



专题：网络空间安全

移动应用安全深度检测能力开放平台及部署关键技术

蔡逆水¹, 石屹嵘^{1,2}, 邱晨旭¹

(1. 移动互联网系统与应用安全国家工程实验室, 上海 201315;
2. 中国电信股份有限公司上海研究院, 上海 200120)

摘要: 关注电信运营商在现网移动应用安全监测服务所面临的挑战, 包括移动恶意 App 入口、移动应用安全实时监测和预警、快速阻断、及时告警、海量数据处理能力、定制服务方面等。在此基础上, 探讨了电信运营商移动应用安全深度检测服务能力开放平台分省服务模式, 提出了平台现网部署方案建议。

关键词: 移动应用安全; 深度检测; 能力开放平台; 安全特征库; 部署方案

中图分类号: TP393

文献标识码: A

doi:10.11959/j.issn.1000-0801.2018126

Open platform and key technology of mobile application security depth detection capability

CAI Nishui¹, SHI Yirong^{1,2}, QIU Chenxu¹

1. Mobile Internet System and Application Security National Engineering Laboratory, Shanghai 201315, China
2. Shanghai Research Institute of China Telecom Co., Ltd., Shanghai 200120, China

Abstract: The challenges that telecom operators faced in mobile network application security monitoring services were focused on, including mobile malicious application entry, real-time monitoring and early warning, rapid blocking, timely warning, massive data processing capabilities, customized services, etc. Based on this, the telecom operator's deep application of mobile application security, the service mode of the open platform and the distributed service mode of the open platform were discussed, and the platform's current network deployment plan was put forward.

Key words: mobile application security, depth detection, capacity open platform, security feature library, deployment scheme

1 引言

近年来, 电信网络诈骗越来越多。2016年9月23日, 最高人民法院、最高人民检察院、公安部、工业和信息化部、中国人民银行、中国银行业监

督管理委员会六部门联合发布了《防范和打击电信网络诈骗犯罪的通告》, 明确了电信网络诈骗犯罪是严重影响人民群众合法权益、破坏社会和谐稳定的社会公害, 必须坚决依法严惩。电信运营商响应通告精神, 积极探索防范电信网络诈骗

收稿日期: 2018-01-08; 修回日期: 2018-03-06



的有效手段，例如语音业务方面规范国际通信业务出入口局主叫号码传送，堵截“虚假来电”；短信业务方面重点识别、打击伪基站。上述工作在实际应用中已经取得效果，一定程度上降低市民受到诈骗的可能性。2017年第4季度，诈骗电话拨打次数同比下降78.2%，收到诈骗短信人数同比下降75.4%。在诈骗号码基数大幅减少、用户反诈骗意识增强双重因素影响下，诈骗号码标记数量同比下降47.4%^[1]。除电话、短信等方式外，移动互联网也成为诈骗犯罪分子的重点作案渠道，其原因包括：移动互联网强调体验，往往采用简化安全验证手段，诈骗分子更容易发现流程的漏洞；移动互联网用户防范意识较弱，普通用户很难识别诈骗信息。2017年第4季度网络诈骗类型表现异常，涉案金额占比从第3季度的17.1%提升到51.7%，案件数量从第3季度的36.8%提升到第4季度的66.9%，成为最大的诈骗类型^[1]。

移动互联网时代的今天，99%的网络诈骗都是通过网址作为入口，而恶意App作为高效的诈骗工具，操作更隐蔽、功能更强大。恶意URL和App采用盗号钓鱼、仿冒伪造等方式骗取用户的账号、密码等行为，为下一步实施诈骗做准备^[2]。面对严峻的网络犯罪形势，有效提升电信网络诈骗防范效率，电信运营商需要提供更加高效、实时、完善的移动应用安全监测服务系统，进行全网的移动应用监测。在移动恶意App实时监测和预警、快速阻断、及时告警、海量数据处理能力和定制服务方面提供移动互联网电信网络诈骗的防范和预警能力。

2 现网移动应用安全监测服务系统的关键问题及关键技术

为了更好地服务电信运营商移动网络用户、移动应用市场、金融机构和政企用户，移动应用安全监测服务系统需要满足如下关键需求。

(1) 电信运营商移动网络用户防范电信网络

诈骗实时监测预警需求

- 移动网络用户上网URL的分析，及时识别恶意URL。
- 移动网络用户下载App的分析，及时识别是否为仿冒伪造、病毒木马等类型的App。
- 发现风险后，通过短信提示、页面提示、实时阻断方式进行预警和阻断，将电信网络诈骗的来源以及影响范围降至最低。

