



电话诈骗防治技术解决方案与 运维对策研究

李力卡¹, 马泽雄¹, 陈庆年², 李程¹

(1. 中国电信股份有限公司广东研究院 广州 510630;

2. 中国电信股份有限公司广东分公司 广州 510081)

摘要:当前利用电话实施诈骗案高发,给人民群众财产造成巨大损失。通过对问题根源分析,探讨电话诈骗机制、行为特征,研究网络安全模型与防治体系,提出核心网号码保护能力提升建议,研究出一套基于信令大数据的预警拦截技术系统模型并通过现网效果验证,最后给出了相应的关键运维管理对策。

关键词:电话诈骗;防治;预警;拦截;对策

doi: 10.3969/j.issn.1000-0801.2014.11.028

Research of Technology Solutions and Operation Countermeasures to Telephone Fraud Prevention and Control

Li Lika¹, Ma Zexiong¹, Chen Qingnian², Li Cheng¹

(1. Guangdong Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China;

2. Guangdong Branch of China Telecom Co., Ltd., Guangzhou 510081, China)

Abstract: Currently the incidence of using telephone for fraud is growing up to a new high level, cause huge losses to the people property. According to the root cause analysis, telephone fraud mechanism and behavior characteristics were discussed, network security model and the control system were researched, the recommending of core network number protection ability to ascend was proposed, and a set of early warning and intercept technology system based on big data model of signaling was developed. The real network testing and effect, as well as the key operations management countermeasures were presented.

Key words: telephone fraud, prevention and control, early warning, intercept, countermeasure

1 引言

近年来,利用信息手段进行诈骗的案件层出不穷,犯罪分子电话冒充公检法、电信、邮政快递、银行等服务人员行骗,给人民群众造成巨大的经济损失,影响社会安定和公信力。而电话诈骗问题复杂,属于业界难题,本文从电话诈骗的机制深入分析,并提出了科学合理的系统性解决方案与运营对策。

2 问题根源

通信诈骗具有集团化、专业化、高科技、跨区域的特点,内容翻新快,蔓延迅速。作案采用科技手段,号码多变,位置隐蔽,跨境犯罪突出且大案要案频发。

现阶段通信网络全球化,越来越庞大,业务更加开放,通信手段更加丰富,同时VoIP技术、IT平台技术、移动互联网技术兴起,为诈骗电话突破常规通信监管提供了技术

条件。基于利益驱使,一是有些高科技公司提供廉价非法终端或技术手段,如 VoIP 呼叫平台、群呼器、短信群发器、伪基站等,为犯罪提供技术条件;二是某些境外中间运营商或境内服务提供商、外呼中心平台违规操作,提供非法呼叫的大网接入或中转,获得改号或接入的高额收益,成为诈骗利益链条中的一环。

电话诈骗猖獗,其原因主要有:作案成本低而非法收益巨大,民众防范意识薄弱,相关法制不健全,立法滞后,电信、银行存在监管不够严密,电信诈骗犯罪全球化产业链已经形成等。

3 通信诈骗形成机制与特征

目前,诈骗电话界定没有一致的技术标准,执法部门也无法明确案发前可清晰辨识诈骗呼叫的特征。一般从诈骗手法来分,高科技通信诈骗主要有以下几种。

- 点对点诈骗:个人随机拨打号码以借钱行骗,如“猜猜我是谁”一类,一般用手机号码“漫天撒网”,也有仿冒号码“精确下套”。
- 自动群呼诈骗:通过平台群呼,播放钓鱼通知音,以各种理由将被叫引诱至人工座席实施诈骗,危害最大,受害者甚至倾家荡产,主叫号码多属于伪造以骗取信任,被叫有按键转接行为。
- “一声响”诈骗:通过平台群呼响铃一声,引诱被叫回电行骗,犯罪分子多提供呼叫中心号码呼转至手机行骗。
- 短信诈骗:群发钓鱼诈骗短信(含银行账号、诈骗号码或钓鱼网站),引诱被叫上钓鱼网站或回电行骗。

可见,常见的主要是虚假主叫诈骗方式,指通过伪造或仿冒主叫号码诈骗。犯罪分子通过网络改号平台进行号码转换功能,能在对方终端上显示任意号码。改号平台可以置于国外或国内,位于国外的,改号后通过国际运营商及国际接口局进入;位于国内的,通过 VoIP 接入座席,租用某些不具有鉴权能力的中继落地。目前改号主要有两种形成方式。

