CAICT 中国信通院　Tencent 腾讯

软件开发包（SDK）安全研究报告

（2021 年）

中国信息通信研究院安全研究所
深圳市腾讯计算机系统有限公司

2021 年 12 月

版权声明

编制说明

本报告的编制获得深圳市腾讯计算机系统有限公司以下团队的支持，在此一并感谢（排名不分先后）:

前　言

近年来，随着移动互联产业的兴起，移动应用软件（Application，App）逐渐渗透到社会生活的各个领域，为大众提供精细化场景化服务。在面向细分领域发展的同时，App 种类和数量呈爆发式增长，软件开发工具包（Software Development Kit ，SDK）被广泛集成、应用，为日益丰富的 App 功能、服务提供了技术上的解决方案。

数字经济时代下，移动应用场景迅速扩展，SDK 逐步成为移动业务价值拓展的重要组成部分。然而，由于 SDK 具有泛用性、灵活性等特点，一旦出现安全问题，不仅自身业务受到直接影响，也会威胁到集成 SDK 的 App 业务安全和数据安全，严重的情况下甚至可能影响移动应用系统生态安全。随着安全形势不断变化，SDK 的安全合规问题已经进入各方视野，SDK 可能存在的安全漏洞、恶意行为，以及隐藏在 App 背后不透明地收集使用个人信息等问题逐渐成为各方关注的焦点问题。

中国信息通信研究院联合深圳市腾讯计算机系统有限公司共同研究编制本报告，报告从场景分析、数据统计、政策标准方面分享了 SDK 行业发展现状，对 SDK 行业面临的合规风险、安全风险进行了分析，面向 SDK 及 App 开发者提出了安全措施建议，并从实践角度分享案例和经验，为促进 SDK 行业生态的健康发展提供参考。

移动互联产业仍处于蓬勃发展阶段，移动应用生态安全亟需多方共同协作努力，报告不足之处欢迎批评指正。

目 录

图 目 录

表 目 录

近年来，随着移动互联产业的兴起，移动应用软件（App）逐渐渗透到社会生活的各个领域，成为线上线下数据交汇的重要节点。根据工信部《2021 年上半年互联网和相关服务业运行情况》监测数据，截至 2021 年 6 月底，我国国内市场上监测到的 App 数量为 302 万款。其中，本土第三方应用商店 App 数量 166 万款，苹果商店（中国区）App 数量 136 万款[1]。在数量迅速增长的同时，App 也进入了精细化开发阶段，软件开发工具包（Software Development Kit ，SDK）[2]帮助 App 高效率、低成本地实现各类功能，为缩短 App 开发周期提供了便利。

一、SDK 行业发展现状

SDK 为日益丰富的移动应用功能、服务提供了技术上的解决方案，App 正在成为自研、商用 SDK 的组合。一方面，部分 App 开发者通过自研 SDK 提高 App 开发、更新、维护的便利性与灵活性；另一方面，各类第三方功能、服务、接口通过 SDK 技术被广泛应用于 App 产品。

（一）SDK 应用广泛，行业发展持续活跃

1.SDK 种类繁多，场景丰富

SDK 通过专业化分工服务，帮助移动 App 快速实现业务功能、降低开发成本、缩短开发周期、有效节约资源，具有广泛的应用场景

[1] 工业和信息化部，2021 年一季度互联网和相关服务业运行情况，https://www.miit.gov.cn/jgsj/yxj/xxfb/art/2021/art_71a9adc43c2149cebcb6b527f77e654f.htmll

[2] 软件开发包，即协助软件开发的相关二进制文件、文档、范例和工具的集合。

和价值空间，与移动互联产业高度共生。按照 SDK 功能划分，目前比较成熟的 SDK 有广告类、推送类、数据统计分析类、地图类等，如表 1 所示。

表 1 常见 SDK 类型及典型供应商

序号	SDK分类	功能描述	典型供应商
1.	广告类	提供广告展示和广告相关数据分析等功能，通过使用广告 SDK，App 提供者可以在 App 中展示广告商投放的广告，进而根据最终用户的点击赚取收益	广点通、力美、友盟、TalkingData、有米、多盟等
2.	推送类	向用户推送各类消息、通知等	极光推送，个推推送，Mobpush，友盟推送，百度推送，云巴推送等
3.	数据统计分析类	提供收集最终用户与 App 之间的交互行为的功能。根据用户使用 App 的情况，开发者可以有针对性地改进 App	Appsee、Mixpanel、Google Analytics 等
4.	地图类	提供定位、优化路线、轨迹纠偏、图层绘制、AR、全景等功能	腾讯地图 SDK、百度地图 SDK、凯立德 SDK、googlemap SDK 等
5.	第三方登录类	提供通过其他账号体系(如微博、微信、QQ)等第三方账号登录 App 的功能	QQ 互联、微信开放平台、微博开放平台
6.	社交类	提供社交功能，如消息、分享、排行等功能	QQ 互联、微信开放平台、微博开放平台
7.	支付类	提供付款、财务管理、分销等功能	微信支付、支付宝、百度钱包、银联、Apple Pay、Bmob 支付 SDK、万普支付 SDK、Ping++ 支付 SDK、Beecloud 支付等
8.	Crash 监控类	提供 App 崩溃、App 无响应、卡顿的数据收集与分析	Bugly、Umeng、firebase 等
9.	人工智能应用类	人脸识别、人体识别、人像处理、文字识别、视频技术、AR 与 VR 技术、语音或拍照翻译等等海量的功能	腾讯 AI 开放平台 SDK、Face++ 旗下多款 SDK 产品、百度 AI 开放平台旗下多款 SDK 产品等

来源：公开资料整理

（1）广告类 SDK

广告类 SDK 可以为 App 开发者提供广告接入、广告监测功能，通过在开发的 App 中加入广告类 SDK，App 可以通过插屏广告、浮层广告、原生广告、激励广告等形式向用户展示广告，为开发者提供了变现和盈利的途径。

常见的广告类 SDK 包括广点通、力美、友盟、TalkingData、有米、多盟等。

（2）推送类 SDK

推送类 SDK 可以实现服务器对 App 用户推送各类消息或者通知，从而提高用户与软件的互动。各类新闻资讯软件、天气软件、社交软件、音乐软件等可通过推送类 SDK 实现推送功能，推送方式灵活多样，如通知栏通知、展示热点内容、资讯服务、版本更新、支付状态等，还可以通过定时的方式发送本地通知，无需依赖网络。除此以外，推送类 SDK 通常还具有数据统计功能，对推送数量、点击率等其他详细的数据进行统计分析。

目前主流的推送类 SDK 供应商包括极光推送，个推推送，Mobpush，友盟推送，百度推送，云巴推送等。

（3）数据统计分析类 SDK

数据统计分析类 SDK 植入 App 后，通过埋点，可以追踪到 App 所有的页面的进入、退出、点击等行为动作，并通过数据化图表等多种形式进行数据统计。数据统计分析类 SDK 被 App 开发者用于分析用户行为、更新完善产品，以提高用户体验，而 App 用户对此类 SDK

的存在几乎难以察觉。

常见的数据分析类 SDK 包括 Appsee、Mixpanel、Google Analytics 等。

（4）地图类 SDK

部分 App 在用户使用时需要调用地图功能，例如某网约车 App 使用某电子地图厂商的地图类 SDK，即可调用相关地图信息及服务。地图类 SDK 主要围绕地图功能，可以提供定位、优化路线、轨迹纠偏、图层绘制、AR、全景以及调用其他各种地图数据等服务。

常见的地图类 SDK 包括腾讯地图 SDK、百度地图 SDK、凯立德 SDK、googlemap SDK 等。

（5）第三方登录类 SDK

第三方登录类 SDK 可提供其他服务的账号登录功能，如 App 或网站可通过使用 QQ 互联提供的 SDK，实现用户使用 QQ 账号登录 App 或网站的功能。

目前常见的第三方登录类 SDK 包括 QQ 登录、微信登录以及微博登录等。

（6）支付类 SDK

在使用 App 时，用户经常需要在购买会员或服务等支付场景使用支付宝或者微信支付进行付款，支付类 SDK 集成于 App 内实现产品的付款功能。此类场景下常用的支付类 SDK 有支付宝、微信、百度钱包、银联、Apple Pay 等。