(2) 金融机构等行业用户移动恶意程序溯源预警需求

恶意URL和恶意App以获取目标客户的账号、密码和隐私数据为目标。在识别之前如果已经发生用户信息泄露，则可提供给银行等金融机构行业客户，用于向其终端用户预警。

(3) 应用商店用户移动应用安全审查需求

- 移动应用商店每天上线App数量众多，通过人工检测的方式进行安全审核效率低下，且经常有“漏网之鱼”。通过自动化安全检测系统对上线App进行安全审查，及时发现恶意行为、违规内容和盗版应用并阻止其上架。
- 定期安全自查。根据《移动互联网应用程序服务管理规定》及上级主管部门相关规定，应用商店需要定期进行安全检测自查，并通过自动化安全检测系统定期检测并上报结果。

(4) 安全监管部门案件调查及涉恐、涉毒等违规检测需求

- 发布恶意URL路径、行为特征和实时跟踪，辅助执法部门打击伪基站等专项治理。
- 仿冒伪造、病毒木马等恶意App发布者溯源。
- 对发布应用内涉黄、涉赌、涉毒、涉恐和涉暴等内容的应用进行违规检测。

为了满足上述各类客户的关键需求，现网移动应用安全监测服务系统需要具备如下关键技术。

(1) 快速检测与深度检测相结合的移动应用安全检测方法

基于 App 及 URL 特征库的常规快速检测方法便于在现网实时监测,而 App 及 URL 深度检测方法有利于挖掘和发现新的移动恶意程序,包括 App 高危漏洞检测、App 内容违规检测、App 带壳检测、App 盗版检测、短码还原的检测项,其中内容违规检测利用图片检测、文本检测、音频和视频检测手段,对移动程序进行内容违规检测,并生成相关报告^[3]。

(2) 灵活的接口

针对不同应用场景,开展定制化安全服务。向各分公司提供不同行业、不同性质用户的差异化服务。

(3) 广泛的数据源

目前,各省公司只根据自己内部的数据进行检测,还需要整合基于互联网主流分发渠道市场与电信网络流量进行大数据分析,不仅拥有内部数据,还能快速爬取应用市场数据,及时更新。数据源应该覆盖国内 300+应用发布渠道,包括第三方应用市场、软件下载站、手机论坛等等,7×24 h 进行监测与分析,为监测系统提供海量的基础数据。只有拥有广泛的数据源,结合特色的检测内

容,才能更准确地实现对移动恶意程序的全方位、实时监测。

(4) 行业先进的检测技术

①可扩展的海量移动 App 爬取、存储及分析
检测移动 App 总数超过 600 万,每天更新应用数超过 10 万,反编译源码大小超过 80 TB。上述数据保存在以 HBase 为主的 NoSQL 数据库中,同时支持病毒木马分析、恶意行为分析、漏洞分析、盗版分析等多个分析引擎。

②多种类型检测技术

采用多种检测技术,对 App 进行检测。如图 1 所示,动静双引擎深度检测,快速判断内容违规、恶意行为;使用机器学习带壳检测,快速定位带壳信息;运用模式匹配方式进行多类型检测^[4]。