- 联网登录方式:由用户登录改号平台后进行相关设置才可使用,一般主要用于联网的 PC 上。
- 电话拨打方式:由用户拨打改号平台提供的接入码,通过平台回拨后进行二次拨号后使用。

以电话拨打方式为例,图 1 所示为采用电话拨打方式的改号功能实现方法。此方式典型改号流程如下。

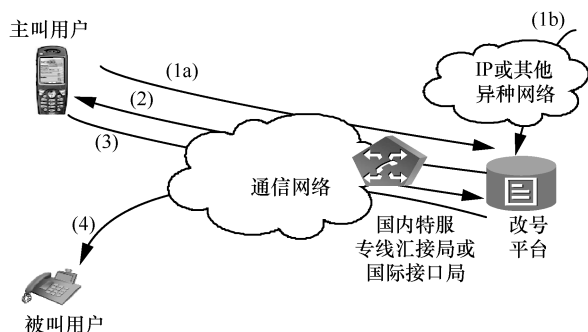


图 1 虚假主叫号码产生原理示意

(1)主叫通过手机(见图 1 中(1a))或互联网 VoIP 软终端或网页(见图 1 中(1b))呼入改号平台,听到平台回铃后由平台自动挂断呼叫。

(2)平台通过电话网络发起到主叫用户的呼叫。

(3)主叫用户接起后可按照语音提示输入二次拨号信息(如#账号#密码#显示号码#被叫号码),也可在系统预置。

(4)改号平台根据用户输入/设置的被叫号码,通过运营商网络接续被叫,向被叫改送主叫用户输入/设置的显示号码。

另一类危害极大主要诈骗方式是引诱被叫按键转接座席,犯罪分子冒充公检法诈骗。按键转接类(或回拨)诈骗电话原理:

(1)诈骗平台群发钓鱼录音呼叫,多显示国际号码、高仿号码(如 0010000,显示为+10000);

(2)被叫通话后,依照提示按键转接人工座席;

(3)诈骗平台将该通话接入人工座席,一般套取基本身份资料,然后由二、三线诈骗分子进行角色扮演,如公检法,转以点对点方式实施连环计(如涉黑洗钱)。

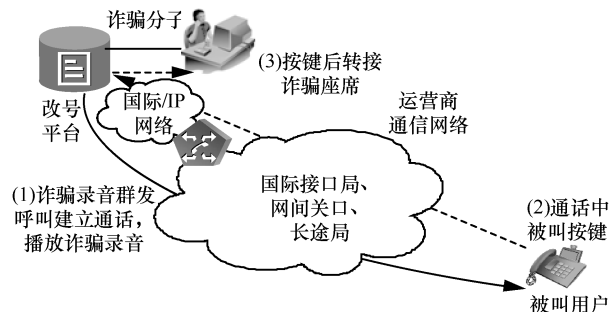


图 2 按键转接/回拨类诈骗原理

从诈骗呼叫的主叫号码观察,主要有以下几个突出的行为特征。

(1) 号码不规范或明显仿冒

多采用国际号码、过短号码或高仿号码,是无法直接



回拨的,如0010652043330 仿冒公安部经济犯罪举报中心01065204333,00xxx110 仿冒某地报警电话110,0095588 仿冒工商银行服务号码95588;或采用完全一致的号码用于点对点诈骗,如仿冒某地公安办公电话。

(2)来话源隐蔽

诈骗呼叫来话源隐蔽,路由不确定,据公安部门统计目前境外改号网络电话进入中国大陆的渠道主要有3个:一是通过3个运营商的国际接口局落地进入交换网;二是各地电信业务承包企业违法经营VoIP网络电话,将境外改号诈骗电话落地对接进入电话网,如“3·10”专案截获的84万条诈骗VoIP网络电话是经某地运营商电话网络对接落地的;三是境外改号电话经香港电话公司非法落地后转接入内地电话网,如“10·11”专案的2100万条诈骗电话被改号为境内公检法机关号码,是从铁通香港公司转接的。

