移动应用全生命周期管理平台的研究与实践

殷铭，李琳
（中国电信股份有限公司研究院，上海 200120）

摘　要：针对移动应用各种安全服务的发展现状，研究了目前主流的移动应用安全检测监测技术。在结合软件行业中的全生命周期管理概念的基础上，将多种安全理念和安全技术合理地融入移动应用全生命周期中的各个阶段，并基于此设计和构建了一个安全功能全面、多系统协同工作的移动应用全生命周期管理平台。

关键词：移动应用；全生命周期；管理平台；安全
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2020316

Research and practice of mobile application lifecycle management platform

YIN Ming, LI Lin
Research Institute of China Telecom Co., Ltd., Shanghai 200120, China

Abstract: According to the development status of various security services for mobile applications, the mainstream mobile application security detection and monitoring technology was studied. Based on the concept of full life cycle management in software industry, a variety of security concepts and security technologies were reasonably integrated into each stage of the whole life cycle of mobile applications. Based on this, a mobile application lifecycle management platform with comprehensive security functions and multi system cooperation was designed and constructed.

Key words: mobile application, life cycle, management platform, security

1　引言

得益于信息化技术的蓬勃发展，移动终端设备正在大量地普及，移动互联网基础设施也在不断地完善。鉴于目前移动互联网庞大的生态体系，众多开发者不断地为其贡献着大量的移动应用。截至 2019 年 12 月，我国市场上监测到的移动应用数量为 367 万款，第三方应用商店在架应用分发总量达到 9 502 亿次，下载量呈现爆发式增长。海量移动应用在给日常生活带来便利的同时，还带来了诸多安全隐患，由移动应用带来的隐私泄露和财产损失的新闻屡见不鲜。这一系列的风险为广大开发者和用户都敲响了警钟，因此需要从移动应用全生命周期的角度进行整体的安全防护，而不是基于当前片面的安全防护甚至忽视安全防护的重要性。

收稿日期：2020−09−01；修回日期：2020−12−04

目前在移动应用安全方面已经有众多的研究成果，同时，在移动应用全生命周期的安全管理方面，参考文献[1]做了一定的理论探究。

2 管理平台介绍

移动应用全生命周期管理平台定位为集团移动应用全生命周期的安全管理平台，逐步将集团对内和对外服务的移动应用纳入全面的安全监管，促进集团内优良的移动应用生态的建设，避免从开发到运营的整个流程中可能出现的风险。此外，在满足集团需求之余，将安全管理服务的范围扩大到普通公众用户。针对目前移动应用安全现状，有必要从移动应用的整个生命周期内对其使用相应的安全检测监测手段。通过采取一系列的安全措施，使移动应用不易被反编译和篡改，以此达到保障应用自身的安全。对于盗版、仿冒等恶意应用进行定期有效的安全检测和风险识别，对应用在运行过程中面临的威胁以及产生的恶意行为进行实时监测并及时阻断。

基于上述要求，移动应用全生命周期管理平台参考了软件行业的全生命周期理念，同时采用了安全软件开发生命周期模型和热门的DevSecOps 模式。基于软件开发周期的移动应用全生命周期管理如图 1 所示。

移动应用全生命周期管理流程如图 2 所示，可以看出，基于软件安全开发周期的移动应用全生命周期管理覆盖移动应用开发、测试、上线、发布、运营各个环节，可以实现多种工具的集中管理、做到任务的集中分发以及数据的集中统计。

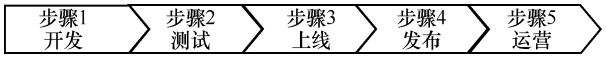


图 2 移动应用全生命周期管理流程

在整个流程中，全生命周期管理包含了对移动应用的安全检测、渠道监测、安全加固、个人隐私风险检测、应用发布、应用合规检测、威胁感知预警和态势分析等众多服务。这种管理方式可以帮助移动应用实现安全管理实现全流程落地，提供对移动应用进行全生命周期的一站式安全解决方案；做到对接入的移动应用进行全方位治理，营造清朗的网络空间，同时在当今“互联网+”的趋势下，进一步面向各行各业进行安全赋能。区别于传统的安全管理流程，除了将安全技术体现在流程的各阶段外，移动应用安全开发知识的培训以及安全开发规范和移动应用管理制度贯穿始终，成为移动应用全生命周期管理的重要组成部分。创新部分主要从以下 4 个方面体现。