③基于人工智能的威胁预警与态势感知

实现基于应用源代码敏感行为识别的应用安全性分析方法,如通过逆向工具获取源代码;构造敏感行为的集合;敏感行为数据处理及特征值选取;构造训练集及安全性分析。

利用机器学习技术,可有效提高检测恶意应用的准确率。在此技术上,通过相似度算法计算各个恶意应用之间的关联性,及时发现恶意应用

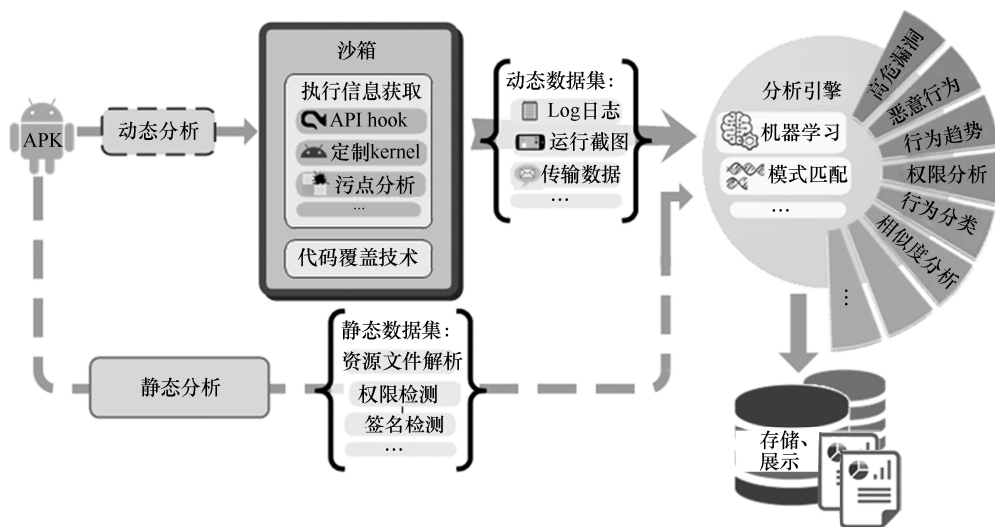


图1 动静双引擎深度检测



变种。同时，基于图分析算法技术描述恶意应用传播途径，确定传播范围并预测传播趋势，及时进行预警。

3 电信运营商移动应用安全深度检测服务能力开放平台

电信运营商为了实现全网渠道监控、实时检测和预警、快速阻断、及时告警等安全服务能力，需整合和优化现有的移动恶意程序监测相关的系统资源，集中建设移动应用安全深度检测服务能力开放平台；该平台提供统一的服务能力开放接口，对接各个省公司，为不同行业、不同性质用户提供差异化服务；实现在某运营商各个分公司的部署和实施，满足现网公众用户威胁预警和实时阻断需求、满足应用市场应用上架前审核需求、满足金融级和政企客户渠道监测需求^[5]。

3.1 系统架构

总体技术架构如图 2 所示，为三级结构，分

别是集团公司服务能力层、省公司资源与服务能力层和最终用户层。

(1) 集团一级管理员

某运营商作为一级管理员，享有最高权限。通过整合分散的安全能力，如在本项目中集成和开放运营商已有的 App 恶意检测能力以及 URL 检测能力，新增如 App 内容检测、App 高危漏洞检测、App 盗版检测、带壳检测、短码还原的检测能力，构建安全数据库，如 App 黑白名单、URL 黑白名单、App 特征库、URL 特征库，形成可在省公司具体落地实施的安全能力。