(3)恶意呼叫

诈骗呼叫具有高频次、时间长的恶意呼叫特征。

(4)被叫覆盖面大

呼叫具有扫描轮询特征,被叫号码重复性极小,被叫号段短时间内相对集中,按号段连号或跳号。

(5)具有游牧特性或驻留性

诈骗号码呼叫目的地多具有游牧特性,一般在一个区域呼叫一段时间后将目标转移到下一个区号;但也有针对性强的,仿冒本地区号高价值号码,长期定向呼叫某地,如0020110、002011185。

(6)接通率低,通话时长异常

诈骗呼叫接通率低,空号率高,通话时长偏短(20~30 s),有部分受害者,其通话时间可长达1~2 h。

(7)号码具有随机可变性

一旦某个号码被拦截,诈骗分子可很快变换新号码,突破电信网静态防御能力。如在某地对0075710000实施网络拦截后,一周后诈骗分子改用00175710000发呼。

由此可见,诈骗电话防治属于业界难题,灵活号码变换能力与路由方式突破了电信网络现有能力。

4 信息安全模型与防治体系研究

为了提升电话网信息安全防治能力,需要结合新形势建立相适应的网络安全模型,以指导诈骗电话的防范。

APPDRR信息安全模型是业界常用而成熟的信息安全模型。APPDRR认为信息安全由风险评估(assessment)、安全策略(policy)、防护(protection)、检测(detection)、响应

(response)和恢复(restoration)6部分完成。其首先通过风险评估,掌握网络信息安全面临的风险信息;其次网络信息安全策略将因应风险评估的结果和安全需求的变化而制定,具有原则性的指导地位,其后的检测、响应诸环节都应在安全策略的基础上展开;防护则体现了网络静态保护能力;检测、响应、恢复3个环节,体现了从发现到恢复的动态过程。

APPDRR信息安全模型如图3所示。

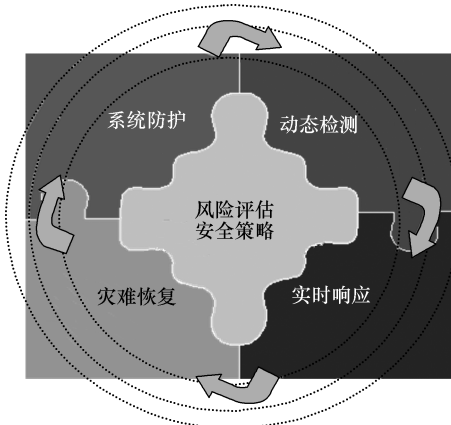


图3 APPDRR信息安全模型

APPDRR信息安全模型表明了网络安全的相对性和动态螺旋上升的过程,通过6环节的循环流动,网络信息安全逐渐地得以完善和提高,从而实现最终安全目标。

依据APPDRR信息安全模型,本文首次研究提出相应电话网信息安全的解决思路或系统性方案。APPDRR对应于电话核心网信息安全,相应6步为风险评估、安全策略、网络防护、动态检测、及时响应、封堵拦截,构成一个完整安全体系并能根据情况不断调整优化。

核心网信息安全的APPDRR模型如图4所示。

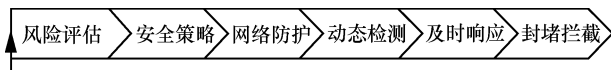


图4 核心网信息安全的APPDRR模型

5 核心网号码防护能力提升建议

根据以上安全模型,基于网络中存在诈骗呼叫的风险点的评估分析后,相关局点的安全策略、实施的防护功能建议如下。

(1) 国际、长途、网间局点:目前国内运营商已按工业和信息化部要求实施了主叫号码传送规范,确保号码如实传递,不能被修改,但仍需要加强非法号码的监控。

- 国际长途号码传送规范:对于没有主叫透传要求的国际来话,统一按要求变换为 00019x+国际字冠+接入点区号+国际局序号;对于国际 IP 电话,主叫规范为 00179xx;对于要求透传的国际来话方向,确认符合国际号码传递规则,拒绝 0086 字头号码,同时针对超短、超长号码监控。
- 长途传送规范:在长途字冠规范基础上,对异地发出本地区号话务进行分析。
- 网间传送规范:对于网间号码传递规范后的超长、超短号码进行拦截。