此外，许多公司在上述 SDK 的基础上开发比如聚合支付平台等

新的 SDK 产品，以实现财务管理、多级分销、多门店分销等功能，多元化地满足商户和消费者的支付需求。常见的此类 SDK 包括 Bmob 支付 SDK、万普支付 SDK、Ping++支付 SDK、Beecloud 支付 SDK 等。

（7）Crash 监控类 SDK

Crash 监控类 SDK 可以为移动 App 开发者提供专业的异常上报和运营统计等功能，帮助开发者快速发现并解决异常，同时掌握产品运营动态，及时跟进用户反馈。

目前常见的 Crash 监控类 SDK 包括 bugly、Umeng、firebase 等。

（8）人工智能应用类 SDK

人工智能应用类 SDK 可以实现人脸识别、人体识别、人像处理、文字识别、视频技术、AR 与 VR 技术、语音或拍照翻译等功能。人脸识别方向的 SDK 可以进一步应用于智慧安防、智慧零售等场景；文字识别方向的 SDK 可以帮助判断身份证照片是否清晰可使用、是否存在遮挡等情况，从而采集规范的身份证照片，被广泛用于银行、保险等行业。

常见的人工智能应用类 SDK 包括腾讯 AI 开放平台 SDK、Face++旗下多款 SDK 产品、百度 AI 开放平台旗下多款 SDK 产品等。

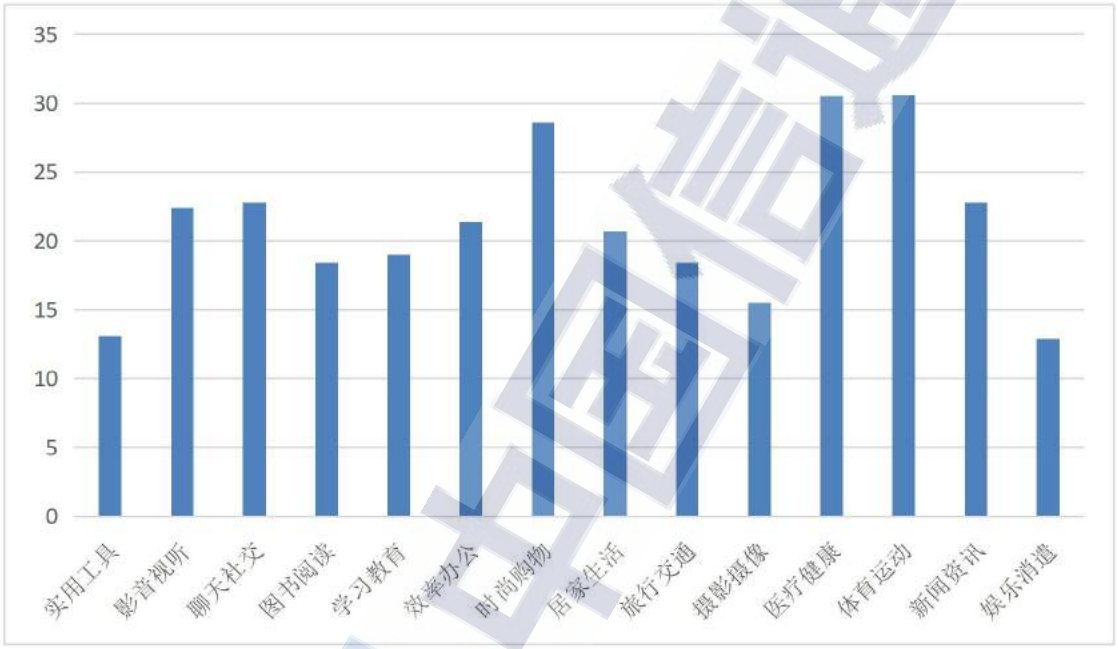
2.App 集成多款 SDK，形成共生关系

SDK 已经成为移动应用生态中的重要一环，开发者、运营者出于开发成本、运行效率考量，在 App 开发设计过程中普遍使用自研或第三方 SDK 简化流程、节约资源，且一款 App 通常集成多款 SDK，

互相之间形成共生关系。

（1）各类 App 平均集成 SDK 数量统计

据信通院及腾讯数据统计，目前国内一款 App 平均集成超过 20 款 SDK，其中体育运动类、医疗健康类、时尚购物类 App 平均使用第三方 SDK 数量位列前三，分别为 30.6、30.5 和 28.6。

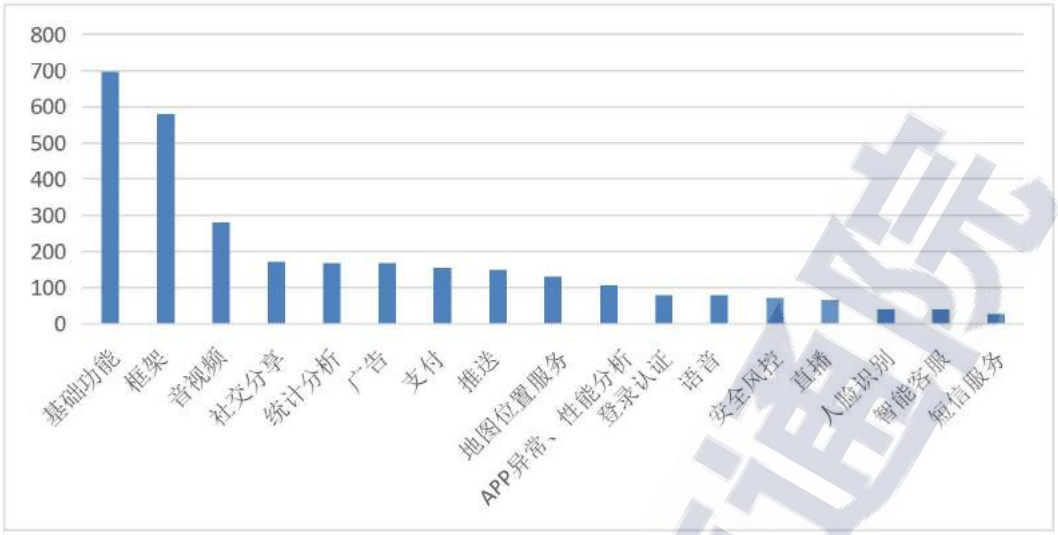


来源：中国信息通信研究院整理

图 1 各类 App 平均集成 SDK 数量

（2）App 集成第三方 SDK 的类型分布

第三方 SDK 的发展非常迅速，据统计，被 100 款以上 App 集成的第三方 SDK 代码包超过 30000 款。另外对集成次数较多的 3000 款 SDK 进行统计分析，SDK 类型及相应数量分布如图 2 所示。

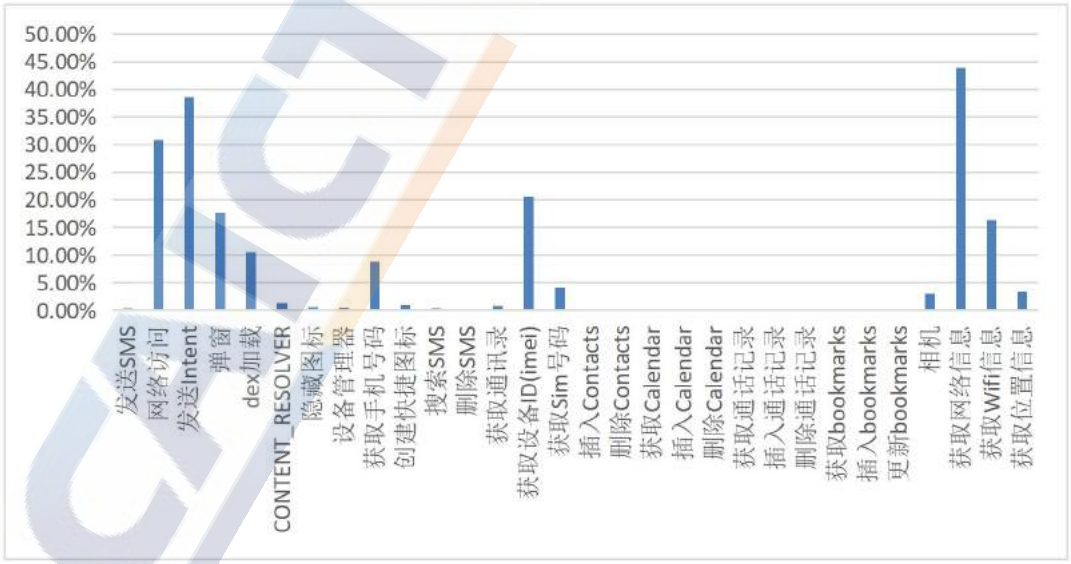


来源：中国信息通信研究院整理

图 2 集成次数较多的第三方 SDK 类型分布

（3）第三方 SDK 各类敏感行为统计

第三方 SDK 为了实现相关的功能，有可能会收集使用用户个人信息和设备信息，下图统计了各类敏感行为在第三方 SDK 中出现的情况，其中网络访问、设备 ID 获取、动态 dex 加载等行为出现的频率较高。