(2) 省电信二级管理员

各省公司作为二级管理员和具体落地部署的单位，具体实施和部署本项目系统，权限内容由某运营商决定。各省公司根据辖区内客户具体需求提供定制化的安全服务。

(3) 典型客户

第三级为客户。目标客户包括高净值 / VIP

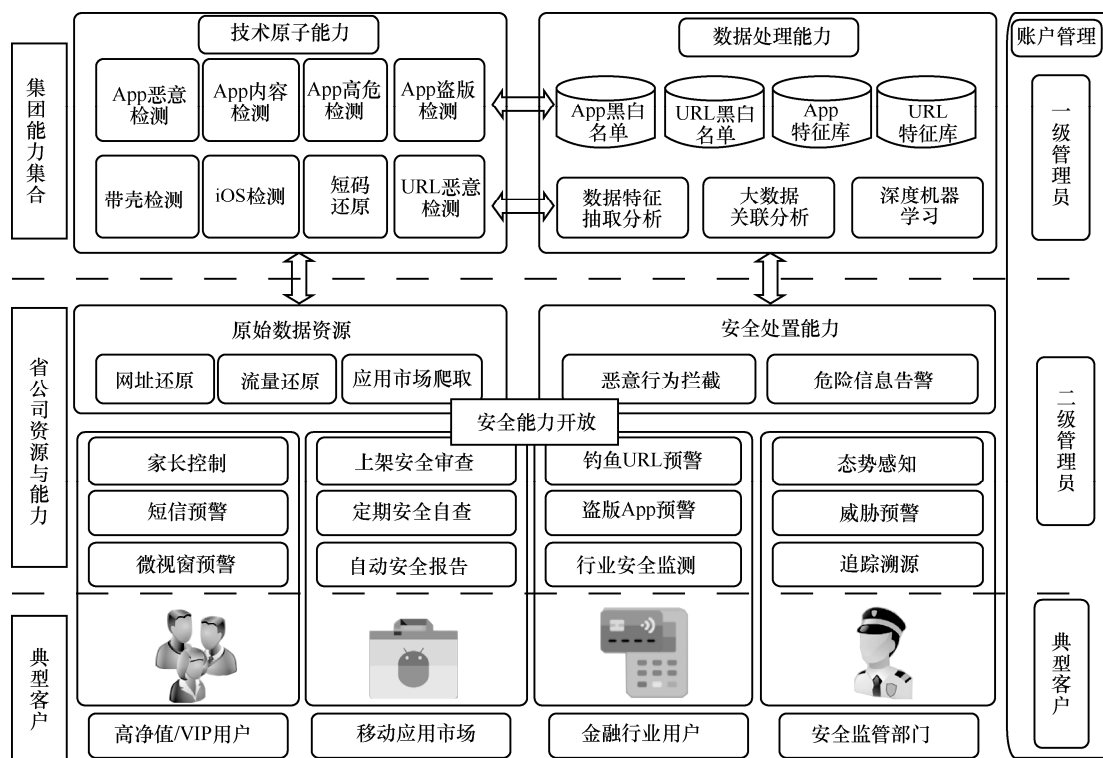


图 2 系统结构

用户、移动应用市场、金融行业用户和安全监管部门，可以申请以下服务：渠道监测、应用市场安全状态感知和应用检测能力开放等。

3.2 系统功能

本系统总体功能结构如图 3 所示，为三级结构，分别是对外服务平台、系统调度平台及检测能力。

(1) 对外服务平台

典型用户，如高净值用户、政企和应用市场等，需要提供数据分析能力，为省公司提供与处置系统对接接口，提供报警、提醒能信息及时推送客户，为省公司提供运行状况、分析、预警、高危漏洞、恶意 URL 和 App 的变化趋势等数据分析能力。

(2) 调度平台

省公司根据辖区内客户具体需求提供定制化的安全服务，根据调研结果，各省公司主要需要以下功能：大客户定制服务，如金融客户要求能够掌握各应用市场的应用安全态势；接入现网流量进行恶意应用识别，对接已有现网处置方式，并回传恶意应用 MD5 和恶意 URL，用于服务公

众用户；应用检测能力开放，并集成现有处置分析系统及其他检测系统检测能力。

(3) 检测能力

App 内容检测、App 高危漏洞检测、App 盗版检测、带壳检测、短码还原的检测能力，构建安全数据库，如 App 黑白名单、URL 黑白名单、App 特征库、URL 特征库，并形成可在省公司具体落地实施的安全能力。

3.3 权限管理

如图 4 所示，系统分为三级管理权限：普通用户、省公司业务管理员、集团级管理员。普通用户可分为个人用户、应用市场用户、企业用户等，并根据省级运营商开通服务类型提供不同服务。省公司业务管理员对业务人员进行管理、授权等：开通用户业务，提供行业安全态势、省级安全态势分析，威胁预警。集团业务管理员具有省级权限，拥有整个 URL、App 黑名单的管理以及全国安全态势分析、威胁预警的权限。