（1）先进的理念

移动应用全生命周期管理平台通过引入了软件行业的全生命周期理念，结合目前热门的敏捷开发、微服务、中台、云原生 2.0、安全软件开发生命周期、DevSecOps 和零信任，使本平台从开发到运营过程都保持以先进的理念作为内核。

（2）多系统联动

管理平台的各项功能并不是单纯的技术堆砌，多个检测系统可以相互融合，互相调用。例如，对于上报的 App 资产，平台会自动进行安全

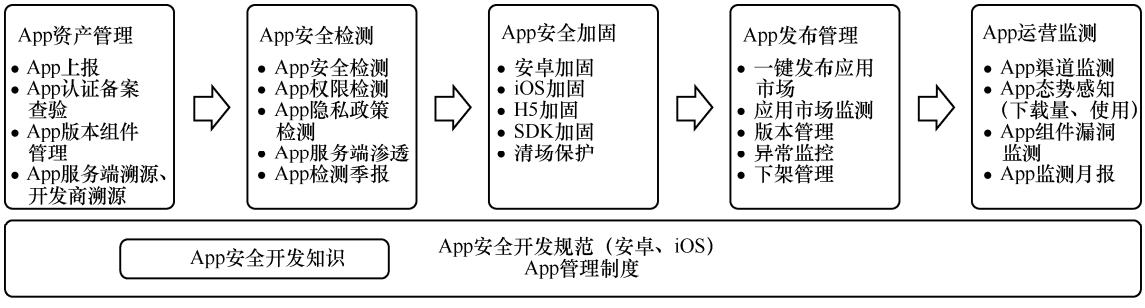


图 1 基于软件开发周期的移动应用全生命周期管理

检测以及渠道监测，同时对发现的恶意应用进行服务端溯源。通过系统间的协同，使它们不再孤立，能够发挥“1+1>2”的效果。

（3）多种服务方式

以公有云账号的 SaaS 方式和 API 的 PaaS 方式提供服务，既方便用户通过在线方式提交移动应用使用服务，也使用户可以很容易通过接口调用平台提供的能力用于集成到自己的项目中。

（4）智能预警

移动应用全生命周期管理平台能够提供智能预警服务。

对于用户提交过第三方 SDK 检测的移动应用进行应用与第三方 SDK 的关联，当管理平台发现某款第三方 SDK 出现风险时，可以将调用了该 SDK 的应用提取出来，对上传该应用并订阅了此预警功能的用户进行及时通知，使用户能在第一时间了解相关风险。

对于用户提交过渠道监测并订阅了预警功能的移动应用，管理平台可以定时更新该应用的最新渠道情况，并及时将应用存在的下载渠道、盗版仿冒情况以及下载链接是否失效等信息及时反馈给订阅用户，使得用户能够了解应用的渠道情况并为应用的下架提供技术支持。

3　管理平台实践

移动应用安全主要包括移动应用客户端的安全、移动应用服务端的安全以及两者之间数据传输的安全。从软件的全生命周期角度审视，移动应用的安全则应贯穿于软件开发前的环境配置、软件开发的过程以及软件开发完成后的上线运行等全部阶段。

3.1　整体设计思路

（1）循序渐进

移动应用全生命周期管理平台是一个需要不断迭代升级的大型项目，需要对其设计和构建过程进行详细地规划并循序渐进地进行。本管理平台采用敏捷开发的模式方便项目快速推进以及不断升级完善。

（2）模块化

移动应用全生命周期管理平台不是一个一成不变的项目，随着技术的更迭、外部市场环境的变化以及技术实力的积累，针对于管理平台中的部分模块可能存在增删或者替换的需求，现有系统的搭建必须考虑拓展性并做到“高内聚、低耦合”的形式。因此，此管理平台采用目前热门的微服务架构搭建并引入移动应用中台的概念，不仅能做到复用多个模块方便开发，还能优化整体程序架构，将管理平台中各个模块间的相互影响降到最低。

（3）云服务

移动应用全生命周期管理平台充分利用了以云计算为基础的云原生 2.0 的优势，发挥其 Docker 容器化部署的“一处打包、到处部署执行”的易于部署和扩展的特性。通过主从备份模式和一系列及时处置措施保证管理平台的平稳运行并尽力避免霾计算的产生，为用户提供稳定、高效的服务。

