电信终端产业协会研究报告

R/TAF 001-2020

移动智能终端免安装应用程序安全问题研究

Research on the security of non-installed applications of smart mobile terminal

信息安全与用户数据保护工作组（WG4）

2020 年 7 月

版 权 声 明

目　录

前　言

随着移动智能终端免安装应用程序的不断发展，其使用过程中的安全问题被越来越多的用户所关注。本研究报告阐述了移动智能终端免安装应用程序的概念、分类、框架和实现机制，重点分析研究移动智能终端免安装应用程序的安全问题，包括框架型操作系统的安全性、免安装应用程序的安全问题及标准化建议。针对这些安全问题，需要研究如何能够提高框架型操作系统的安全管控能力以及免安装应用程序自身的安全防护能力。从而促进移动智能终端免安装应用的良性健康发展。

研究单位：中国信息通信研究院、博鼎实华（北京）技术有限公司、OPPO 广东移动通信有限公司、北京百度网讯科技有限公司、深圳市腾讯计算机系统有限公司、小米科技有限责任公司、华为技术有限公司、维沃移动通信有限公司

项目负责人：董霁

项目参加人：董霁、李腾、李笑如、庞霞、周圣炎、余洪辉、王江胜

移动智能终端免安装应用程序安全问题研究

1 范围

本研究报告主要研究移动智能终端免安装应用程序的安全问题及其背景情况，包括移动智能终端免安装应用框架的分类，免安装应用发展现状和应用场景、敏感行为调用情况，以及免安装应用程序安全问题研究。

适用于移动智能终端桌面型框架型操作系统和预置的免安装应用，以及通过移动智能终端下载、使用的框架型操作系统和应用程序。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

移动智能终端 Smart Mobile Terminal

能够接入移动通信网，具有能够提供应用软件开发接口的操作系统，具有安装、加载和运行应用软件能力的终端。

3.1.2

移动智能终端操作系统 Operating System of Smart Mobile Terminal

运行在移动智能终端上的系统软件，控制、管理移动智能终端上的硬件和软件，提供用户操作界面、应用软件编程接口和其他系统服务的应用软件。

3.1.3

移动智能终端应用软件 Smart Mobile Terminal Application

移动智能终端内，能够利用移动智能终端操作系统提供的开发接口，实现某项或某几项特定任务的计算机软件或者代码片段。包含移动智能终端预置应用软件，以及互联网信息服务提供者提供的可以通过网站、应用商店等移动应用分发平台下载、安装、升级的应用软件。

3.1.4

移动智能终端预置应用软件 Smart Mobile Terminal Preloaded Application

移动智能终端内，在主屏幕和辅助屏界面（不包含进入界面后，通过菜单进入或者调起的功能）有用户交互入口并且可独立使用的移动智能终端应用软件。

3.1.5

框架型操作系统 Frame-based Operating System

框架型操作系统是指在移动智能终端或应用软件上，提供控制和管理应用软件的能力，并为在其上运行的应用软件提供相应开发接口的框架，主要形态有桌面型框架操作系统和应用型框架操作系统。

3.1.6

移动智能终端免安装应用程序 Non-installed Applications of Smart Mobile Terminal

在移动智能终端或框架型操作系统上，能够利用操作系统提供的开发接口，实现某项或某几项特定任务的应用程序，无安装过程。

4 移动智能终端免安装应用程序基本情况

4.1 移动智能终端免安装应用框架分类

框架型操作系统按照用户交互模式，分为桌面型框架操作系统和程序型框架操作系统。若用户交互的系统桌面属于框架型操作系统桌面，其上运行的多为免安装应用，则该框架型操作系统属于桌面型框架操作系统。

框架型操作系统按系统资源和能力提供方式，分为系统耦合型免安装应用框架操作系统和程序类免安装应用框架操作系统。快应用属于终端及操作系统深度结合的免安装应用，搭载在系统耦合型免安装应用框架操作系统中。微信小程序、智能小程序等，在其他应用软件上层运行的免安装应用，搭载在程序类免安装应用框架操作系统中。