来源：中国信息通信研究院整理

图 3 第三方 SDK 各类敏感行为统计

（二）政策标准逐步明晰，为 SDK 安全落地提供导向

SDK 具有泛用性、灵活性等特点，与 App 存在密切联系，一旦出现安全问题，不仅自身业务受到直接影响，也会威胁到集成 SDK 的 App 业务安全和数据安全，对 App 的安全治理工作形成阻碍。目前国内关于 SDK 安全的要求主要分散在 App 相关的法律法规和标准中，SDK 的合规问题与安全风险已经进入各方视野，相关工作在持续研究和推进，并不断完善。

1.监管层面

2020 年 7 月，中央网信办、工业和信息化部、公安部、国家市场监管总局四部门启动 2020 年 App 违法违规收集使用个人信息治理工作，年度治理重点专门提到了对第三方 SDK 的治理。

2021 年 3 月 12 日，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局联合制定《常见类型移动互联网应用程序必要个人信息范围规定》，按照基本功能服务分类明确了移动互联网应用程序所需的必要信息。规定对 App 集成的 SDK 收集个人信息同样具有约束作用。

2021 年 4 月，在国家互联网信息办公室的统筹指导下，工业和信息化部会同公安部、市场监管总局起草的《移动互联网应用程序个人信息保护管理暂行规定》公开征求意见。其中，对 APP 第三方服务提供者应当履行的个人信息保护义务提出了要求。

2.标准层面

2020 年 11 月全国信息安全标准化委员会发布了《网络安全标准

实践指南—移动互联网应用程序（App）使用软件开发工具包（SDK）安全指引》（以下简称 SDK 安全指引），同期每日互动正在起草国家标准《信息安全技术 移动互联网应用程序（App）软件开发工具包（SDK）安全要求》（以下简称 SDK 安全国标）。腾讯正在牵头起草行业标准《移动应用软件开发工具包（SDK）安全使用要求》（以下简称 SDK 安全行标）。

SDK 安全指引由中国电子技术标准化研究院、腾讯等十余家企事业单位共同编写，针对当前 App 使用 SDK 过程中可能面临的 SDK 安全漏洞、恶意行为、违法违规收集使用个人信息等问题，参考当前 SDK 安全最佳实践，给出了 App 使用 SDK 的安全实践指引，旨在减少因 SDK 造成的 App 安全与个人信息保护问题。

SDK 安全国标[3]由每日互动、中国信息通信研究院、腾讯等多家企事业共同编写，主要从 SDK 的生命周期出发，提出了设计、开发、部署等环节的安全要求，同时也对个人信息保护以及 SDK 和 App 之间的联动提出了要求。

SDK 安全行标由腾讯、中国信息通信研究院、CNCERT 等多家企事业单位参与，从 SDK 应用安全角度出发，明确移动应用软件使用第三方 SDK 的安全要求，梳理常见 SDK 类型信息收集范围，增强恶意 SDK 的识别、检测和防范能力。

除上述一般标准或规范之外，金融行业也针对 SDK 制定了《个人金融信息保护技术规范》《移动金融客户端应用软件安全管理规范》

[3] 由于 SDK 安全国标及安全行业标准目前尚未正式发布，对于具体内容在此不再分析。

等具有行业特色的标准，内容主要包括:

- 授权同意: 使用 SDK 收集处理个人金融信息时，应确保 SDK 经过信息主体授权。
- 安全评估: 通过 SDK 实现个人金融信息的共享转让，应定期检查或评估 SDK 的安全性和可靠性，并留存检查评估记录; 若委托第三方 SDK 对个人金融信息进行处理，应对 SDK 开展技术检测。
- 交易记录: 使用 SDK 对外提供金融交易服务，应记录 SDK 信息及引用该 SDK 的外部应用信息。

二、SDK 的合规风险

SDK 能够帮助 App 开发者在无需了解技术细节的情况下快速实现特定功能，但也导致其开发、运营具有一定封闭性，用户和 App 开发者难以完全掌握第三方 SDK 收集使用个人信息的范围、方式、用途等。如果 SDK 收集使用个人信息方面存在合规风险，App 集成 SDK 并应用时将对用户个人信息构成威胁。

(一)SDK 收集使用个人信息的合规风险分析

1.SDK 未经用户同意收集个人信息

SDK 通常无法独立展示前台页面，其告知行为往往需要借助宿主 App 传达给用户，但由于部分 SDK 未向 App 告知或完整告知自身所收集的个人信息，或者 SDK 公开了收集使用规则但 App 未向用户明示等原因，使得用户对 SDK 收集个人信息行为毫无感知。还有部

分 SDK 未经用户同意，私自调用权限隐蔽收集个人信息，私自通过自启动、关联启动等方式收集个人信息。SDK 未经用户同意收集个人信息，不仅增加了自身的违规风险，也会为宿主 App 制定收集使用规则，全面列举收集使用的个人信息带来障碍。

2.SDK 超范围收集个人信息

SDK实际收集的用户个人信息超出公开文档所声明的系统权限和个人信息。此类行为主要表现为SDK收集与其所提供服务无关的个人信息，强制申请非必要的权限，私自调用权限隐蔽收集个人信息，私自通过自启动、关联启动等方式收集个人信息，自动收集个人信息的频度和时机不合理等。例如，部分SDK会收集非必要的设备信息、网络环境信息，读取用户设备已安装应用程序列表，甚至超范围收集用户通讯录、通话记录、地理位置等敏感个人信息。

3.SDK 未经用户授权使用个人信息

SDK 帮助 App 开发者实现登录、支付、推送、数据统计分析等业务功能，存在未经用户授权使用个人信息的合规风险。一方面，SDK 收集的个人信息可能涉及个人身份、财产等敏感信息，还可以通过 App 权限情况获得位置信息、短信信息、鉴权信息等，如果未经用户授权使用，有可能严重损害用户权益。另一方面，第三方 SDK 可能被各行业各类型的 App 集成，从而汇集多款 App 用户个人信息，一旦相关信息被用于实施诈骗、社会工程攻击等违法行为，其危害程度较单个 App 数据滥用事件更加严重。

4.SDK 违规传输个人信息

一方面，部分 SDK 存在明文传输用户电话号码、设备 MAC 地址等个人信息，或者私自向其他应用或服务器发送、共享用户个人信息的情况，可能被宿主 App 或本地恶意程序截获，导致用户个人信息泄露。另一方面，在未经用户同意的情况下，SDK 有可能采取加密等方式私自传输收集的个人信息，如果 SDK 收集使用个人信息行为及相关信息未完全向宿主 App 告知，会为宿主 App 带来额外的合规风险。

5.App 对嵌入 SDK 的安全管理监督不足

目前许多 App 与 SDK 通过开放平台在线签署开发者服务协议来约定权利义务，然而开发者服务协议通常缺少专门约束数据安全的规定，同时 App 针对 SDK 收集个人信息行为进行技术检测存在一定难度，使得 App 对嵌入的 SDK 收集使用个人信息情况难以完全掌控，集成第三方 SDK 时容易引入个人信息合规风险。服务提供方应如何合法、合规地收集、保存、使用个人信息，App 如何对共享给 SDK 的个人信息、双方权利义务及第三方 SDK 收集使用个人信息情况等加强管理监督，正逐渐成为移动应用领域亟待解决的问题。

（二）SDK 个人信息安全合规要求的总结

不仅 App 本身收集使用个人信息的合规问题受到监督，“隐藏”在 App 中的 SDK 的合规问题也引起各方重视。对于存在收集使用个人信息行为的 SDK，SDK 服务提供者作为个人信息处理者应遵守个人信息保护方面的法律法规、政策标准，主动承担个人信息保护责任和

