浅谈应用 APP 全生命周期用户个人隐私安全保护的研究

王　琪　康雅萍　王升元
（中国移动内蒙古有限公司，内蒙古 呼和浩特，　010090）

摘要：近年来，手机 APP 过度索权、超范围收集个人信息的现象大量存在，APP 的个人隐私安全问题面临着严峻挑战。为了更好地保障个人隐私安全，本文分析了 APP 个人隐私安全存在的缺少统一监督检查标准和规范、没有完善的 APP 管理流程和组织体系、个人隐私检测能力不足的问题。通过对移动应用 APP 全生命周期用户个人隐私安全保护的研究，对分析的问题提出针对性的建议。

关键词：APP 个人隐私保护；安全检测；安全管理

一、引言

随着移动互联网相关技术的快速发展和应用，我国移动设备和智能终端占据市场规模份额持续增长，移动互联网应用程序（Application，APP）得到广泛应用，在促进经济社会发展、服务民生等方面发挥了不可替代的作用。据国家互联网应急中心统计，我国境内应用商店数量已超过 200 家，上架 APP 近 500 万款，下载总量超过万亿次，发展势头迅猛。但 APP 背后的个人隐私安全问题也日益突出，严重危害信息安全和移动互联网健康发展。在此严峻形势下，中央网信办、工信部、公安部、市场监管总局在全国范围内针对 APP 强制授权、过度授权、超范围收集个人信息等突出问题，组织开展 App 违法违规收集使用个人信息专项治理，对 APP 个人隐私保护提出更高要求，也给 APP 运营单位带来极大挑战。

二、APP 安全需求分析

（一）相关部委的安全监管要求

伴随着移动互联网的快速发展、国家网络安全法规日益完善，《中华人民共和国网络安全法》系统确定了国家、主管部门、网络运营者、网络使用者等主体的网络安全责任，确立了保障网络产品和服务安全、网络运行安全、网络信息安全等基本制度。相关部委监管部门先后发布了《关于开展 App 违法违规收集使用个人信息专项治理的公告》等多项要求和规范，并连续三年开展专项治理行动。因此，APP 安全具有自上而下的监管需求。

（二）运营单位面临的 APP 安全防护需求

移动互联网应用作为用户数据收集的主要入口之一，APP 运营单位掌握了大量的用户信息，一旦信息泄露，将带来巨大经济损失和严重的社会负面影响。因此 APP 运营单位存在 APP 安全保障需求的内部驱动力。

（三）APP 使用者的安全诉求

随着大数据、人工智能的快速发展和应用，APP 搜集用户信息的规模不断扩大，个人信息窃取成为网络违法活动的，用户个人信息盗取和倒卖的案件时有发生。随着国家普法进程的加快，国民自我保护意识加强，信息安全防护意识提高，对 APP 的使用需求不再单一停留在业务功能层面，安全因素逐步成为考量标准之一。