（4）平台自身安全

移动应用全生命周期管理平台在对外提供服务的同时，需要考虑平台自身以及与客户端交互过程中的数据传输安全。管理平台在设计和建设过程中严格按照软件安全开发规范进行落实，并制定和严格执行管理平台运维管理办法，确保用户使用管理平台的过程中用户数据的存储安全。在数据传输安全方面，依据本平台 2C（business to customer）和 2B（business to business）业务的不同，采用不同的数据传输方案。针对 2C 业务的场景，由于需要直接对外公网全网暴露，故采用网络 ACL（access control list）及 WAF（Web application firewall）技术对出入流量进行控制与过滤，同时采用 IDS/IPS（intrusion detection system/intrusion protection system）实现对异常流量的

告警和及时处置。针对 2B 以及定制化业务，本平台采用零信任网关技术以及基于此技术的更为智能的精益信任的理念，做到非授信用户无法探测管理平台入口，同时实现将产生异常行为的授信用户进行降级，甚至临时列入失信名单的智能化处置。

3.2 方案设计和功能说明

移动应用全生命周期管理平台各模块展示如图 3 所示，移动应用全生命周期管理平台的设计依赖于图 3 的整体方案，所以整个安全管理平台的构建也按照这 5 个步骤进行详细地划分。通过将各项安全技术和功能模块进行合理的安排，移动应用全生命周期管理平台能够做到在移动应用从开发到运维的过程中，充分融入安全的理念，将 DevSecOps 的理念真正落实到实践中。

（1）开发阶段

安全开发规范：在传统软件开发领域中，将安全因素越早考虑进来，随后因安全因素所带来的软件开发成本才会越低。这一原则在移动应用开发领域也同样适用，因为在开发阶段对安全重视才能从源头上避免一些安全问题的出现。然而，由于当前移动应用开发周期越来越短，而且较多的开发者一味地追求应用功能的丰富以及对安全知识缺乏了解或者本身并不重视软件的安全性，所以为了避免这种情况的出现，本管理平台会在开发阶段提供《移动应用安全开发规范（Android 篇）》和《移动应用安全开发规范（iOS 篇）》等在内的一系列安全编码规范，以期在此阶段提高用户的安全开发意识和水平。

代码审计：通过遵守安全开发规范能在很大程度上杜绝一些应用漏洞的产生，但是随着应用复杂度的提升以及开发过程中难免会有一些疏漏，移动应用全生命周期管理平台在开发阶段还提供了代码审计功能。它能对用户开发的移动应用源码进行全方位的分析，包括对应用进行安全开发规范方面的检查以及发现应用源代码中存在的 SQL 注入漏洞、XSS 漏洞、CSRF 漏洞等威胁。

安全 SDK 组件：在开发过程中，为了在加强安全防护的同时降低开发者在安全防护方面的压力，移动应用全生命周期管理平台需要提供安全 SDK，方便开发者集成到自己应用中起到保护作用。目前管理平台会提供的安全 SDK 功能如下。

- 清场 SDK：在移动应用被安装之前对当前系统运行状况进行检测，包括设备是否 root/越狱，应用运行的环境是否安全等。
- 安全键盘 SDK：将普通键盘的键序随机化，并对用户输入的数据进行加密，同时防止键盘被截屏攻击，使用户的输入数据不会被监听和窃取。

（2）测试阶段

安全检测：对移动应用内部存在的安全风险进行检测，针对发现的安全问题给出解决建议，帮助开发者了解并提高其开发程序的安全性。此外，对于加固的移动应用，能够进行自动化脱壳，以提高检测的准确性。检测结合了静态检测项和动态检测项，特别地，在动态检测部分使用了模

