整体性能。随着用户规模的扩大,最终客户对审计分析系统的性能提出了更高的要求,这意味着相关产品的性能必然要“精益求精”、“与时俱进”。

- 审计分析设备性能方面的重要指标是“捕获分组能力”,主要体现在大流量、高并发这两方面,具体包括吞吐量、并发连接数、新建连接数等指标。吞吐量越大,需要审计分析设备的捕获数据的能力越强;并发连接数越大,单位时间内保持的连接数越高,设备可管理的用户数量越多;新建连接数越大,单位时间内新增连接数越多,设备对网络突发流量的处理能力越强。
- 审计分析类产品的技术核心是其数据分析能力。数据分析能力是所能识别的协议、应用种类,也包括正则表达式规则的精确性,其分析能力会导致审计结果日志存储完整性、保存的时间长短、查询速度的快慢、查询的精确性、模糊性等问题。

基于运营商承载网络或骨干链路中的数据流量,采用 DPI/DFI 技术进行流量分析及安全审计,可以有效发现移动应用的安全问题,发现并报告当前网络流量中的异常情况。目前,基于运营商管道异构网络中的混合流量的安全审计技术存在以下几方面的问题。

- 运营商骨干网普遍采用多条 10GE 光纤进行数据传输,现有基于 Intel 架构的多核处理器对 IP 报文的处理能力有限,其极限在 5 Gbit/s 左右,大流量数据的实时分析性难以得到保障。
- 由于运营商数据链路骨干网的负载均衡和路由不对称等原因,同一个会话的多个报文可能被负载均衡到多条链路上,现有审计平台架构采用直接汇接分光方式,难以实现对异构网络中大数据流量的实时分离和监测。
- 在网络流量安全审计过程中,不同应用所需审计的复杂度和报文处理层级也不同。采用传统流量均衡分流的方式难以提升系统的整体性能。
- 当运营商网络中发现异常流量时,现有的审计分析平台由于性能原因对短字节报文进行了分组丢失处理,难以实现对异常网络流量进行细粒度的精确定位、反向追踪分析。

因此,本文通过对海量数据相关汇聚分流、安全审计、用户关联分析等关键技术的研究入手,提出面向运营商移动网

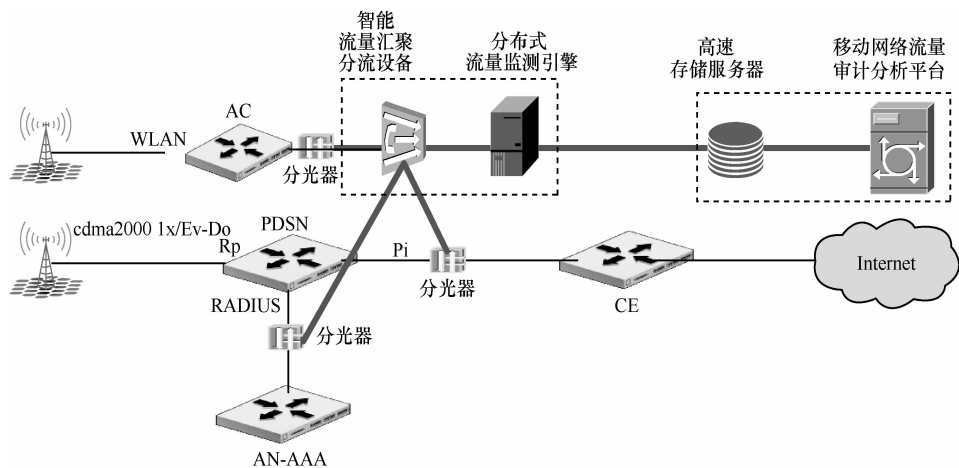


图 1 汇聚分流组网

络的流量安全审计总体技术架构,并给出平台部署建议。

3 移动网络流量安全审计关键技术分析

3.1 大数据汇聚分流技术

目前运营商网普遍采用混合组网方式,即 Rp、Pi、RADIUS 接口中上/下行流量混合在同一对 10GE 光纤上,现有组网方式存在的主要问题如下:

- 由于现有技术架构和平台能力没有对重要低速流量与普通高速流量进行分离,导致同时监测时容易丢失报文;
- 没有对异构网络(3G、WLAN、LTE)中的流量进行标识,关联分析困难;
- 难以实现异常网络流量的细粒度精确定位、反向追踪分析。