作为分级系统，存在多种定制需求，包括敏感词定制、恶意类型筛选、个性化移动评估体系、违规内容定制、敏感权限定制和处置方式定制等，

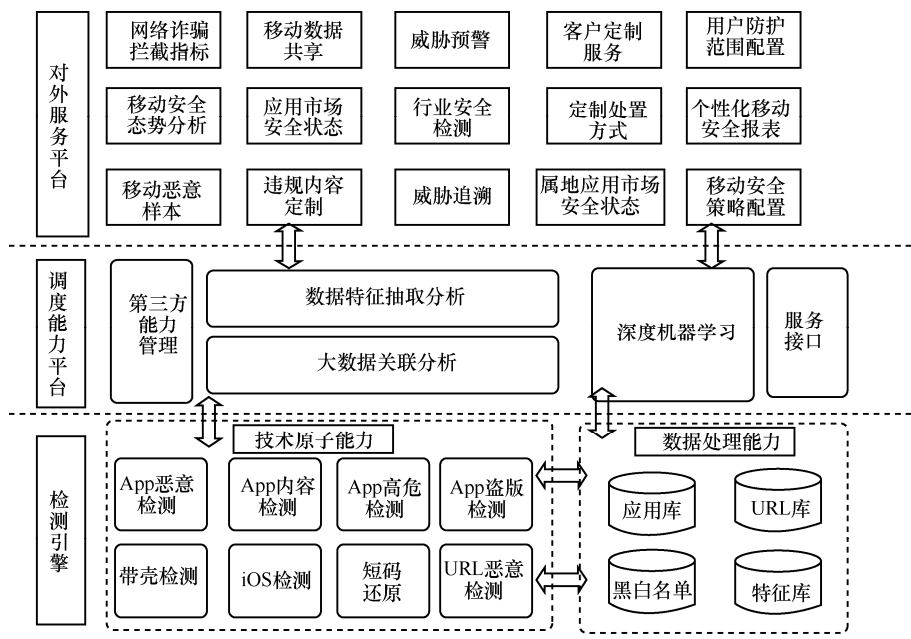


图3 功能设计

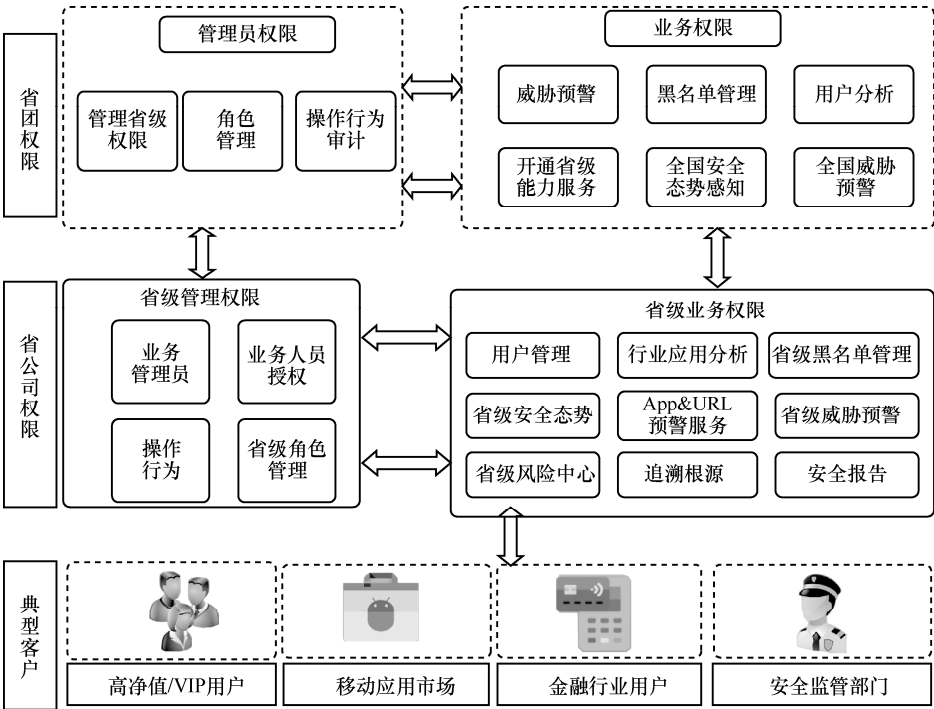


图4 三级管理

这些服务都需要定制化和

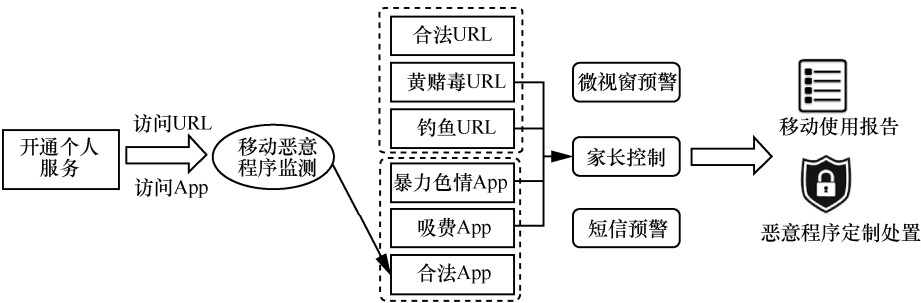
4 某运营商移动应用安全深度检测服务能力开放平台现网对接运营

4.1 平台现网部署实施方案

某运营商为了更好地满足各个省公司的移

动应用安全监测服务需求，集中建设了移动应用安全深度检测服务能力开放平台。其中，对接某省级运营商公司服务移动网络用户的移动应用安全监测服务需求，服务需求如图5所示。