(2)特服专汇局:针对用户租赁中继,进行主叫号码绑定、鉴权或呼入呼出限制,但由于部分老旧机型对主叫鉴权、黑名单等功能不支持或不完善,还存在需要采用其他监控手段弥补。

(3)汇接局:需要增强中继主叫鉴权与黑名单能力。

(4)呼叫中心:对主叫号码的鉴权和规范,需要排除由于座席转包产生的非法话务。

(5)短信网关/短信中心:基于垃圾短信拦截平台,支持更多诈骗相关的关键词、非法号码拦截。

以上新功能可能需要对网络部分功能、信令监测系统的升级支持。

但也应该看到,以上方法虽能在源头起到较好接入控制作用,做到转接过程中的号码规范性,但对于盗用他省号码或来自境外局点的诈骗呼叫这类风险,由于号码完全合法却能轻易突破网络防护,网络静态安全策略和防护能力是远远不足的,难以有效遏制这些诈骗呼叫。

因此,引入动态检测、多重封堵拦截能力是十分必要的,但若要有网络支持这两点,首先电信设备技术规范需要补充修订新的功能(如接入点信息的全程携带与鉴权),其次全网设备改造面广、投资成本高、周期长,不可能全球网络都解决,而且很可能跟不上诈骗手法的更新换代。因此,需要借他山之石来解决这些深层次风险问题。

6 防通信诈骗预警拦截系统试验

由于网络静态防护能力的局限性,需要结合外部系统能力形成新的目标解决方案。本文创新性地提出了基于信令大数据的防诈骗预警关键技术及网络拦截技术相结合的解决方案。

境外诈骗号码预警拦截系统是基于实时信令 TDR 实时订阅技术、大数据智能分析技术的随机伪号甄别功能、

信令关联溯源技术等关键技术,结合网络的黑名单拦截技术,由信令系统+业务平台+网络能力构成的综合系统,提供了对诈骗呼叫的动态检测、及时响应、封堵拦截一整套高效解决方案。

境外诈骗号码预警拦截系统模型如图 5 所示。

境外诈骗号码预警拦截系统技术实现原理如下。

- 在全网汇接局侧监测来话局到汇接局的信令消息,提取境外主叫呼叫事件的起呼信息后送订阅服务器,进行格式适配、呼叫去重、清洗以及号码规范,进行信令大数据的挖掘分析。
- 诈骗预警分析服务器采用大数据智能分析技术,可基于云架构部署,建立一套防诈骗分析经验模型,设置好诈骗特征参数模板,如主叫号码、相对频次、接通率、被叫关系或分布、路由方向等多项特征,辨析恶意呼叫,实现动态检测,周期性或指定时段输出涉嫌诈骗名单(灰名单)TopN 告警。
- 应用服务器支持灰名单的统计报告而后转为黑名单、黑名单跟踪、呼叫记录回溯、拦截状态设置以及闪信告警。呼叫回溯可以获取呼叫上一跳的信息。
- 当执法部门查证确认要拦截的黑名单后,提交运营商采用网络或拦截平台方式,实施黑名单全拦截或部分拦截,也可以转接到语音交互平台进行通知或话路屏蔽。

该系统经过现网 800 Gbit/s 信令数据的训练优化经验模型后,在某地固网在线进行 24 h 的运行验证,得到国际可疑诈骗号码的呼叫统计情况如图 6 所示。从图中可以看出,系统所分析出来的诈骗号码一半以上曾遭到网络举报诈骗且系统能发现未曾被网络举报的新恶意号码。

系统经近两个月对某地进行境外诈骗电话预警分析,所发现的情况分析如下。

(1)主动预警有效涉嫌诈骗的灰名单号码 377 个,其中最多的主叫为 001 开头(如高仿 11x、12x 特服、手机号码),占涉嫌诈骗呼叫 59.7%,其中呼叫量最高的一个恶意诈骗号码呼叫 33 850 次。