义务。目前国内关于 SDK 的合规要求分散在 App 相关的法律法规和政策标准中，下表梳理了部分重要文件和标准中明确对 SDK 提出合规要求的相关内容。

表 2 部分 SDK 合规相关要求

合规风险	合规要求	依据
SDK 未经用户同意收集个人信息	违规收集个人信息。重点整治 APP、SDK 未告知用户收集个人信息的目的、方式、范围且未经用户同意，私自收集用户个人信息的行为。	《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》
	以下行为可被认定为未明示收集使用个人信息的目的、方式和范围——未逐一列出 App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等	《App 违法违规收集使用个人信息行为认定方法》
	APP 第三方服务提供者应当履行以下个人信息保护义务: （一）制定并公开个人信息处理规则; （二）以明确、易懂、合理的方式向 APP 开发运营者公开其个人信息处理目的、处理方式、处理类型、保存期限等内容，其个人信息处理活动应当与公开的个人信息处理规则保持一致;	《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》
	当使用 SDK 收集个人信息时，应向用户明示所收集个人信息的目的、类型。	《App 违法违规收集使用个人信息自评估指南》
	2.1 是否逐一列出 App 收集使用个人信息的目的、方式、范围等 c)如嵌入的第三方代码、插件（如 SDK）收集个人信息，说明第三方代码、插件的类型或名称，及收集个人信息的目的、类型、方式。	《网络安全标准实践指南—移动互联网应用程序(App)收集使用个人信息自评估指南》
SDK 超范围收集个人信息	超范围收集个人信息。重点整治 APP、SDK 非服务所必需或无合理应用场景，特别是在静默状态下或在后	《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》

	台运行时，超范围收集个人信息的行为。	
	APP 第三方服务提供者应当履行以下个人信息保护义务: （三）未经用户同意或者在无合理业务场景下，不得自行进行唤醒、调用、更新等行为;	《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》
SDK 未经用户授权使用个人信息	违规使用个人信息。重点整治 APP、SDK 未向用户告知且未经用户同意，私自使用个人信息，将用户个人信息用于其提供服务之外的目的，特别是私自向其他应用或服务器发送、共享用户个人信息的行为。	《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》
	APP 第三方服务提供者应当履行以下个人信息保护义务: （四）采取足够的管理措施和技术手段保护个人信息，发现安全风险或者个人信息处理规则变更时应当及时进行更新并告知 APP 开发运营者;	《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》
	评估点 21：当使用 SDK 收集个人信息时，应向用户明示所收集个人信息的目的、类型。	《App 违法违规收集使用个人信息自评估指南》
	强制用户使用定向推送功能。重点整治 APP、SDK 未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为。	《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》
SDK 违规传输共享个人信息	APP 第三方服务提供者应当履行以下个人信息保护义务: （五）未经用户同意，不得将收集到的用户个人信息共享转让;	《移动互联网应用程序个人信息保护管理暂行规定（征求意见稿）》
App 对嵌入 SDK 的安全管理监督不足	9.7 第三方接入管理 当个人信息控制者在其产品或服务中接入具备收集个人信息功能的第三方产品或服务且不适用 9.1 和 9.6 时，对个人信息控制者的要求包括:	《信息安全技术 个人信息安全规范》（GB/T 35273—2020）

	a) 建立第三方产品或服务接入管理机制和工作流程，必要时应建立安全评估等机制设置接入条件； b) 应与第三方产品或服务提供者通过合同等形式明确双方的安全责任及应实施的个人信息安全措施； c) 应向个人信息主体明确标识产品或服务由第三方提供； d) 应妥善留存平台第三方接入有关合同和管理记录，确保可供相关方查阅； e) 应要求第三方根据本标准相关要求向个人信息主体征得收集个人信息的授权同意，必要时核验其实现的方式； f) 应要求第三方产品或服务建立响应个人信息主体请求和投诉等的机制，以供个人信息主体查询、使用。	

来源：公开资料整理

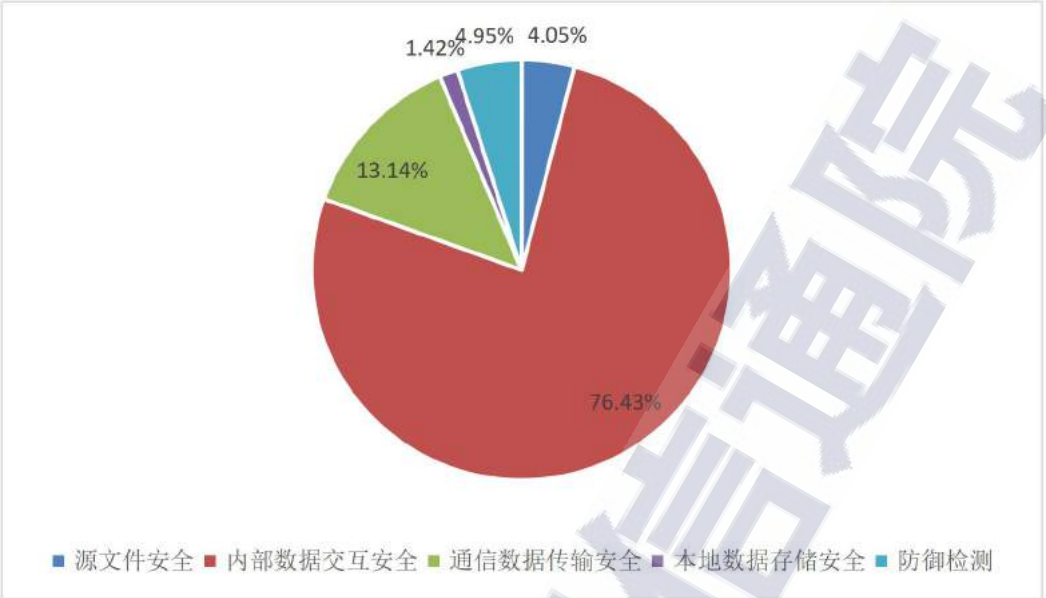
三、SDK 的安全风险

在 App 开发逐渐模块化、去中心化的趋势下，App 业务功能的实现愈发依赖 SDK，而 SDK 可能向 App 屏蔽特定功能的实现细节，其行为具有隐蔽性。一旦 SDK 出现安全问题，还会影响宿主 App 及其用户。SDK 可能存在的安全漏洞、恶意行为，以及隐蔽在 App 背后不透明地收集使用个人信息等问题逐渐成为各方关注的焦点问题。

（一）SDK 的安全漏洞问题不容忽视

SDK 在设计开发时聚焦于功能的实现，安全漏洞难以完全避免，需要通过规范安全开发流程尽量减少漏洞。按照漏洞产生的原因，通常可以将 SDK 安全漏洞划分为五类：代码源文件安全类、内部数据交互安全类、本地数据传输安全类、通信数据存储安全类和防御检测

类等，图 4 展示了这几种类型的漏洞出现的占比情况。



来源：中国信息通信研究院整理

图 4 SDK 安全漏洞类型占比

1.代码源文件安全

从代码安全层面来看，当前 SDK 的开发，主要基于苹果的 iOS 及谷歌的安卓环境。其中 iOS 环境较为封闭，在代码规范、编译方法、混淆处理等方面均有要求；而基于 JAVA 语言的安卓环境开发灵活性较大，且缺少统一的分发平台与安全审核机制，开发者可能调用敏感的安卓系统权限、使用不安全的弱加密算法，并且存在 SDK 未经加固、混淆处理即编译分发等容易引发安全风险的情况。

在 JAVA 开发环境下，SDK 一般会在编译后通过 jar 代码包的形式提供给 App 开发者。如果 App 开发者将 SDK 源代码简单封装，未对源代码进行混淆、加固处理即发布，其 Java 代码易被反编译解析，可能导致 SDK 业务执行逻辑、敏感配置、关键字段、传输通道、加解密协议等信息泄露。攻击者可以通过逆向分析和破解 SDK 核心逻

辑，进一步破坏 SDK 安全机制或者恶意篡改代码，甚至嵌入后门代码，严重威胁 SDK、宿主 App 以及用户的数据安全。

2.内部数据交互安全

在内部数据交互安全方面，SDK 也面临多重安全风险。从技术业务逻辑上看，SDK 产品作为某类业务功能的底层实现手段，为宿主 App 实现业务功能或提供推送、统计、分析等轻量附加功能，与宿主 App、系统组件、其他应用进行联调、交互，存在引发安全风险的可能性。调用系统本地浏览器组件过程中存在的安全配置问题是 SDK 本地交互中存在的典型问题之一。