深度检测服务能力开放平台与某省级运营商现网移动互联网恶意程序监测防治系统对接，通



服务内容	服务描述	后续动作
微视窗预警（免费）	平台默认安全策略，恶意程序触发后通过微视窗发送提示	无
恶意程序定制处置	家长在后台定制需要控制恶意程序策略、时间	定制安全策略，自主控制处置方式
移动使用报告	触发的恶意程序使用统计	明确使用方式及特点

图5 面向公众用户的服务需求

过 SFTP 方式接收现网的移动互联网恶意程序监测处置系统中还原出的 App, 调用深度检测服务能力开放平台的八大技术原子能力对应用程序进行深度检测和安全漏洞挖掘分析, 及时识别恶意行为和安全风险, 形成移动应用安全分析报告, 通过 API 的方式反馈到某省级运营商 URL 和 App 特征统一安全库, 最终通过省公司现有的用户服务平台进行能力输出, 满足移动网络用户安全服务需求。

移动互联网安全研判分析系统建立在用户服务平台和移动互联网恶意程序监测处置系统之上, 如图 6 所示, 现网对接系统架构由数据采集层、数据仓库层和数据分析层 3 部分组成。

(1) 数据采集层

- 数据采集接口: 以 FTP 方式采集移动互联网恶意程序监测处置系统还原的应用程序包。
- 海量 URL 预处理: 将海量应用程序分组预处理 (去重去白、异常值处理等) 后放入数据仓库, 降低存储成本、提高后期分析准确性。

(2) 数据仓库层

- 采用 Hadoop 架构进行存储, 对应用程序分

组进行缓存, 采用内置任务调度工具对搜索、挖掘、匹配等任务进行管理。数据采集层处理完后的原始数据和数据分析层比对之后的数据都存入数据仓库。数据仓库层按照数据分析层的逻辑规则将最终分析数据对接、更新现有 URL 和 App 特征统一安全库。

(3) 数据分析层

利用五大功能模块对数据仓库层的原始数据进行分析与处理, 形成最终数据, 并存入数据仓库层。主要有以下几个组成部分。

- App 深入检测模块: 该模块调用 App 检测及安全漏洞挖掘分析接口, 以 SFTP 方式准实时传输数据, 分析匹配完成后通过该接口回传相应的“恶意 App 及安全漏洞分析报告”“安全态势分析报告”。
- App 初步检测模块: 对移动网络中的 App 进行初步的判断分析, 并将结果为疑似恶意的 App 发送至恶意 App 检测任务调度模块。
- App 检测任务调度模块: 配置检测任务调度规则及自有库更新的触发规则, 依据初