考虑到上述问题,在原有的流量审计系统中设计了智能流量汇聚分流设备,如图 1 所示。

该设备的逻辑框架如图 2 所示。

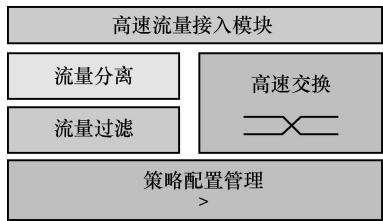


图 2 汇聚分流设备功能框架

相对传统审计系统,引入该设备后,可以实现以下功能:

- Pi、Rp、RADIUS 流量分离,上、下行流量分离;
- Ev-Do/cdma2000 1x/WLAN/LTE 10GE 光流量接入,实现异构网络的流量标识与分离;

- 多端口流量汇聚,出、入端动态配置,实现重要低速流量(如 RADIUS 报文)与普通高速流量(业务报文)的分离;
- 基于端口、五元组、二层以太网协议流量过滤压缩功能;
- 接收审计平台安全策略,实现细粒度的流量实时跟踪监测。

3.2 DPI/DFI 联合细粒度审计分析

如图 3 所示,普通的报文识别技术只能识别 IP 报文五元组(源地址、目的地址、源端口、目的端口以及协议类型)及以下层级报文的内容。

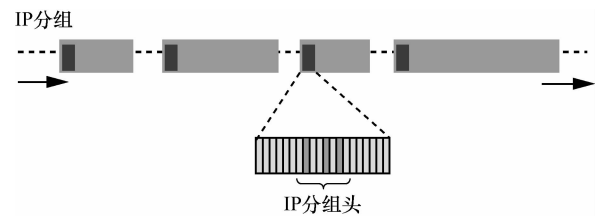


图 3 普通的报文识别技术

而 DPI(deep packet inspection,深度数据分组检测),不仅分析 IP 分组头的五元组,而且还增加了应用层分析,识别各种应用及其内容,如图 4 所示。

DFI(deep/dynamic flow inspection,深度/动态数据流检测)技术采用的是一种基于流量行为的应用识别技术,通过分析会话连接流的分组长、连接速率、传输字节量、分

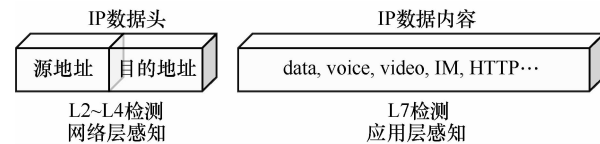


图 4 DPI 技术



组与分组之间的间隔等信息来与流量模型对比,从而实现鉴别应用类型。

鉴于 DPI 在应用区分、识别精度、功能扩展等方面优势明显,而 DFI 在对新应用和加密协议的识别方面有一定的优势,建议采用以 DPI 分析技术为主,传统普通报文分析和 DFI 技术来处理分析加密应用协议为辅的方式综合分析数据分组、应用层特征值和应用协议行为,UDP/TCP 端口、端口范围和端口列表,IP 地址、地址范围、子网或主机列表,MPLS 标签、IP precedence、MPLS EXP,传输方向等。以此来达到精确分析应用和协议的目的,如图 5 所示。

3.3 用户关联分析

基于运营商网络中认证流量与业务流量的关联分析,可以识别用户,实现面向用户的智能关联分析,通过组合多种分析方法,可以更加准确地分析用户的动态行为特征。

如对于 3G 系统,首先基于 AAA 系统接口上的 RADIUS 流量建立认证流,提取 IP 地址、IMSI、MSISDN 的对应关系,同时基于高速流量接入模块采集 Pi 口上业务流量建立会话流。对上述流量进行关联合并分析,得到以用户手机号码为中心的行为分析和内容审核结果。以下是现有 3G 系统中 AAA 服务器的 RADIUS 消息核心字段示例:

- 消息中用户标识字段包括 calling-station-ID 和 served-MDN,分别是手机用户的 IMSI 号码和用户手机号码;
- 消息中 acct-status-type 字段标识了用户认证的类别,包括用户上线(accounting-start)和用户下线(accounting-stop);
- 消息中 framed-IP-address 字段标识了用户的终端 IP 地址;