另外，如果 SDK 存在组件漏洞，攻击者可以通过这些漏洞对 App 进行攻击，可能导致 App 崩溃或信息泄露等严重危害。例如某 SDK 存在可越权调用未导出组件漏洞，利用该漏洞可实现对集成该 SDK 的 APP 的任意组件的恶意调用、任意虚假消息的通知、远程代码执行等攻击。

3.本地数据存储安全

部分 SDK 在用户终端设备上创建本地数据库文件，用于存储运行所需的数据，然而 SDK 本地数据库未加密、未采取访问控制措施、敏感数据明文存储等问题较为常见。甚至有 SDK 在本地数据库中存储个人信息、资源地址等涉及用户隐私及业务安全的敏感数据，可能被不法分子通过未授权访问、越权备份等方式恶意窃取。

4.通信数据传输安全

在数据传输的安全机制方面，部分 SDK 存在使用不安全的传输

协议、数据明文传输、未验证服务器证书等风险，使得数据在传输过程中可能被截获、窃取，其中 HTTP 传输协议明文数据传输、HTTPS 协议允许任意主机名等传输环节安全问题较为突出。特别在金融证券、医疗服务等领域，涉及个人敏感信息、国家经济数据等重要数据，SDK 在关键业务数据传输环节未启用 HTTPS 双向认证机制，可能面临中间人攻击等威胁。

5.防御检测

在防御检测方面，需要对关键参数进行合法校验，关键数据的文件进行加密、合法性和完整性校验，防止被恶意利用漏洞。以 ZipperDown 漏洞为例，由于 App 使用第三方 Zip 库解压 Zip 文件的过程中没有对 Zip 内文件名做校验导致，如果文件名中含有“../”则可以实现目录的上一级跳转，进而实现 App 内任意目录的跳转和文件覆盖，攻击者便可以对应用资源、代码进行任意篡改、替换，从而实现远程代码劫持等高危操作，危害应用业务场景。

（二）SDK 的恶意行为带来隐藏风险

SDK 恶意行为会影响到 App 的安全性和稳定性，部分 SDK 为了隐蔽恶意行为，在被集成到 App 的初期不会表现出恶意行为，后续可能利用热更新机制，动态加载恶意代码，对用户的个人信息以及用户权益造成危害。典型的 SDK 恶意行为包括流量劫持、资费消耗、隐私窃取等，详见表 3。

表 3 典型 SDK 恶意行为

序号	行为名称	恶意行为
1	流量劫持	SDK信息拉取、上报和展示目标与App提供者设定的目标不同，恶意劫持App流量，可能对App造成损害。
2	资费消耗	SDK通过消耗用户网络套餐资费、恶意发送收费短信，订阅收费服务等行为，造成用户的资金损失。
3	隐私窃取	SDK在用户不知情或误导用户的情况下，隐蔽窃取用户的通讯录、短信息等个人敏感信息，隐蔽进行拍照、录音等敏感行为，并发送给恶意开发者。
4	静默下载安装	SDK在后台静默下载、安装其它恶意软件或病毒木马。
5	广告刷量	SDK在用户不知情的情况下，在后台模拟人工点击广告链接的行为来牟利。
6	恶意广告	SDK向用户推送包含欺诈内容、病毒木马的广告链接。推送过量广告，进而长期占用系统通知栏、屏幕界面，干扰用户正常使用App。
7	勒索	SDK恶意加密用户手机中的文件，干扰用户对手机的正常使用，并以恢复正常使用为由向用户勒索钱财。
8	挖矿	SDK在用户不知情的情况下利用其手机的计算能力来为攻击者获取电子加密货币，对用户设备硬件造成性能损耗。
9	远程控制	SDK在手机端启动本地后台服务器，接收远程控制端发来的控制指令，隐蔽进行上述其他恶意行为。
10	剪切板劫持	SDK对系统剪切板进行监听，获取剪切板中的敏感信息，或者根据剪切板内容的变化出发悬浮窗，干扰系统功能，欺骗用户，或者影响其他应用正常使用。

来源：公开资料整理

1.恶意 SDK 非法获取用户隐私

一些恶意开发者开始从开发恶意 App 向开发恶意 SDK 转移，利

用 SDK 能够嵌入多个 App 的特点来达到快速传播的目的，不仅非法获取用户个人信息，还可以非法控制用户手机暗刷流量变现获利。整个环节可以分为三个阶段，具体如下。

（1）制作和传播

恶意开发者开发恶意 SDK，通过与 App 签合同或者免费下载的方式集成到 App（实际案例中被感染的 App 数量可到达上千款）中，在 App 不知情的情况下接触到用户。恶意 SDK 潜伏一段时间后，恶意开发者通过使用代码分离和动态代码加载技术，从云端对包含该 SDK 的用户设备进行非法控制，具有很强的隐蔽性和对抗杀毒软件的能力。

（2）采集信息环节

在未经用户允许和用户不知情的情况下，回传用户设备信息和应用列表，作为大数据存储，并下载恶意子包潜伏在用户设备中。

（3）盈利变现

根据广告商的需求，在用户无感的情况下，通过恶意子包进行 App 拉活、广告刷量等行为。

来源：腾讯

图 5 恶意 SDK 动态更新后隐蔽执行恶意行为

2.新型物联网 SDK 黑产

黑产在硬件设备出厂前嵌入其恶意 SDK，后通过云端控制入侵家庭物联网终端，如机顶盒、路由器、手机等，窃取家庭正常 IP，构建海量的 IP 池（千万 IP）,包装成秒拨 IP 产品出售给赌博、网络水军、刷量平台、爬虫、撞库等黑灰产，难以识别和对抗。

来源：腾讯

图 6 新型物联网 SDK 黑产

四、面向开发者的安全措施建议

SDK 的安全涉及到设计、开发、分发、集成等关键环节，SDK 开发者和 App 开发者都需要关注 SDK 的安全问题，并根据自己的角色定位，评估和排查相关安全风险。

（一）面向 SDK 开发者

1.处理个人信息应满足相关法律法规要求

SDK作为个人信息处理者，应满足《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》《常见类型移动互联网应用程序必要个人信息范围规定》等相关法律法规的要求，保护用户个人信息权益，承担个人信息保护责任和义务，定期自查自纠，及时排查安全隐患。

2.将安全与合规覆盖 SDK 整个生命周期，遵循合理、最小、必要原则

安全防护是整个SDK研发团队的共同责任，需要将安全合规贯穿整个生命周期，从安全设计、安全研发、安全测试、安全运维等各个环节。SDK收集使用个人信息和申请敏感权限应遵循合理、最小、必要原则，作为个人信息共同控制者或独立控制者收集使用个人信息的第三方SDK，应向用户告知收集使用个人信息的行为并征得用户同意。

3.向 App 开发者提供合规与安全开发指南

作为被集成方，SDK开发者可通过主动向App开发者提供合规指南的方式，引导App开发者在集成并使用SDK时，采取必要的措施保

护用户个人信息安全。SDK开发者应主动向App告知SDK的相关信息，告知的信息应完整、准确、及时，不存在故意隐瞒、欺骗等行为。

4.与 App 开发者约定双方在个人信息保护方面的责权

可通过在线开发者协议或者合同等形式，明确SDK收集的个人信息类型、申请的敏感权限、个人信息的使用目的、保存期限、以及向App提供的个人信息类型等，明确双方在个人信息保护方面分别应采取的措施、承担的责任和义务等。当双方存在重大变更时，应重新达成合作协议。

（二）面向 App 开发者

1.遵循合法、正当、必要的原则选择 SDK，建立 SDK 安全规范

App开发者应遵循合法、正当、必要的原则，使用提供者基本信息明确、沟通反馈渠道有效的第三方SDK。针对SDK的引入、使用、运维到退出全生命周期中可能面临的安全风险进行全面分析，制定SDK安全规范，降低因引入SDK带来的安全风险。

2.依法依规处理与 SDK 相关的个人信息

应按照相关法律法规的要求，向用户告知所接入的第三方SDK的名称或类型，第三方SDK收集的个人信息类型、收集目的及使用方式、申请的敏感权限、申请目的及使用方式等，并征得用户同意。建议在停用某第三方SDK后，及时从App中移除该第三方SDK的代码和调用该第三方SDK的代码，存在通过本App共享或收集个人信息的，应敦