面临上述三方面的安全需求驱动力，APP 生产和运营单位需要提高 APP 防护能力，加强内部监管。

三、研究过程

（一）APP 生产和运营单位面临困境分析

1. 在移动互联网环境下， APP 集成厂商众多，运营人员难以管控每个业务逻辑，容易出现对集成功能模块把关不严格的现象。

2. 移动互联网市场瞬息万变，APP 用户需求不断变化导致版本迭代频繁，开发厂商需要兼顾快速上线和安全防护的双重需求，但安全防护工作往往滞后于应用快速迭代。

3. 对业务下线缺少报备流程监督，APP 从立项规划、建设开发、上线报备、运行监测到下线管理整个流程难以实现管理闭环。

（二）解决方向

1. 根据国家 APP 专项治理小组下发的《APP 违法违规收集使用个人信息自评估指南》，并结合监管政策标准和法律法规，整合统一的检查标准和规范。

2. 将相关防护要求纳入安全管理流程，建立 APP 主动防御管理体系，明确应用需求、运营、管理等多个部门的责任划分，出具详细职责管理规范。

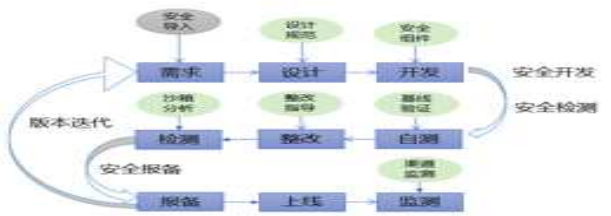
3. 通过建设 APP 安全保障平台，实现对 APP 进行个人隐私安全专项指标实时动态监测。

4. 开发核心安全能力组件，形成安全 SDK，实现安全开发能力的有效积累和标准化推广。

四、移动应用 APP 个人隐私闭环管理体系和支撑技术应用研究

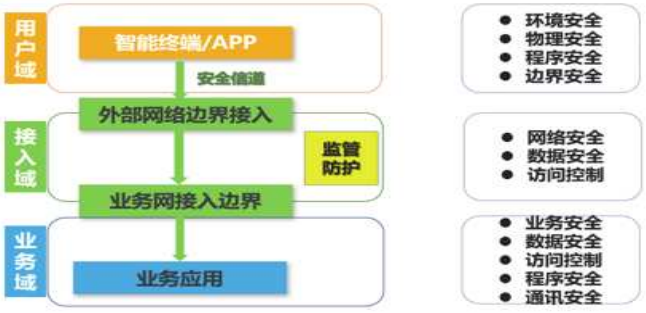
在 APP 整个生命中，存在设计、开发、检测、报备、发布和下线的环节，安全防御工作介入的越早，安全事件发生机会越少，造成的损失越小。因此可将 APP 安全防御工作前置，在设计阶段同步植入安全要素，利用 IT 技术支撑安全运营工作，掌握 APP 全生命周期安全状态。通过安全设计有规范、安全开发有保障、安全检测有手段、安全报备有渠道、安全发布有监管的管控思路，加强 APP 安全管控力度，构建 APP 闭环安全管理体系。

安全管理工作，强调管理与技术并重，流程与能力融合。通过建立 APP 发布、更新报备机制，形成 APP 应用与版本、样本间的映射关系，将信息化技术和能力嵌入管理流程。



（一）形成基于分级分域的安全设计规范和开发指南

遵照等级保护管理思想，对 APP 应用及后台信息系统进行分级分域安全防护，根据 APP 应用及业务的特点划分安全域和相应设计要求，指导业务部门、APP 开发厂商在 APP 设计阶段引入安全思想和设计要求；针对应用开发环节，依据安全设计的安全架构方案，在开发团队中贯彻安全开发指南，落实安全设计。



通过建立和发布一套根据国家部委等检测规范要求，结合 APP 个人隐私安全现状特点，定义 APP 应用检测指标要求，覆盖程序安全、业务安全、通信安全等维度，明确定义指标规范和风险等级的 APP 个人隐私安全管理制度规范。

形成 APP 个人隐私安全风险管控机制，贯穿 APP 安全设计、安全开发、安全检测、安全加固及安全认证等全生命周期的关键环节，以此实现 APP 个人隐私安全规范“发布－执行－反馈－改进”的闭环管理流程。

（二）建立 SDK 安全组件库

为提高 APP 开发效率，实现业务的快速迭代，APP 生产厂商经常会用到软件开发工具包（Software Development Kit）。通过开发核心安全能力组件，形成安全 SDK，并对引用的第三方 SDK 进行管理，将第三方 SDK 上传、下架等录入管理流程。同时将 SDK 安全组件嵌入到上线 APP 中，包括：安全键盘 SDK，用来加密键盘事件通信数据，防止外部程序非法监听键盘窃取隐私数据；数据加密 SDK，对核心能力进行加密，保护 APP 本地隐私数据加密存储等，实现 APP 安全能力的有效积累和标准化推广，帮助 APP 快速提升底层个人隐私安全防护能力。通过组件化和标准化的安全能力框架，形成 APP 安全开发快速迭代能力。