- 消息中 3GPP2-BSID 字段标识了用户所在的基站小区信息,该字段是 16 进制字符串,其中前 4 个字节是 system ID,第 5~8 个字节是 network ID,第 9~12 个字节是 cell 标识;其中 cell 标识中高 12 位是 cell ID,低 4 位是扇区。

3.4 安全处置策略

(1)实时异常行为处置策略

系统定制各种用户异常行为处置策略,可以定制审计对象、审计时间、审计内容,制定审计策略,例如仅审计用户邮件的收发。基于运营商网络的流量安全审计系统可以实现从精准研判到快速阻断的过程,从事前预警到事后告警,形成了闭环的全方位防控体系,如图 6 所示。

(2)细粒度的免监控策略

- 提供可信证书、证书链,区分可信的 HTTPS 网络(如网络银行、网络支付等),防范网络盗链与钓鱼网站;
- 可信 IP 地址、免监控 key,防范总裁、高层领导网络访问行为,财务部收发的邮件等关乎组织机密信息的审计与泄露;
- 可信 QQ、MSN、飞信等策略,提供部分人员可以使用 QQ 对外联系业务,应用层高级用户的可信提供了比可信 IP 地址、免监控 key 更细粒度的风险防范;
- 邮件收发账号免监控,保护总裁、高层领导的邮件收发内容的审计,应用层高级用户的可信提供了比可信 IP 地址、免监控 key 更细粒度的风险防范。

(3)基于应用、用户、时间段的策略组合

基于应用对象、用户对象、时间对象、运营单位自定义对象等,通过应用控制策略、流量控制策略、内容审计等方式,最大限度地满足各层面客户在用户行为分析、内容审计、实时告警等方面的不同需求。