促第三方SDK提供者按照合作协议约束，删除从本App共享或收集的个人信息或做匿名化处理。

3.完善合作协议，动态监测 SDK 安全性

完善与第三方SDK提供者的合作协议，明确双方在个人信息保护方面分别应采取的措施、承担的责任和义务等。对集成后的第三方SDK进行持续动态监测或定期进行安全评估。对于已经发现的第三方SDK安全漏洞及时修复，或者采用其它替代方案，并从官方渠道及时更新SDK。对于已经发现存在恶意行为的第三方SDK，及时停止使用。

附录一 SDK 安全实践

（一）信通院发起 SDK 安全专项行动

2021 年 6 月，中国信息通信研究院安全研究所大数据应用与安全创新实验室（以下简称实验室）发起“SDK 安全专项行动”，实验室始终紧跟信息技术发展趋势，依托在数据安全、移动应用安全等领域技术能力和实践积累，积极开展前瞻研究和实践探索，形成完整的 SDK 安全评测方案和评测指标体系。

1.SDK 安全评测范围

（1）评测对象为安卓（Android）系统 App 集成的 SDK 产品，包括企业自研自用的 SDK 以及第三方 SDK 产品。

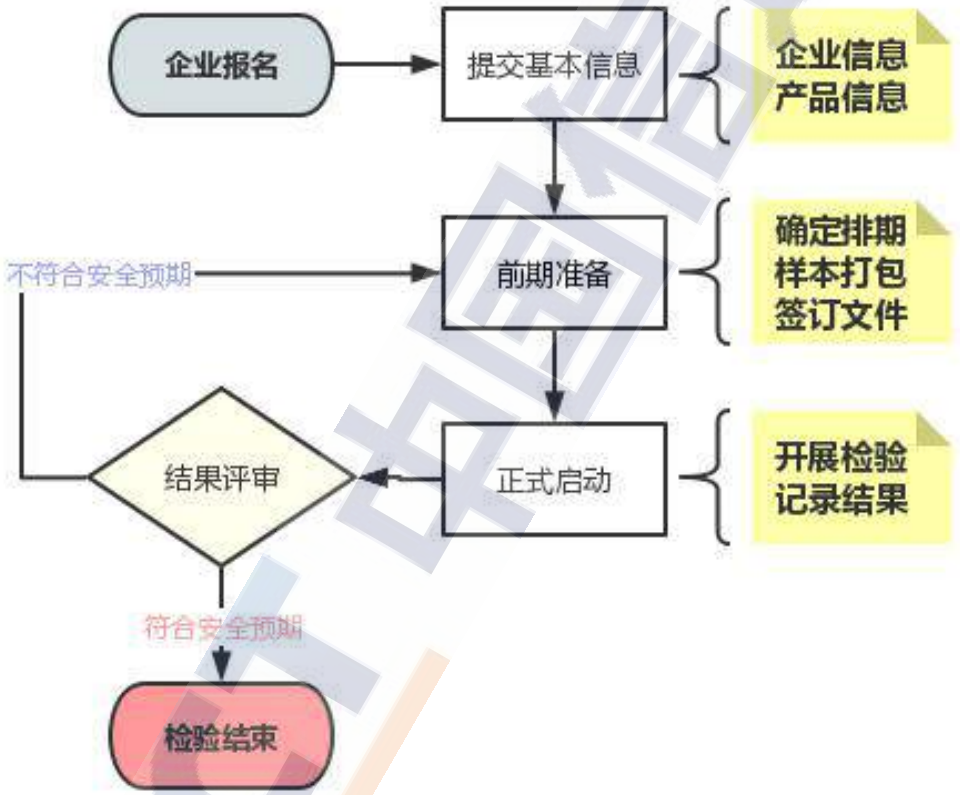
（2）评测范围主要覆盖 SDK 数据安全存储、数据安全交互、关键组件安全、代码及资源文件安全防护等方面。评测方案由实验室依据相关国家以及行业标准制定。

来源：中国信息通信研究院

图 7 SDK 安全专项行动评测范围

2.专项行动进展

专项行动已顺利完成一期和二期评测，共 13 款 SDK 产品通过评测，并于 11 月启动三期评测。技术评测在实验室搭建的标准化测试环境中进行，评测名单和证书可通过**信通院官网**和**大数据应用与安全创新实验室微信公众号**查询[4]。



来源：中国信息通信研究院

图 8 评测流程

[4] 信通院大数据应用与安全创新实验室 SDK 安全专项行动 第一期通过评测企业及名单&评测证书信息 https://mp.weixin.qq.com/s?__biz=MzkwODI0OTQ3MQ==&mid=100000406&idx=1&sn=ece18fc1322e13a0fdd3dc8a2d17d708&scene=19#wechat_redirect

3.下一步行动计划

实验室“SDK 安全专项行动”将定期开放 SDK 安全评测，帮助 SDK 开发者、使用者预先发现 SDK 自身存在的安全问题，提早部署防范措施。有意向参与 SDK 安全专项行动的企业，可通过信通院官网及大数据应用与安全创新实验室微信公众号跟踪动向。

实验室诚邀业界同仁参与本项目，汇集多方智慧，推动建立标准化的 SDK 安全评测流程与评测环境，强化 SDK 开发、集成、应用的安全性，提高行业 SDK 安全评测工作准确性、高效性、权威性，推动移动互联网行业健康有序发展。

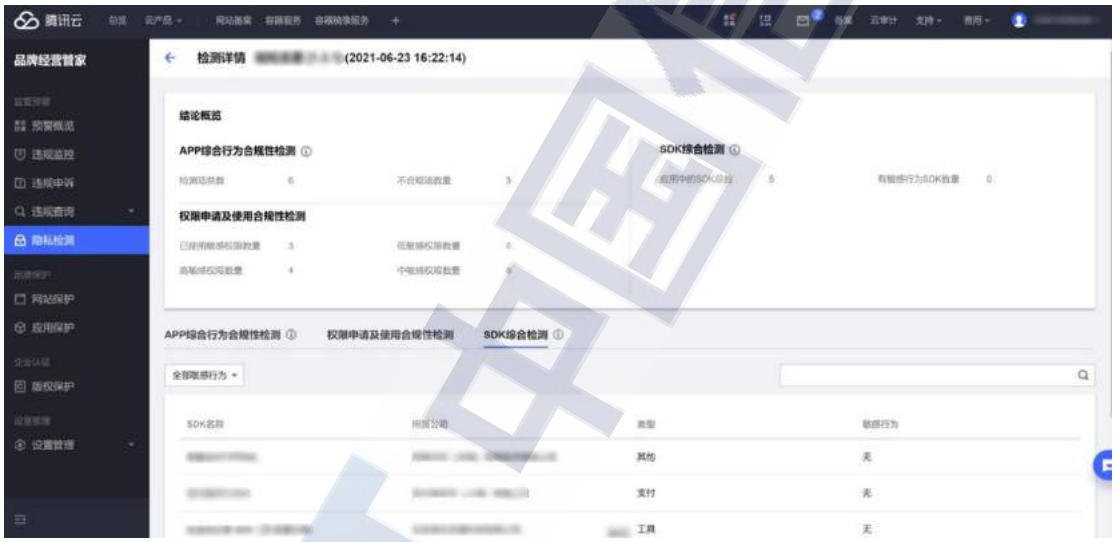
（二）腾讯探索 App 及 SDK 合规解决方案

1.腾讯云移动合规检测平台

腾讯云App隐私合规检测产品支持App及其集成的第三方SDK相关的安全和隐私合规检测。APK隐私检测目前针对相关单位发布的规范、文件等进行自动化检测，辅助以人工审核的方式，识别APK是否存在不合规获取用户隐私的问题。检测的方案主要基于《工业和信息化部 337号令》、《工信部信管函〔2020〕164号》、《App违法违规收集使用个人信息行为认定方法》和《个人信息安全规范》，对APK中是否存在隐私问题进行检测识别。