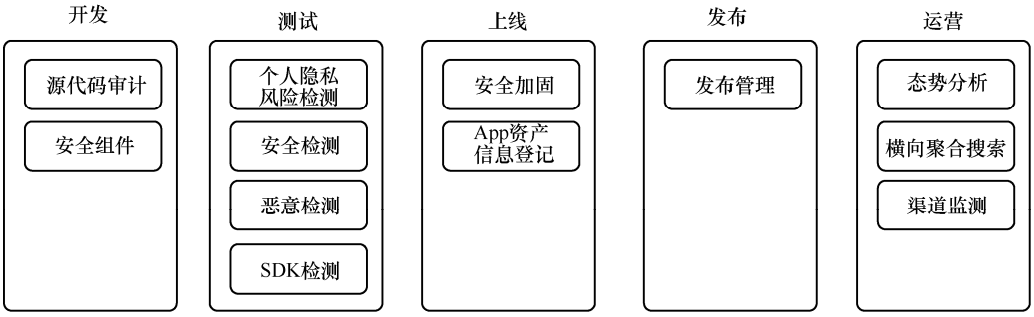


图 3 移动应用全生命周期管理平台各模块展示

拟器和真机相结合的方式。

个人隐私风险检测：对移动应用中涉及个人隐私的权限获取和数据泄露情况进行检测，包括个人数据传输泄露风险及本地存储泄露风险，可以有效检测移动应用违法违规获取个人隐私数据的行为。

恶意检测：采用特征码匹配融合人工智能的方法，前者能够快速地发现已知的恶意应用，而基于深度学习的人工智能方法，通过从 AndroidManifest.xml 文件中提取的权限等静态特征进行 one hot 编码与 API 调用等动态特征相结合，能够有效地识别未知的恶意应用，同时由于系统采用了半监督学习以及强化学习的方式，使其具有一定的自学习能力，能够在不断的自我学习中提高对未知恶意应用的检测能力。

第三方 SDK 组件检测：随着移动应用的快速发展，目前一款应用所含的功能十分丰富，除此之外，一些如广告、推送、第三方登录、分享以及安装、下载的统计等众多通用接口或模块都会通过集成成熟的第三方 SDK 的方式进行调用。这在方便开发者的同时也将一些不确定因素引入了自身的应用。

- 这些被调用的第三方 SDK 对于使用它的开发者而言依旧是黑盒的，所以存在第三方 SDK 窃取用户信息的可能。
- 第三方 SDK 如果出现漏洞的话，即使原本的应用是安全的，也会因此受到威胁，而且由于第三方 SDK 不受应用的开发者控制，所以应用开发者不容易知晓 SDK 何时出现何种漏洞以及出现的漏洞何时会被修补。

上述不确定因素影响着移动应用的安全，所以针对移动应用安全性的考量不能只重视开发自身所编写的代码质量。管理平台不仅会对用户上传的移动应用进行所有第三方 SDK 基本信息的获取，同时会对这些 SDK 的安全性进行检测，通过与漏洞库的结合，发现其中存在的安全问题。

（3）上线阶段

安全加固：集成行业领先的加固技术，为用户提供全面的移动应用加固加密技术和攻击防范服务，使加固后的应用具备防逆向分析、防二次打包、防动态调试、防进程注入、防数据篡改等安全保护能力。

移动应用资产信息登记：资产备案系统可为企业和个人提供移动应用资产信息登记管理服务。其中包含资产登记、资产审批、资产审核、数据统计、月度报告五大功能模块；资产登记信息涵盖基本信息、扩展信息、联系人信息、许可资质与自评估文件、应用文件 5 个部分。用户可将应用资产在系统中进行登记，按要求填写内容，操作简单。子用户的应用资产需经上级用户审批后提交，审批审核流程均在线上操作，流程便捷可靠。

（4）发布阶段

发布管理：发布管理包含了合规服务和发布服务。由于近两年来，国家越来越重视用户个人隐私，同时也发布了多项针对移动应用在隐私合规方面的文件，因此在应用正式发布之前，对应用进行用户隐私合规方面的检查就凸显了其重要性。移动应用全生命周期管理平台对于将要上线应用市场的移动应用通过 NLP 结合部分人工的方式进行半自动化的隐私合规文本的检测。在移动应用合规性之外，开发者可能为了了解应用在不同渠道的下载量以及留存率等数据，需要对即将发布的应用进行多渠道打包。为了减少用户在应用发布到不同应用市场时所需进行的操作，管理平台提供了多渠道打包服务，给每个应用按照要投放的市场，打上独有的标识。