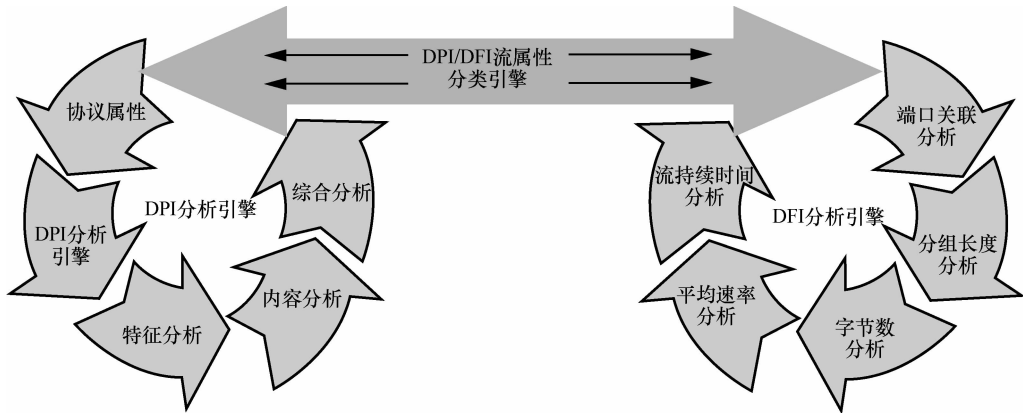


图 5 DPI/DFI 联合分析框架

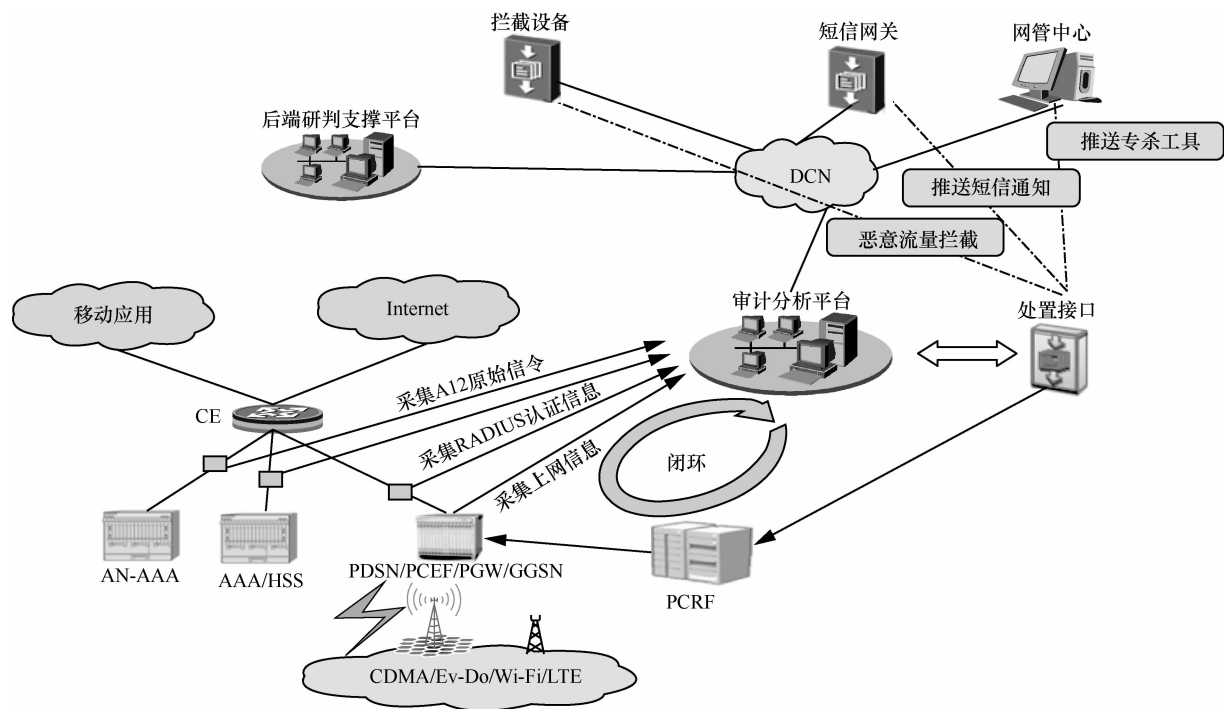


图 6 实时异常行为处置示意

4 移动网络流量安全审计系统总体架构及部署策略

面向运营商移动网络的流量安全审计系统主要由系统层、数据采集层、审计分析层、可视化门户平台等部分组成,如图 7 所示。

- 系统层是基于定制安全 Linux OS 内核, 构建一个统一、高效、安全的运行环境。
- 数据采集层包括高速流量数据采集、会话重组、高

速备份缓存等功能。

- 审计分析层包括 3 个子系统:移动应用行为审计分析系统、移动应用内容审计分析系统、移动应用综合审计服务系统。
- 可视化门户平台基于 Web 架构, 为系统管理和维护人员提供统一的管理界面。