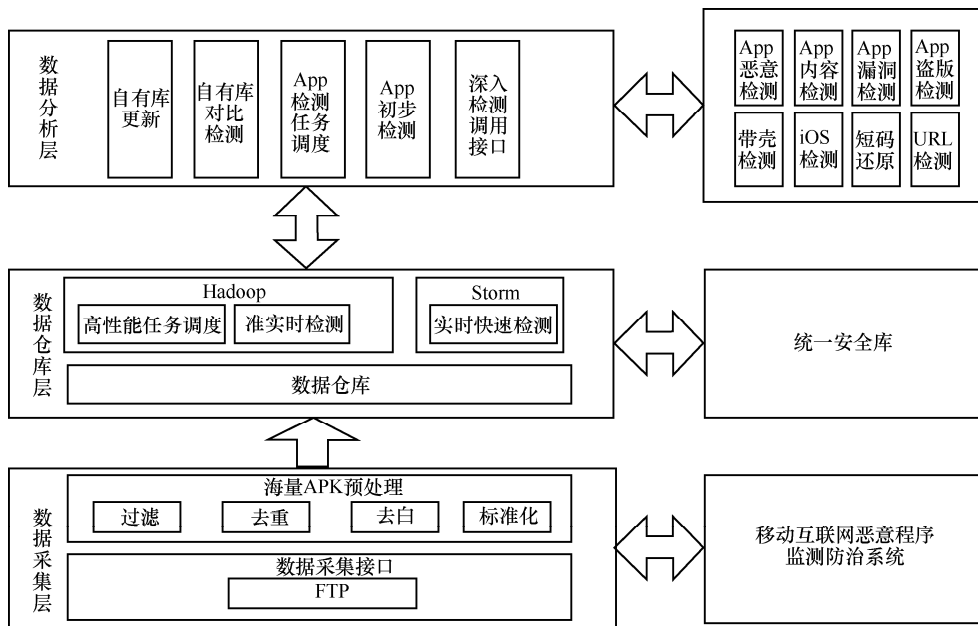


图6 现网对接系统架构



步研判分析结果进行任务调度，并将结果为疑似恶意的 App 发往深入检测调用接口进行深度检测及安全漏洞挖掘分析；再根据反馈结果对自有统一安全库进行更新。

- 自有库比对检测模块：将移动互联网用户访问的 App 与 URL 和 App 特征统一安全库进行实时比对预判。
- 自有库更新模块：对自有库进行更新维护，删除分析后确认已失效的 App 特征值；新增检测为恶意但尚未纳入统一库的 App 特征值。

深度检测平台现网对接部署实施如图 7 所示。

(1) 深度检测平台

集团集中部署，主要包括对外服务平台、能力调度平台、内部能力管理、检测引擎等。

- 对外服务平台：针对高净值用户、政企、应用市场等典型用户，需要提供数据分析能力，为省公司提供与处置系统对接接口，将报警、提醒信息及时推送给客户，为省公司提供运行状况、分析、预警、高危漏洞、恶意 URL 和 App 变化趋势等数据分析能力。
- 能力调度平台、内部能力管理：能力调度平台整体协调自主研发能力及现有危险处理系统和第三方检测能力，内部能力管理是

指对 App 内容检测、App 高危漏洞检测、App 盗版检测、带壳检测和短码还原的检测能力进行管理，构建安全数据库，如 App 黑白名单、URL 黑白名单、App 特征库和 URL 特征库，发现现网流量中存在的恶意 App 和恶意 URL。

- 检测引擎：提供 App 内容检测、App 高危漏洞检测、App 盗版检测、带壳检测和短码还原的检测能力。

(2) 各省现网服务平台

部署在省公司，主要包括检测前置机和处置系统。

- 检测前置机：目前已经具有部分检测能力，保存对恶意 App 和 URL 的分析数据和分析结果。服务器根据数据类型分发能力调度平台为整个系统检测能力提供服务支持。
- 处置系统：通过对接接口为用户提供预警、实时阻断。

(3) 系统接口

目前与现有能力、处理能力接口方式为 FTP 文件服务器中转模式。所有所需检测文件、文件格式说明、处理结果统一放置 FTP 服务器。

4.2 平台对接某省级运营商运营效果

自从某运营商移动应用安全深度检测服务能力

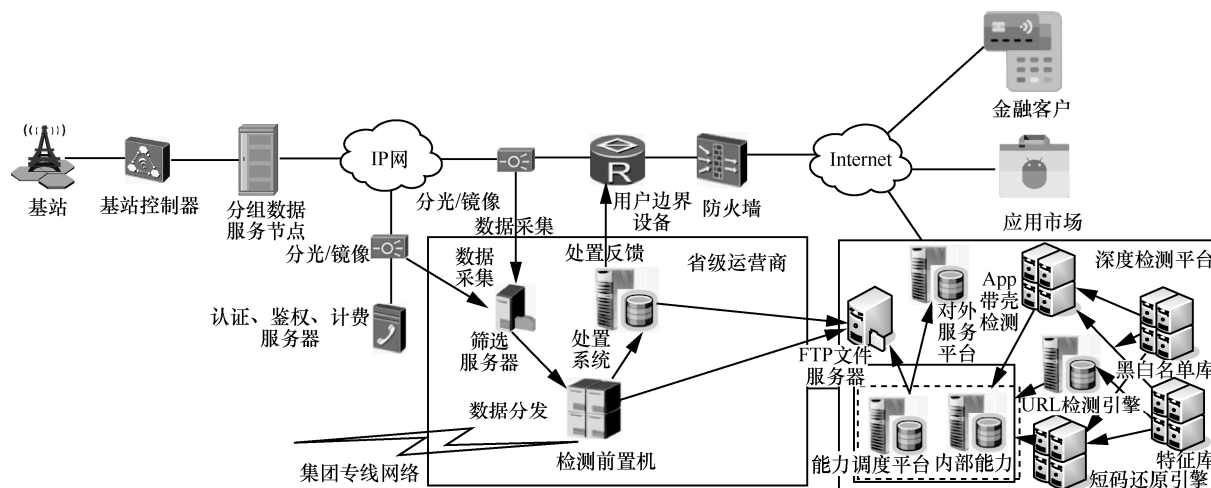


图 7 某省级运营商部署网络拓扑

开放平台与某省级运营商现网移动恶意程序监测防治系统对接运营以来,初期日均处理 APK 数量约 3 000 个,每周检测出的恶意 APK 数量在 82 个左右,每日漏洞数量在 1 600 个左右,每日检测完成率为 100%。