（5）运营阶段

渠道监测：提供渠道数据分析、疑似盗版仿冒应用的识别和分析服务，帮助客户管理应用推广渠道，第一时间发现可疑盗版仿冒应用，保护

客户合法权益。

态势分析：通过自动化爬取和解包模块，收集海量数据，能够实时展示全网应用的仿冒率、代码混效率、加固率、应用检测排名、应用风险排名、下载量以及活跃度等指标，清晰直观掌控全网移动应用的安全状况，并能对应用开发者、后台服务端信息进行溯源。

横向聚合搜索：将获取到的海量移动应用数据进行关联整合，可以从多维度了解移动应用的详细信息。

3.3 系统架构设计

移动应用全生命周期管理平台的实现总体分为两个子平台，将面向用户的业务平台与自身的能力平台分开。业务平台主要包含用户管理、服务管理、计费管理、权限管理和业务管理等，而能力平台的构建通过分层的形式进行设计，包括了能力开放层、能力层、数据存储层、数据处理层、数据采集层和数据源部分。两个子平台通过统一认证模块互联，并由能力开放层通过 REST API 形式形成相互调用。移动应用全生命周期管理平台技术框架如图 4 所示。

整个平台的开发主要使用 Java 语言，框架使用 Spring Boot，配套的爬虫工具采用 Python 编写，使用了 Scrapy 框架。

3.4 物理部署架构

移动应用全生命周期管理平台的拓扑如图 5 所示。用户通过互联网透过防火墙等安全措施访问部署在云上的服务。所有请求会通过代理服务器集群向业务平台服务器转发，业务平台服务器与能力平台服务器交互，间接调用后端部署的各种引擎所提供的服务。由于平台采用了独立崩溃模式，其服务在单个引擎故障的情况下并不会影