（三）自动检测技术

依据国家 APP 专项治理小组下发的《APP 违法违规收集使用个人信息自评估指南》对 APP 全生命周期用户个人隐私进行检测，将评测指南中的个人隐私安全的 6 大类 28 个专项指标配置为检测项。

在报备流程前的自测和检测流程中，利用 APP 逆向工具生成 Smali 文件，再运用全文件检索技术，实现个人隐私安全专项指标中静态指标的自动分析。从代码、行为和数据三个维度，形成特征映射，比对分析发现检测问题，并自动生成检测结果，实现对 APP 个人隐私安全问题的初步检测和基础防护。

（四）利用沙箱进行动态行为分析

部分 APP 虽然制定了隐私政策，但仍存在着隐私政策描述不清晰、不完整的问题，APP 在运行中出现违规收集用户隐私的情况。根据中国消费者协会发布的《100 款 APP 个人信息收集与隐私政策测评报告》显示，91 款 APP 列出的权限涉嫌“越界”，越界违规获取了定位、通讯录、摄像头等信息 APP 占总比 91%。

在报备评测中可利用沙箱监控 APP，对报备 APP 在进行动态行为的监测，如越权操作、敏感访问等。通过动态行为测试，对 APP 进行动态行为的检测和记录，进一步分析 APP 个人隐私安全专项指标中的动态指标，包括收集、使用个人信息是否遵循合法、正当、必要的原则，是否明确收集、使用信息的目的、方式和范围，处理个人信息是否遵循“最小够用”原则等。根据检测结果，生成个人隐私安全专项指标测试结果，作为整改依据。

五、总结

随着移动互联网应用程序数量不断增长，APP 的个人隐私安全需求越来越高。本文首先分析了 APP 个人隐私安全存在的缺少统一监督检查标准和规范、没有完善的 APP 管理流程和组织体系、个人隐私检测能力不足、开发厂家能力不足等问题，提出建立通过 APP 运营单位建立 APP 闭环管理流程，解决规范和检查标准问题，利用技术手段对 APP 进行静态、动态检测，实现安全管理有体系、安全设计有规范、安全开发有保障、安全评测有手段、安全发布有监管的管控思路。

APP 用户个人隐私安全保护工作，是一项不断探索的综合性研究工作，需要以“管技并重”的思想，引入新技术、新手段到管理流程中，支撑 APP 安全开发和安全运营。同时不论是运营商、企业、开发者还是个人用户，都应提高安全防护意识。

参考文献：

[1] 王飞 . 移动互联网 IT 环境下 APP 安全管理技术研究及应用 [J]. 网络空间安全，2019，10（05）：121-125.

[2] 徐建光 . 隐私政策视角下移动政务 APP 用户个人隐私保护评价研究 [D]. 武汉大学，2020.

[3] 殷铭，虞珍妮，闻剑峰 . 移动应用全生命周期管理平台中的标准应用实践 [J]. 信息技术与标准化，2022（05）：135-138+144.

作者简介：

王琪，男，1981 年 11 月出生，2005 年毕业于大连民族学院，大学本科，现任职于中国移动内蒙古有限公司信息技术部，高级工程师，主要从事 IT 支撑网规划、项目管理等工作。

康雅萍，女，1988 年 11 月出生，2013 年毕业于北京科技大学，硕士研究生，现任职于中国移动内蒙古有限公司信息技术部，高级工程师，主要从事 IT 规划、项目管理等工作。

王升元，男，1974 年 3 月出生，2010 年毕业于中国科学院研究生院，硕士研究生，现任职于中国移动内蒙古有限公司信息技术部，高级工程师，主要从事 IT 规划、项目管理等工作。