(2)按照号码呼叫频次来统计,呼叫次数超过 1 000 次的典型诈骗号码见表 1。

(3)按照号码成分分析,以高仿手机、银行、公安、邮政及公众特服号码等居多。高频诈骗号码成分分析见表 2。

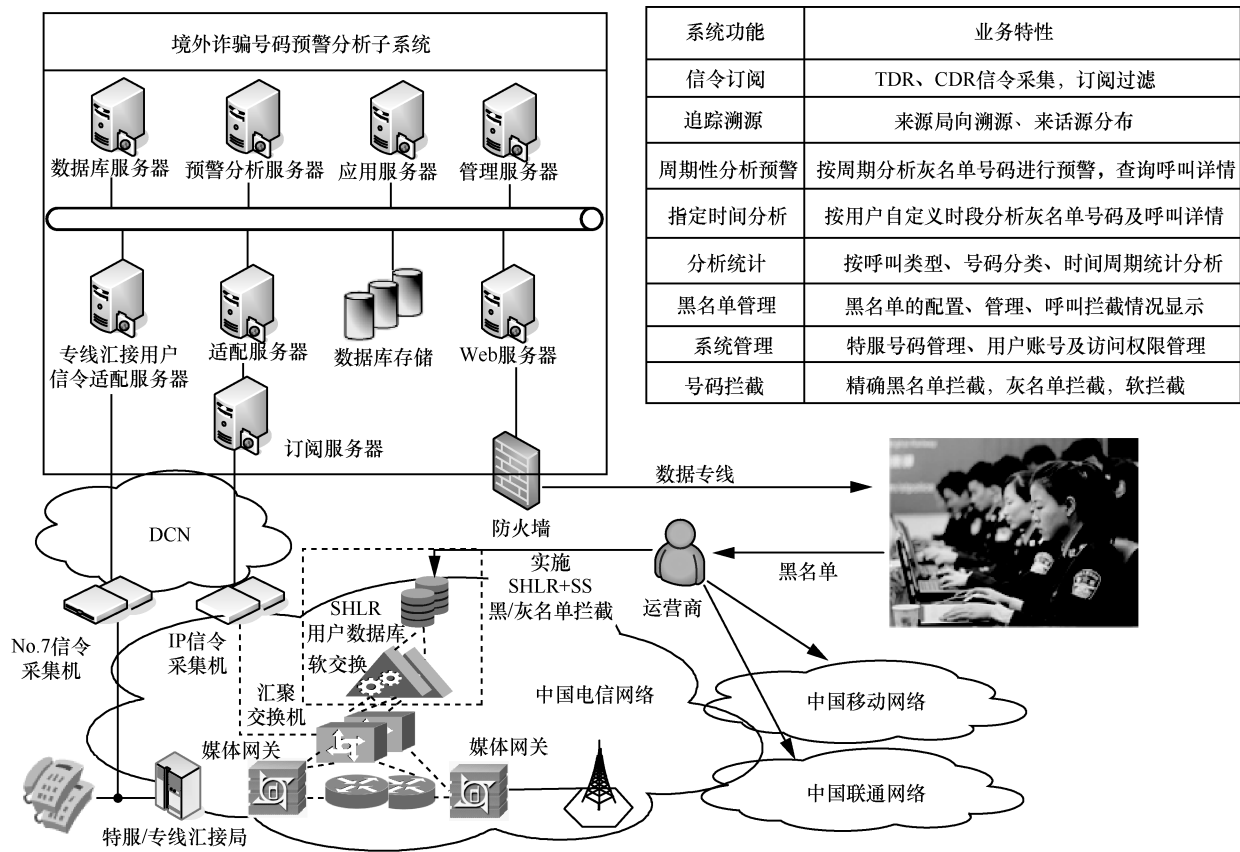


图5 境外诈骗号码预警拦截系统模型示意

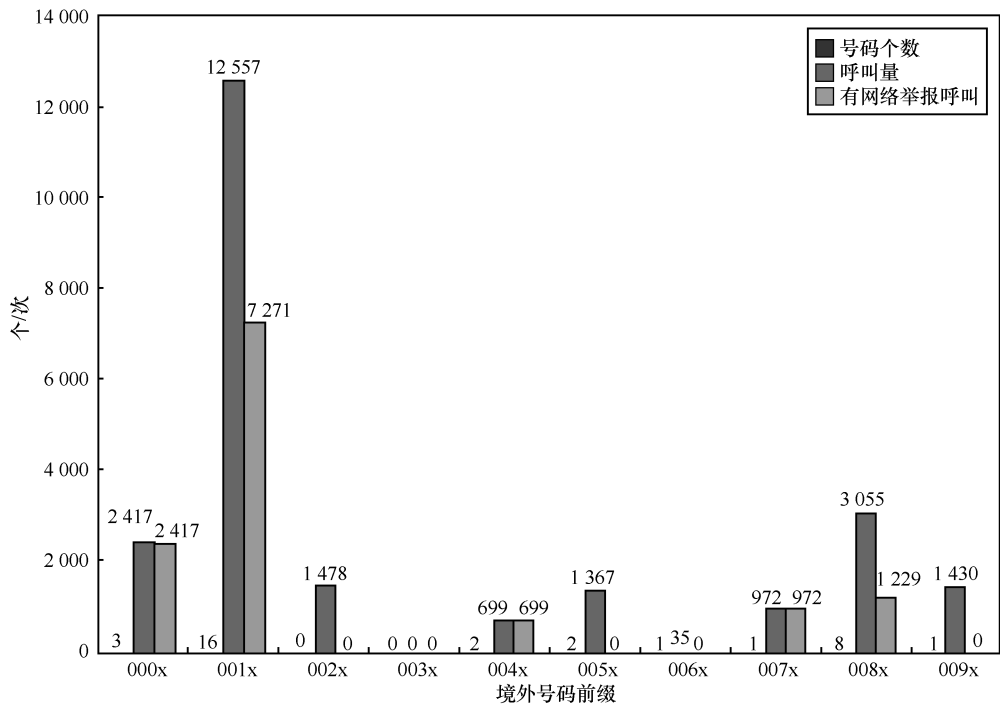


图6 某地固网某24h国际恶意号码情况统计分析

表 1 高频诈骗号码

主叫号码	呼叫次数	所占比例	备注
0014678741403	33 850	46.57%	美、加号码,仿手机号码(电话欠费诈骗)
00757110	5 987	8.24%	高仿佛山(0757)110
0095588	5 608	7.72%	高仿工商银行 95588
002011185	3 926	5.40%	高仿广州 EMS11185
001100	3 202	4.41%	高仿 110
0018185235214	1 291	1.78%	美、加号码,高仿手机号码
001200	1 280	1.76%	高仿急救 120
0020140217	1 199	1.65%	不存在的号码
0075800	1 129	1.55%	俄罗斯号码(包裹投递诈骗)
其他号码	15 207	20.92%	

表 2 高频诈骗号码成分分析

主叫号码成分	典型号码	呼叫次数
仿银行特服号码	0095588	5 608