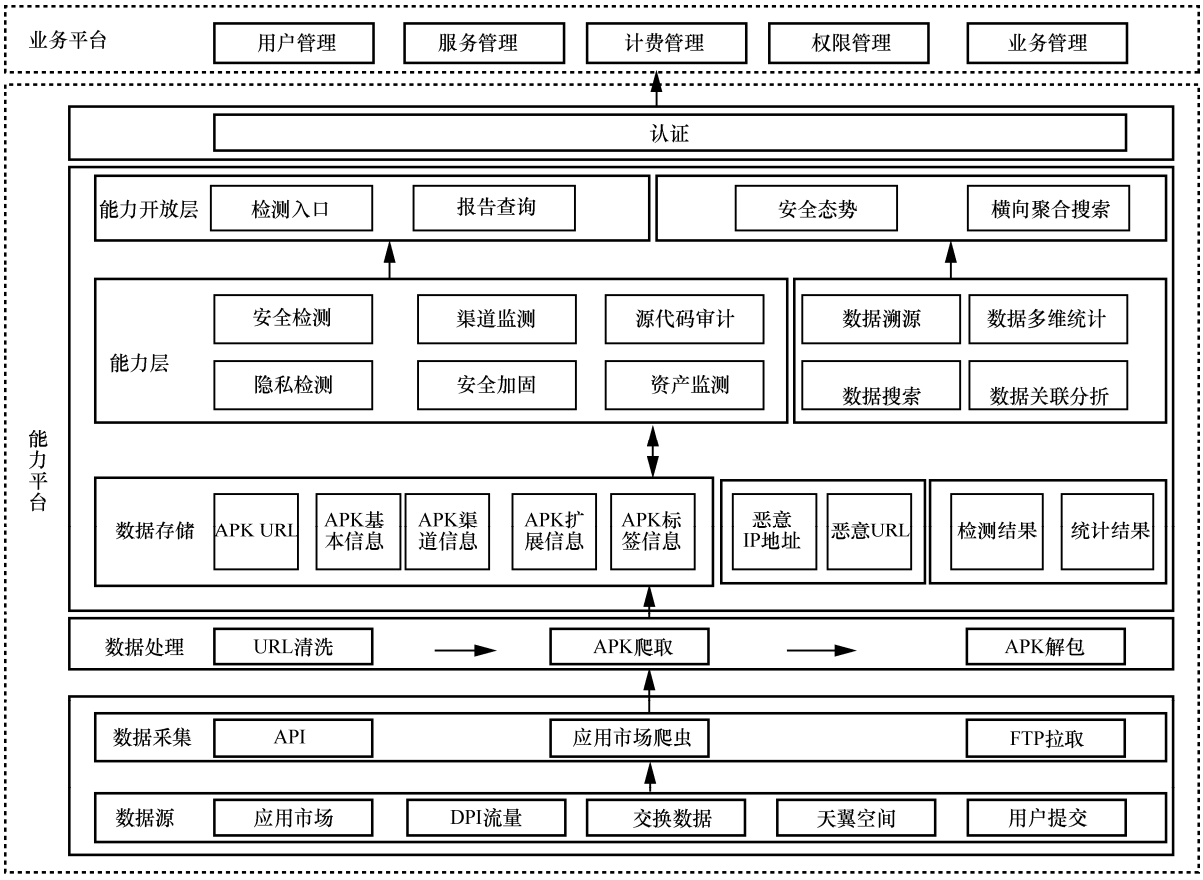


图 4 移动应用全生命周期管理平台技术框架

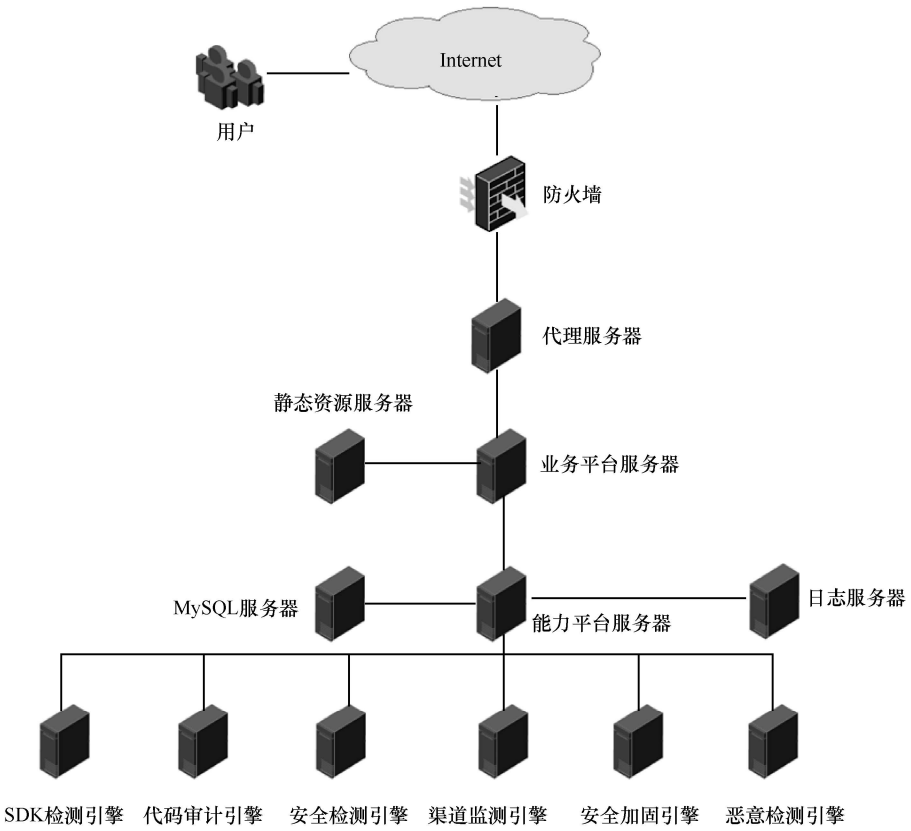
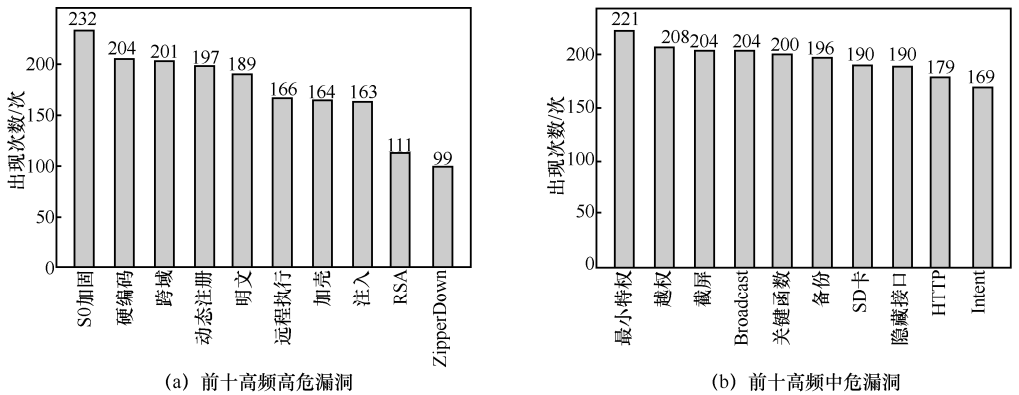