4.2 移动智能终端免安装应用程序发展现状及应用场景

免安装应用无需基于原生系统能力下载、安装、卸载，即点即用，以快应用为代表的系统耦合型免安装应用，以微信小程序、智能小程序等为代表的的程序类免安装应用涉及的相关技术和应用领域发展迅速，终端用户在无明显感知的情况下使用免安装应用。另一方面，我们也看到除了以终端厂家为代表的快应用架构，和以互联网厂家推动的各种免安装框架外，操作系统也逐步推出了系统级的免安装应用接口和应用场景，让框架型操作系统和原生操作系统的边界越来越模糊。随着未来5G的大规模商用，物联网广泛应用，在流量和网络质量得以保证的条件下，免安装应用场景也逐渐变多，轻量、使用快捷的免安装应用有更广泛的应用场景，但系统安全能力保障的欠缺，应用加载和移除模式不统一，也引入了新的问题和风险。

4.2.1 基于系统耦合型免安装应用框架

系统耦合型免安装应用框架和系统能力紧密结合，便于将系统接口转化为框架接口，将免安装应用和系统原生应用的界限模糊化。

快应用（QuickAPP）由主流手机厂商组成的快应用联盟发起并制定相关标准，形成基于手机硬件

平台的新型应用形态，适用手机覆盖华为、金立、小米、魅族、努比亚、OPPO、vivo、联想、中兴和海信等众多型号终端，可应用于应用商店、浏览器、负一屏、短信、网页跳转、桌面图标、全局搜索、推送、锁屏、语音助手、应用卸载替换、智能识屏等多种业务场景。

4.2.2 基于程序类免安装应用框架

基于程序类的免安装应用框架能力均限定在程序框架内，运行其上的免安装应用借助框架提供的接口实现系统资源调用，以微信小程序、智能小程序、支付宝小程序和QQ浏览器小程序等互联网头部应用提供的免安装应用框架为代表。

程序类免安装应用框架依托的应用软件类型和应用领域不同，基于不同框架的免安装应用的使用范围、开发方式、接入方式和接口都有较大差异。原本单一功能的互联网应用，借助免安装应用能力，极大丰富了功能并增长了用户量，提供了基于大体量融合应用全新的连接用户和服务的方式，免安装应用提供了多样化的便捷服务，方便获取和传播，丰富了用户体验。轻量级的开发，借助框架自身的多平台特点，也减轻了开发者的开发和部署成本。

5 免安装应用框架结构及敏感行为调用情况

5.1 框架介绍

5.1.1 系统耦合型免安装应用框架结构

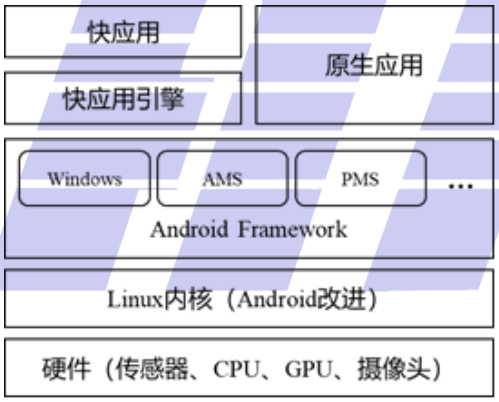

图 1 快应用框架

系统耦合型免安装应用框架由于系统深度耦合性，可以通过框架能力直接调用系统资源，如图1，快应用框架。借助系统级的能力，实现原生应用相近的功能，但无需安装。

5.1.2 程序类免安装应用框架

程序类免安装应用框架透过被搭载的应用程序实现系统资源的调用。免安装应用通过框架实现统一的包管理，应用内的视图层和逻辑层分离，分别实现进行事件和数据交互，数据驱动和生命周期管理。视图层用于呈现免安装应用界面，逻辑层进行免安装应用的事件处理、接口调用和生命周期管理，并通过JS桥传递本地资源的调用，实现扩展的原生功能。如图2，智能小程序架构；图3，QQ浏览器小程序架构。