在对每日数据进行数据清洗后,通过结合动静双擎检测,对数据进行恶意行为方面的分析。据统计,每日恶意行为数量为 20~30,占总接收数据的 0.66%~1.0%。

在漏洞数量方面,每日检测到的数量为 1 200~1 800 个,分为低危漏洞、中危漏洞以及高危漏洞,其中,低危漏洞数量占有所有漏洞数量的近九成,高危漏洞虽占比最低,但是高危漏洞是窃取用户隐私、恶意病毒入侵应用程序的重要突破口,因此需引起足够的重视。

目前,经过半年多的稳定运营,某省级运营商需借助移动应用安全深度检测服务能力开放平台对外开放能力分析的 App 数量从 3 000 个/日下降到 500 个/日。某省级运营商现网移动应用安全监测服务系统平均每月监测到安全事件约 700 万次,保护 250 多万的天翼手机用户,安全事件同比下降超过 40%,运营服务效果显著。

5 结束语

本文分析了电信运营商在现网移动应用安全监测服务所面临的挑战,包括移动恶意 App 入口、移动应用安全实时监测和预警、快速阻断、及时告警、海量数据处理能力和定制服务方面等。在此基础上,探讨了电信运营商移动应用安全深度检测服务能力开放平台分省服务模式,提出了平台现网部署方案建议,并通过具体应用案例,说明了移动应用安全深度检测服务能力开放平台在应对电信网络诈骗风险方面的积极作用。

参考文献:

[1] 第四季度《反电信网络诈骗大数据报告》发布[EB/OL].

(2017-02-07)[2018-01-08]. <http://www.cww.net.cn/article?id=427391>.

Fourth quarter "large data report on anti telecom network fraud"[EB/OL]. (2017-02-07)[2018-01-08]. <http://www.cww.net.cn/article?id=427391>.

[2] 移动应用安全检测平台/App 安全测试评估[EB/OL]. (2018-01-07)[2018-01-08]. <http://safe.ijiami.cn/>.

Mobile Application security detection platform/App security test evaluation[EB/OL]. (2018-01-07)[2018-01-08]. <http://safe.ijiami.cn/>.

[3] DWIVEDI H, CLARK C, THIEL D. 移动应用安全[M]. 李祥军, 罗熊, 译. 北京: 电子工业出版社, 2012.

DWIVEDI H, CLARK C, THIEL D. Mobile application security[M]. Translated by LI X J, LUO X. Beijing: Electronic Industry Press, 2012.

[4] 黄晓庆, 王梓. 移动互联网之智能终端安全揭秘[M]. 北京: 电子工业出版社, 2012.

HUANG X Q, WANG Z. The security of the intelligent terminal of the mobile internet[M]. Beijing: Electronic Industry Press, 2012.

[5] 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[J]. 电信科学, 2015, 31(12): 111-116.

XUE L H, LIANG X J. The key technology of traffic security audit for operator oriented mobile networks[J]. Telecommunications Science, 2015, 31(12): 111-116.

[作者简介]



蔡逆水(1965—), 男, 博士, 移动互联网系统与应用安全国家工程实验室资深安全研究员, 主要研究方向为移动应用安全检测、电信网络反欺诈、移动互联网重点业务和行业风险控制与安全运营技术。

石屹嵘(1970—), 男, 移动互联网系统与应用安全国家工程实验室副主任、高级工程师, 中国电信股份有限公司上海研究院互联网安全部副主任, 中国电信股份有限公司集团级优秀人才。主要研究方向为安全架构设计、安全管理、大数据平台技术、大数据分析和模型设计、信息系统架构设计、企业架构设计等。获得国家多项专利授权, 发表论文 10 多篇, 并获得 CISSP 和 CISA 等多项国际认证。

邱晨旭(1973—), 男, 现就职于移动互联网系统与应用安全国家工程实验室, 主要研究方向为信息安全管理、大数据应用安全、移动互联网重点业务和行业风险控制与安全运营技术。