面向运营商网络的流量安全审计系统可以采用多种方式灵活部署,通过分析处理流入和流出的数据分组,有效地实现对运营商通信网络数据的各应用场景的审计分析。

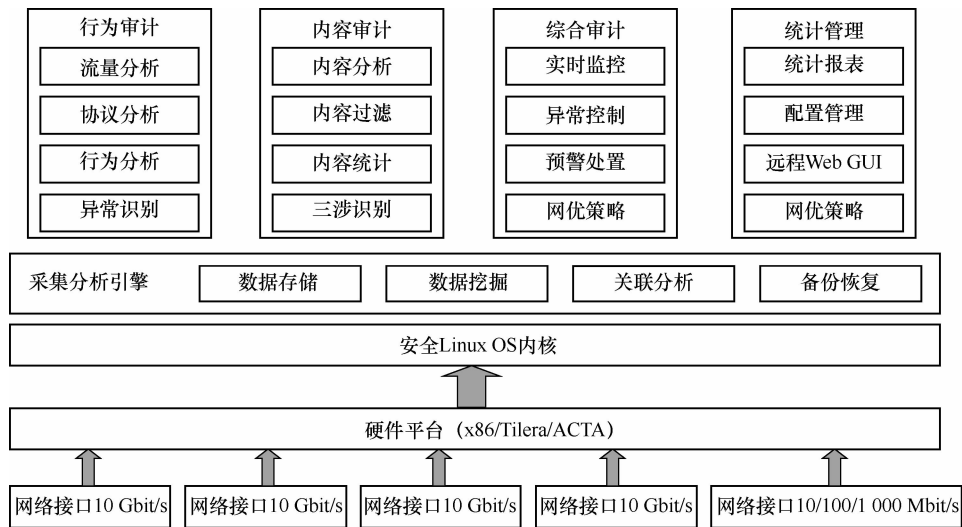


图 7 系统功能架构



4.1 分离式审计平台部署

分离式审计平台系统部署建议如图8所示。

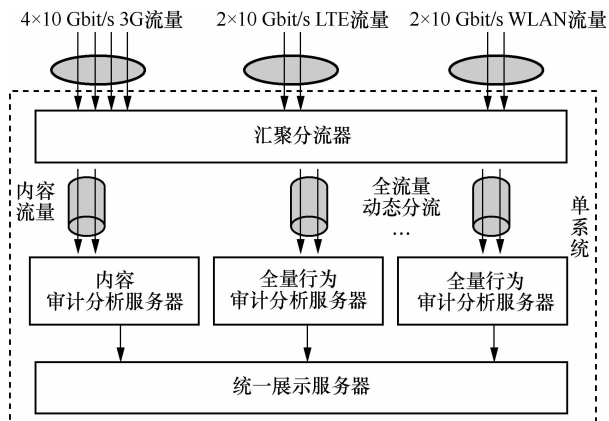


图8 分离式审计平台系统

分离式审计平台系统中,汇聚分流设备、审计分析平台、统一展示服务器均为独立的服务器,技术特点如下。

- 各类服务器可采用集群方式提高整体性能。如汇聚分流器在应对大流量系统时,可采用二级分流方式对流量进行分类;单系统处理能力达10 Gbit/s,采用集群技术扩展后,处理能力可达100 Gbit/s以上。
- 审计服务器可以按照场景进行功能灵活配置。流量通过汇聚分流器后,可按照不同业务流量的审计分析要求,分为内容审计分析服务器、全量行为审计服务器等。

4.2 集成式平台部署

集成式审计平台系统部署建议如图9所示。

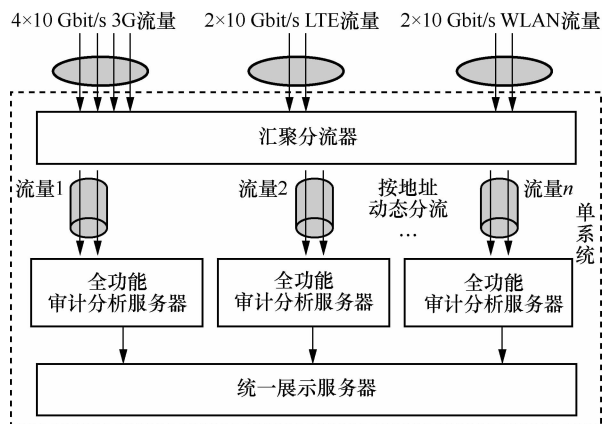


图9 集成式审计平台系统

集成式审计平台系统中,汇聚分流设备、审计分析平台、统一展示服务器采用刀片式服务器,通过统一的物理总线进行相互通信。其技术特点如下。

- 集成度高、成本低。各类服务器采用刀片式服务器,根据现有总线吞吐量,负责进行审计分析的刀片式板卡最高达5块,单台处理能力达50 Gbit/s。
- 流量按IP地址域动态均衡。网络流量按地址域动态分流,平均分配到各审计服务板卡。
- 流量采用全量处理。每块刀片式服务器板卡均具备全量处理能力,即均可以实现行为分析、内容审计等功能。

5 结束语

综上所述,面向运营商移动网络的流量安全审计系统既要考虑实际运营的需要,又要考虑相关行业用户政府的需求,同时还要满足国际、国内的安全标准,从整体上考虑其技术实现架构。在审计分析平台投入运营之后,还需要不断对行业标准、关键技术、运营接口等方面持续进行优化,从而更好地提升审计分析平台性能、丰富产品功能。

参考文献

- 1 CNCERT. 2014年我国互联网网络安全态势报告, 2015
CNCERT. Overview of Internet Security Situation in China in 2014, 2015
- 2 中国电信集团公司. 中国电信安全技术发展白皮书(2014年版), 2015
China Telecom Corporation. China Telecom Security Technology White Paper(2014), 2015
- 3 张秀英, 王铮. 一种基于流量识别技术的网络信息审计模型. 微处理机, 2010(1): 41~44
Zhang X Y, Wang Z. A network information audit model based on traffic recognition technology. Microprocessors, 2010(1): 41~44

[作者简介]



薛立宏,男,中国电信股份有限公司上海研究院高级工程师,主要研究方向为移动互联网、网络信息安全。



梁晓江,男,中国电信股份有限公司湖北分公司网络运行维护部高级业务主管,主要研究方向为互联网及大数据网络。