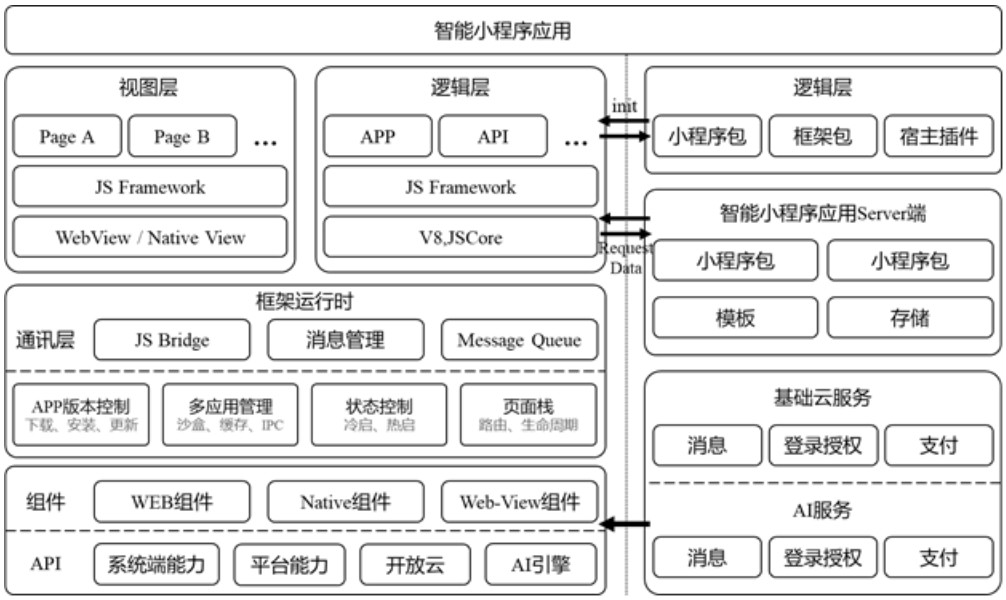

图2 智能小程序框架

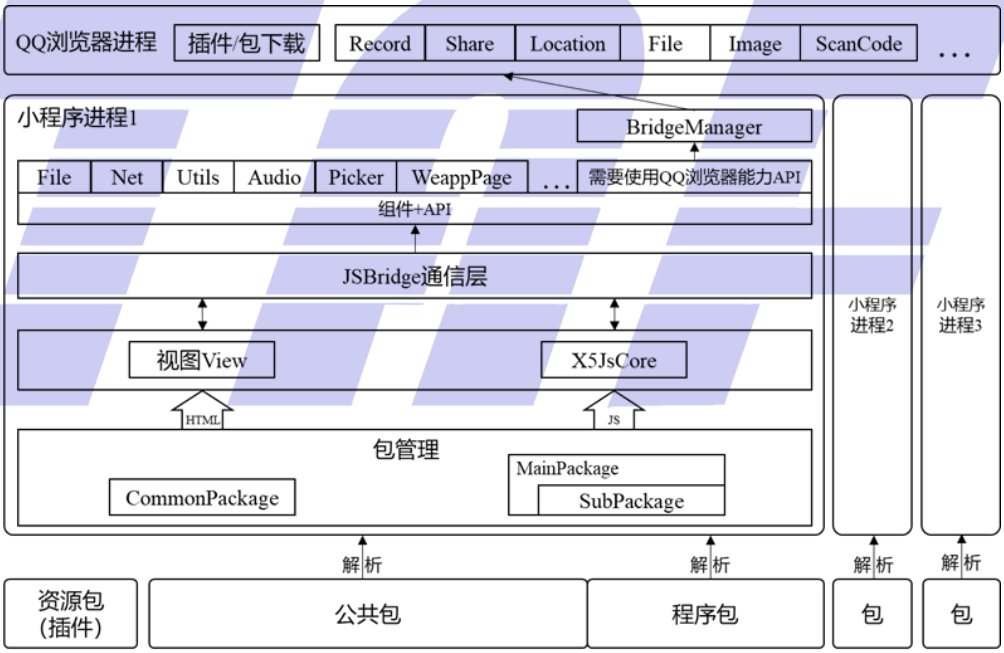

图3 QQ浏览器小程序框架

5.2 敏感行为调用情况

5.2.1 系统耦合型免安装应用

系统深度耦合有助于提供更加丰富的系统能力，实现接近原生应用的使用体验。以快应用为例，除了最基本的文件数据和网络访问外，提供了 20 种系统能力，其中包含地理位置、录音、联系人、发送短信等涉及敏感调用。框架自身提供了敏感行为调用权限申请机制，需要在快应用的 manifest.json 文件中声明所需权限，部分行为需要用户一次或者每次授权。