图 5　移动应用全生命周期管理平台拓扑

响其他服务。

4　应用成效

目前移动应用全生命周期管理平台已经在云上部署并且在小范围内测试以及集团内部使用。根据每月对中国电信自营合作应用的检测和分析，这些应用的平均安全得分均分显著增加，表明中国电信自营合作应用的安全性得到了提升。同时也能从已有的数据中分析得到中国电信自营合作应用中高频出现的高中危风险，提醒开发者注意这些风险漏洞。排名前十的高频高中危漏洞如图 6 所示。



(a) 前十高频高危漏洞　　(b) 前十高频中危漏洞

图 6　排名前十的高频高中危漏洞

5 结束语

本文提出的移动应用全生命周期管理平台是现有移动互联网发展中，针对移动应用安全现状的充分分析，借鉴软件行业中的全生命周期理念所提出并完整落地实现的一种移动应用安全管理的实施方案，也是集团公司“降本增效”要求的具体实践。本管理平台在开发和使用过程中紧跟当前先进的理念和热门的技术，力求在当前移动应用安全越来越受到重视的情况下，通过相关技术的研究以及落地实现，为运营商及其客户的移动应用安全保驾护航。

未来，移动互联网及移动应用的发展依旧会十分迅速，因此移动应用全生命周期管理平台的发展也将持续推进。在 Web3.0 时代，新旧技术的交替不可避免，管理平台的发展不仅要尽量满足当前状况下的移动安全问题，对于正在演进以及未来可能会对移动安全产生影响甚至是变革的理念和技术，也要充分研究并在管理平台接下来的发展中得以体现。

参考文献：

[1] 孙侃. 移动应用 App 全生命周期安全管理[J]. 现代电视技术, 2018, 207(9): 139-142.
SUN K. Security management of mobile app lifecycle[J]. Modern Television Technology, 2018, 207(9): 139-142.

[2] 王渭清, 陈军, 薄明霞. 电信运营商应用软件安全开发生命周期管理[J]. 电信科学, 2011, 27(Z1): 291-294.
WANG W Q, CHEN J, BO M X. Application software security development lifecycle management of telecom operators[J]. Telecommunication Science, 2011, 27(Z1): 291-294.

[3] 刘长建. DevSecOps 的一些关于企业安全的思考[J]. 计算机与网络, 2017(19): 54-55.
LIU C J. Some thoughts on enterprise security of DevSecOps[J]. Computer and Network, 2017(19): 54-55.

[4] 张松, 林树顺. 基于云平台的安全移动应用研究与实践[Z]. 电力行业信息化年会, 2014.
ZHANG S, LIN S S. Research and practice of secure mobile application based on cloud platform[Z]. Annual Meeting of Power Industry Informatization, 2014.

[5] SCTTO B. How a zero trust approach can help to secure your AWS environment[J]. Network Security, 2018(3): 5-8.

[6] 蒋绍林, 王金双, 张涛, 等. Android 安全研究综述[J]. 计算机应用与软件, 2012(10): 211-216.
JIANG S L, WANG J S, ZHANG T, et al. Overview of Android security research[J]. Computer Application and Software, 2012(10): 211-216.

[7] 管东升, 李浩铭. 信息化软件项目全生命周期管理研究[J]. 项目管理技术, 2012(12): 97-102.
GUAN D S, LI H M. Research on lifecycle management of information software project[J]. Project Management Technology, 2012(12): 97-102.

[作者简介]

殷铭（1994– ），男，中国电信股份有限公司研究院应用安全研究所安全研究员，主要研究方向为移动应用安全、信息安全、云计算和人工智能等。

李琳（1994– ），女，中国电信股份有限公司研究院应用安全研究所安全研究员，主要研究方向为移动 App 的安全。