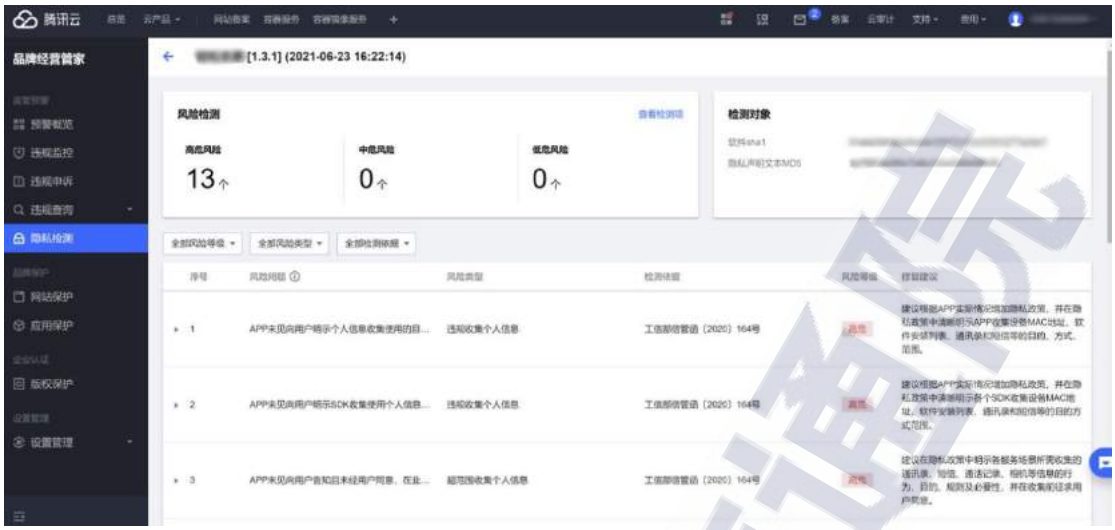
来源：腾讯

图 9 腾讯云移动合规检测平台



来源：腾讯

图 10 平台检测示例 1



来源：腾讯

图 11 平台检测示例 2

目前，可以自动化进行识别检测点主要包括:

（1）违规收集个人信息

App、SDK未告知用户收集个人信息的目的、方式、范围且未经用户同意，私自收集用户个人信息的行为。

（2）超范围收集个人信息

App、SDK非服务所必需或无合理应用场景，特别是在静默状态下或在后台运行时，超范围或超频次收集个人信息的行为。

（3）违规使用个人信息

App、SDK未向用户告知且未经用户同意，私自使用个人信息，将用户个人信息用于其提供服务之外的目的，特别是私自向其他应用或服务器发送、共享用户个人信息的行为。

（4）强制用户使用定向推送功能

App、SDK未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为。

（5）强制、频繁、过度索取权限

App安装、运行和使用相关功能时，非服务所必需或无合理应用场景下，用户拒绝相关授权申请后，应用自动退出或关闭的行为。短时长、高频次，在用户明确拒绝权限申请后，频繁弹窗、反复申请与当前服务场景无关权限的行为。未及时明确告知用户索取权限的目的和用途，提前申请超出其业务功能等权限的行为。

（6）频繁自启动和关联启动

App未向用户告知且未经用户同意，或无合理的使用场景，频繁自启动或关联启动第三方App的行为。

（7）账号注销难

App未向用户提供账号注销服务，或为注销服务设置不合理的障碍。

2.腾讯灵犀隐私保护平台

腾讯灵犀隐私平台依托公司内部安全实验室能力，构建全网百万级 SDK 标准样本库，基于代码特征学习匹配算法及大数据分析能力，对 SDK 进行分析和检测。从而可通过技术扫描并识别出 App 内集成的 SDK 包名、及 SDK 在全网范围内的个人信息采集和上传表现。

灵犀搭建专门的 SDK 配置库及合规库，为 App 匹配生成符合法规要求、格式标准的第三方 SDK 目录，一键解决第三方 SDK 合规披露的诸多风险。

通过技术的检测，灵犀帮助腾讯自研 SDK 验证采集个人信息的类型、时机和频次，并按照法律法规、国家标准等合规要求指导产品进行优化，同时通过内部通知途径，将 SDK 的合规版本通过宿主列表一键推送给 App，实现高效双向合规。

附录二 SDK 安全关键技术

（一）SDK 研发环境

SDK 的研发环境和底层依赖与 App 开发基本一致，区别在于 SDK 开发的是实现某特定功能的模块，可以被其他 App 集成并使用。

SDK 的分发可以采用编译好的 Jar 包、ARR 包或源代码分发等多种方式。一般商用的 SDK 都会采用编译好的 Jar 包、ARR 包的分发方式，从而尽可能地保证 SDK 源代码不被泄露和篡改。

（二）SDK 安全防护技术

SDK 的安全防护主要目的保护自身功能的核心逻辑不被恶意破解和篡改，因此针对 SDK 自身的防护技术主要包括：代码混淆、代码加密、SO 加固等。

代码混淆是指将程序的代码转换成一种功能上等价、但是难以阅读和理解的行为，主要包括：将代码中的各种元素，如变量、函数、类的名字改写成无意义的名字；重写代码中的部分逻辑，如将 for 循环改写成 while 循环，将循环改写成递归，精简中间变量等。

代码加密是指将程序的核心代码通过加密的方式存储成文件，当 App 运行时，通过校验并解密并加载到内存中执行，以此对核心逻辑进行保护。

SO **加固**是指将部分核心的算法逻辑放到 native 层实现，然后使用 SO 文件保护技术如加壳、VMP 等方式对核心逻辑进行保护。

（三）SDK 安全检测技术

SDK 安全检测可以从来源安全性、代码安全性以及行为安全性等方面开展。

来源安全性检测可通过检查 SDK 提供者的基本信息、SDK 提供者的沟通反馈渠道、SDK 隐私政策链接地址、SDK 提供者的安全能力、SDK 的基本功能、SDK 的版本号、SDK 的安全性自评估报告等方面开展。

代码安全性检测包括但不限于：是否存在已知的恶意代码；是否存在已知的安全漏洞；是否申请敏感权限；是否嵌入了其他第三方 SDK 等。

行为安全性检测包括但不限于：敏感行为产生的场景和频次；索取敏感权限的场景和频次；调用的敏感权限和频率；收集的个人信息类型和频率，以及必要性；个人信息回传服务器域名、IP 地址、所在地域；是否存在热更新行为及热更新是否可主动关闭；传输数据是否加密；是否存在单独收集用户个人信息的界面；SDK 是否会共享个人信息类型给第三方等。

附录三 常见 SDK 安全风险

安全风险名称	安全风险描述
Web 组件远程代码执行漏洞	App 使用 Android 系统提供的 WebView（android.webkit.WebView）对象访问任何网络 url，在同时满足以下条件均可导出远程代码执行漏洞： 1）设置属性 setJavaScriptEnabled(true); 2）通过 addJavascriptInterface API 导出接口与 js 交互(Android < 4.2); 3）未移除系统默认注册导出的对象(searchBoxJavaBridge_/accessibility/accessibilityTraversal)
Content Provider 组件数据泄露漏洞	Andriod 应用对外暴露的 Provider 组件，支持通过 URI 查询关联的应用数据。应用的 Provider 组件对传入的 uri 参数未做严格校验，导致当恶意用户传入../../../../等路径时，可以遍历系统的目录下的文件，包括该应用私有目录下的所有隐私文件
Activity 组件隐私泄露漏洞	Android 应用的内置浏览器（加载 url，并在应用内打开）支持 file 伪协议，用于打开本地 html 文件。典型场景是接收文件后在聊天窗口中打开文件。应用未对 file 协议进行限制，允许其加载本地的 js 脚本，则可导致应用的所有隐私数据被窃取，并上传到远程服务器。 1）Activity 组件支持加载 url 2）支持 file 伪协议加载本地 html 3）未对所加载文件的路径或文件属性等做校验 4）未限制执行 js 脚本
Manifest 不安全属性配置风险	android:allowBackup Whether to allow the application to participate in the backup and restore infrastructure. If this attribute is set to false, no backup or restore of the application will ever be performed, even by a full-system backup that would otherwise cause all application data to be saved via adb. The default value of this attribute is true. 允许通过 adb 命令对应用目录进行拷贝; android:debuggable Whether or not the application can be debugged, even when running on a device in user mode — "true" if it can be, and "false" if not. The default value is "false".
源码泄漏漏洞	代码混淆率较低，建议使用 Proguard 等工具对源码进行进一步混淆，避免造成源码泄漏。
随机数加密破解漏洞	Android 4.4 之前版本的 Java 加密架构(JCA)中使用的 Apache Harmony 6.0M3 及其之前版本的 SecureRandom 实现存在安全漏洞，具体位于 classlib/modules/security/src/main/java/common/org/apache/harmony/security/provider/crypto/SHA1PRNG_SecureRandomImpl.java 文件的 engineNextBytes 函数里。当用户没有提供用于产生随机数的种子时，程序不能正确调整偏移量，导致伪随机数生成器(PRNG)生成随机序列的过程可被预测
https 敏感数据劫持漏洞	应用使用 Android 系统提供的 https API 时，存在以下三种未正确实现 https 网络安全传输的情况。 1）X509TrustManager：自定义 X509TrustManager 类，但未实现严格校验（checkClientTrusted 和 checkServerTrusted 未实现） 2）setHostnameVerifier：使用 ALLOW_ALL_HOSTNAME_VERIFIER 选项或者 new HostnameVerifier 返回 true 3）WebViewClient 的 onReceivedSslError（及 SslErrorHandler 的 proceed）:

	重写 onReceivedSslError 接口，并调用 proceed()在 https 证书校验出错时继续加载
系统组件本地拒绝服务漏洞检测	Android app 注册的组件在接收异常 Intent 消息时，由于组件实现代码未对异常边界值或类型做校验，导致出现空对象引用或类型不匹配的强制类型转换，引发应用崩溃。 典型利用举例如下: adb shell am start -n 包名/组件类名 adb shell am broadcast -n 包名/组件类名 adb shell am [-n 包名/组件类名] -a actionString adb shell am startservice -n 包名/组件类名 另外，针对部分应用需在应用首次启动时动态加载功能代码等情况，可能会出现未完全加载类或某些前置环境未满足，即接收到以上消息来启动它，导致 classNotFoundException 等异常，使得应用崩溃
强制类型转换本地拒绝服务漏洞	Android app 对外暴露的组件在接收外来的 Intent 时，未对 Intent 中的参数进行严格的校验，就强制转换为某种类型。恶意 app 构造包含特殊参数的 Intent，可导致存在漏洞的应用 crash，属于本地拒绝服务漏洞
Intent Scheme URLs 漏洞	Intent Scheme URLs 攻击方式利用了浏览器保护措施的不足，通过浏览器作为桥梁间接实现 Intent-Based 攻击。相比于普通 Intent-Based 攻击，这种方式极具隐蔽性，而且由于恶意代码隐藏 WebPage 中，传统的特征匹配完全不起作用。除此之外，这种攻击还能直接访问跟浏览器自身的组件（无论是公开还是私有）和私有文件，比如 cookie 文件，进而导致用户机密信息的泄露.简而言之，该攻击能够以浏览器的权限发送 intent，属于权限泄漏问题
Activity 组件暴露风险	恶意程序通过发送 Intent 消息，可随时调用 Activity 组件，导致信息泄漏、钓鱼及应用 crash 等风险。如下命令可恶意调用对外暴露的 Activity 组件: A. 发送空 action 的 Intent 消息 adb shell am start -n 包名/组件类名 B. 发送带 action 值的消息 adb shell am [-n 包名/组件类名] -a actionString C. 发送带具体参数值的消息 adb shell am start -n 包名/组件类名（或-a actionString） --es key1 "value1" --es key2 "value2"
Service 组件暴露风险	恶意程序通过发送 Intent 消息，可随时调用 Service 组件，导致信息泄漏、应用 crash 等风险。如下命令可恶意调用对外暴露的 Activity 组件: A. 发送空 action 的 Intent 消息 adb shell am startservice -n 包名/组件类名 B. 发送带 action 值的消息 adb shell am [-n 包名/组件类名] -a actionString C. 发送带具体参数值的消息 adb shell am startservice -n 包名/组件类名（或-a actionString） --es key1 "value1" --es key2 "value2"
Broadcast Receiver 组件暴露风险	恶意程序通过发送 Intent 消息，可随时调用 Broadcast 组件，导致应用 crash、信息泄漏等风险。如下命令可恶意调用对外暴露的 Broadcast 组件: A. 发送空 action 的 Intent 消息 adb shell am broadcast -n 包名/组件类名

	B. 发送带 action 值的消息 adb shell am [-n 包名/组件类名] -a actionString C. 发送带具体参数值的消息 adb shell am broadcast -n 包名/组件类名（或-a actionString） --es key1 "value1" --es key2 "value2" 另：通过动态方式注册的普通广播接收器也是暴露的，可通过以上 B，C 测试
Content Provider 组件暴露风险	恶意程序通过访问相应的 content://... URI 可随时调用对外暴露的 Provider 组件，导致信息泄漏，应用 crash 等风险
自定义权限滥用风险	AndroidManifest.xml 中的自定义权限（permission）应使用 signature 或 signatureOrSystem 保护级别控制权限；此外 Android 系统存在自定义权限绕过的漏洞，导致有安全保护级别的 permission 也可以被任意访问，使用自定义权限保护的组件或消息应在代码层增加更多的安全校验
Intent 消息使用安全建议	恶意程序通过注册合法应用的 Intent 消息（通过 action 隐式调用）对应的组件，来接收合法应用发出的 Intent 消息，导致信息泄漏、恶意钓鱼等劫持风险。如下为 Intent 劫持测试: I. 开发第三方 poc apk，包含对所有可劫持的 Intent 广播的 action 值进行监听的 Receiver，接收广播后执行任意恶意操作; II. 在运行正常应用的同时开启 poc apk，判断是否会产生异常页面或执行非法操作
Keystore 漏洞检测	使用 Android KeyStore 密钥存储组件（android.security.KeyStore）的应用可能存在银行服务和虚拟专用网络（VPN）的密钥、信用卡信息、锁屏密码等敏感信息泄漏的风险（CVE-2014-3100）。应禁止使用该组件存储密钥数据
私有文件泄漏风险	使用 getSharedPreferences 或 openFileOutput 等 API 打开本地文件时，采用 MODE_WORLD_READABLE 或 MODE_WORLD_READABLE 选项处理，存在本地文件内容被窃取的风险。禁用 MODE_WORLD_READABLE 或 MODE_WORLD_READABLE 选项操作本地文件
第三方 SDK 漏洞	第三方 SDK 在研发代码上存在漏洞，可能导致组件权限泄露、任意文件读取或私有目录任意写入等安全问题，历史上出现过后门、强推广告、窃取隐私的 SDK，比如 Linkedme SDK 窃取账号数据、DroidBackDoor 等
AppKey 信息泄露漏洞	APPkey 和密码被硬编码在代码中，可导致数据信息泄露
目录遍历漏洞	如果 zip 包中的文件名带有"../"跳转符，而 App 解压的时候未对文件名进行校验而直接拼接存储路径，就有可能导致目录穿越，即将特定文件保存到了 APP 的私有路径
Content Provider 组件本地 SQL 注入漏洞	Android 应用的 Content Provider 组件，支持通过关联的 uri（如 content://com.example.test/keys），对应用保存在设备的私有存储数据进行访问和修改。若未对 Content Provider 组件进行权限控制，其他第三方应用可以通过关联的 authorities 和 uri 任意访问和篡改应用的私有数据，导致隐私数据泄漏和 SQL 注入等安全问题
私有目录写漏洞	Android 系统给开发者提供了内部存储、外部存储、SQLite 数据库、共享首选项等存储选项来保存应用数据。默认情况下，保存到内部存储的文件是应用的私有文件，其他应用（和用户）不能访问这些文件

	但如果在开发过程中对文件权限设置不当，即使在不具有 root 权限的情况下，其他应用也可以恶意替换、修改该应用的内部存储文件，如 db 数据库、so 文件等，导致敏感数据遭篡改、恶意代码执行等危害
Fragment 框架层注入	导出的 Preference Activity 的子类中，没有加入 isValidFragment 方法，进行 fragment 名的合法性校验，攻击者可能会绕过限制，访问未授权的界面
Scheme SQL 注入	通过 Scheme 远程 SQL 注入数据库
弱加密算法	使用弱加密算法会大大增加黑客攻击的概率，黑客可能会破解隐私数据、猜解密钥、中间人攻击等，造成隐私信息的泄漏，甚至财产损失，比如: 1. DES 弱加密算法 2. RSA 中使用到的 Padding 3. 没有安全的初始化向量 4. 使用 ECB 加密模式 5. AES/DES 密钥硬编码

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62308590

传真：010-62300264

网址：www.caict.ac.cn