仿公安部门号码	00757110、0022110、001100	9 845
仿邮政号码	0011185、002011185	4 582
仿其他公众号码	0018610000、0012333、001200	2 086
仿国内手机号码	0014678741403	33 850

(4)以呼叫次数超过 1200 次的号码为例分析来源分布,有的呼叫源在国外,有的在境内,有的两者皆有。高频诈骗号码来话源分析见表 3。

表 3 高频诈骗号码来话源分析

主叫号码	路由来源	备注(来源)
0014678741403	国际长途 100%	国际
00757110	省际长途 100%	国内
0095588	国际长途 100%	国际
002011185	省际长途 99.91%、关口局 0.09%	国内
001100	省际长途 60%、关口局 20%、省内长途 10%、国际长途 10%	国内、国际
0018185235214	关口局 100%	国内其他运营商
001200	省际长途 50%、国际长途 20%、省内长途 18%、关口局 12%	国内、国际

可见,该系统试验情况表明,基于信令大数据的分析方法是可行的且高效的,对诈骗电话行为的动态检测分析准确率高,极大弥补了网络自身能力的不足,能实现诈骗号码大范围、主动捕捉,为精确封堵拦截提供了基础条件。后经选择部分主要诈骗号码进行固网黑名单拦截后,当地诈骗案发率下降 64%,成效显著。该方法网络适用性强,系

统建造成本较低,推广应用价值高。

7 电话诈骗防治运维管理对策

为更好履行运营商的社会责任,尽最大可能保护用户根本利益,运营商可采取内外兼顾的方式运维管理对策,方能提升电话诈骗防治效果。

- 建议建立地市、省、集团 3 级核心网信息安全监控手段流程,统一防护、治理策略,“全国一盘棋”。
- 建立核心网安全风险评估机制:诈骗呼叫风险主要在网络互通边界、租赁中继及一号通、呼叫中心等平台,建议开展信令层面风险漏洞评估,并加强日常运营中风险管控。
- 支撑工具能力提升:对信令应用系统升级,提升恶意呼叫、非法主叫的监控能力。
- 加强核心网信息安全常态化检查:对本网虚假号码、异常(超长、超短)国际号码、路由异常号码的定期抽查,发现问题及时整改,尤其对于本地接入的租赁中继应重点检查主叫鉴权、白名单情况(租赁合同中明确允许的主叫白名单号码)。
- 依据法律流程优化针对诈骗犯罪主叫号码回溯、查证快速通道,配合公安部门打击诈骗犯罪。
- 采用与公安合作共建或外租服务方式,引入诈骗电话预警拦截系统,解决动态、主动防御问题,在落地侧进行语音、短信诈骗的主动防御,基于号码甚至内容的精确拦截。

8 结束语

本文基于对电话诈骗问题根源与机制特征的研究,理



论结合实践,提出了防治模型、关键技术、解决方案以及运维管理对策,突破性形成一套科学高效的电话诈骗综合解决方案,并验证了有效性,对业界有良好的参考指导意义,有利于打击电话诈骗,有望扭转目前被动应对的局面,开创主动防御的新局面。

参考文献

- 1 胡向阳,刘祥伟,彭魏. 电信诈骗犯罪防控对策研究. 中国人民公安大学学报(社会科学版),2010(5)
- 2 席琨. 电信诈骗的分析与对策. 赤峰学院学报,2012,33(8)
- 3 潘洁,刘爱洁. 基于 APPDRR 模型的网络安全系统研究. 电信工程技术与标准化,2009,22(7)

[作者简介]



李力卡,男,中国电信股份有限公司广东研究院高级工程师,主要研究方向为核心网技术、网络运营技术及业务综合应用技术。



马泽雄,男,中国电信股份有限公司广东研究院高级工程师,主要研究方向为网络运营管理技术。



陈庆年,男,中国电信股份有限公司广东分公司高级工程师,主要研究方向为核心网络的维护及管理研究。



李程,男,中国电信股份有限公司广东研究院助理工程师,主要研究方向为核心网技术。

(收稿日期:2014-10-11)

(上接第 139 页)

文基于开源 SDN 技术,提出了一个综合解决方案,用于解决 NFV 内部虚拟化层、网卡 I/O、业务组链调度等多个方面的性能优化问题。最后通过单机实验结果,验证了开源技术优化能力和本文方案的有效性。

业界对 NFV 技术的研究正逐步深入,运营商关注的热点主要在 NFV 功能架构、业务链组网技术、控制器与协同管理技术等方面,对网络转发性能的研究将有助于该技术的部署应用,本文的 NFV 方案和优化技术讨论尚属于初步阶段,后期的工作方向包括加快原型系统开发、虚拟化层转发效率评估、业务链调度方法研究等几个方面。

参考文献

- 1 Network functions virtualization. <http://www.etsi.org/technologies-clusters/technologies/nfv>, 2014
- 2 Guan H, Dong Y, Ma R, et al. Performance enhancement for network I/O virtualization with efficient interrupt coalescing and virtual receive side scaling. IEEE Transactions on Parallel and Distributed Systems, 2013, 24(6)
- 3 Rizzo L, Lettieri G, Maffione V. Speeding up packet I/O in virtual machines. Proceedings of IEEE/ACM ANCS 2013, San

Jose, CA, USA, 2013

- 4 DPDK: data plane development kit. <http://www.dpdk.org/>, 2014
- 5 王亚,于干,张军等. PF_RING 与 NAPI 结合的捕包性能优化和仿真. 计算机工程与应用,2013(8)

[作者简介]



唐宏,男,中国电信股份有限公司广东研究院数据通信部部长、云计算研究所常务副所长,主要从事 IP 承载网、下一代互联网、云计算方面的研发与管理工作。



欧亮,男,博士,中国电信股份有限公司广东研究院高级工程师,目前从事互联网新技术和 IP 承载网络技术研究工作。

(收稿日期:2014-10-24)