5.2.2 程序类免安装应用

程序类免安装应用的系统资源调用取决于框架程序自身，框架将用户授权的系统能力传递给免安装应用，每个上层应用对于系统资源调用的管控由框架操作系统自身实现。不同的框架操作系统提供不同程度的敏感行为管控能力。

智能小程序提供的敏感信息主要分为两部分，设备相关信息和用户个人信息，设备相关信息主要包含地理位置、相册存储、收货地址、发票抬头数据、录音、开启摄像头等行为或数据，用户信息主要包含用户账户信息（昵称、头像、性别）和手机号。开发者调用框架提供的接口或组件，用户授权后才可访问相关资源。

QQ浏览器小程序提供获取地理位置、录音、摄像头和用户账户信息等系统资源或用户数据的相关接口或组件，仅在用户授权后，调用方可成功。

6 免安装应用程序安全问题研究

6.1 概述

免安装应用程序作为全新的应用生态，相较于移动网页和原生应用，具有无需安装、互联互通、性能好、功能完整和强留存等优势，但正是由于脱离了浏览器和原生系统的系统级安全管控，不同框架的安全机制差异较大，有可能产生新的安全风险。

6.2 框架型操作系统安全

桌面型框架操作系统在用户使用界面上和原生操作系统没有本质差异，操作系统应通过给用户提示和让用户确认的方式来防范安全威胁，当其上安装的应用和免安装应用程序调用敏感行为（通信类功能、本地敏感功能）时，操作系统应具备给用户提示和让用户确认的能力，明确默认加载的免安装或预置应用的敏感行为调用机制，并实现无线外围接口开关和连接可知和可控，提供应用来源识别和密码等基础安全能力。

程序型框架操作系统针对自身提供的 敏感行为调用接口，应具备基本的用户提示和确认机制，依据敏感行为类型和数据保护重要程度，提供单次授权和多次授权机制，实现系统资源的监控、保护和提醒，确保涉及安全的行为总是在受控的状态下，不会出现用户在不知情情况下某种行为的执行，或者用户不可控行为的执行，并应明确免安装应用间数据调用和共享边界。框架型操作系统的框架程序自身不应有未向用户明示且未经用户同意，擅自调用终端功能，造成用户费用损失，流量耗费，信息泄漏的行为。

6.3 免安装应用程序安全

6.3.1 总体安全要求

免安装应用不应有损害用户利益和危害网络安全的行为。例如恶意吸费，未经授权的修改、删除、向外传送用户数据，强制定向推送等行为。

免安装应用运营者收集使用个人信息时要严格履行《网络安全法》规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。

免安装应用应有效并合理的利用框架型操作系统提供的安全机制，敏感行为的调用和操作需求保持一致，避免调用与当前服务场景无关的敏感行为，并谨慎处理用户拒绝调用的情况，用户拒绝授权的情况下，不应影响其他功能的使用。

6.3.2 数据传输安全

免安装应用应采用安全传输方式传输敏感数据。

6.3.3 软件认证签名

若框架型操作系统采用签名机制，免安装应用应包含签名信息，且签名信息真实可信。

6.3.4 数据录入安全

免安装应用在进行支付操作，输入认证/支付密码等敏感信息时，需采取技术措施防止密码被截获，并支持非明文显示方式。

6.3.5 第三方服务接入

免安装应用应谨慎选用接入的第三方服务，仅接入安全可靠的第三方服务。

7 标准化建议

国内的免安装应用标准和相关文件的制定工作主要由框架型操作系统提供方制定，目的用于指导应用开发者，内容主要集中在功能实现上。国际标准组织中，W3C中文兴趣下成立了MiniApps生态社区组，国内互联网厂家积极参与并作出大量贡献。

目前免安装应用从名称到实现方法均呈现碎片化趋势。免安装应用名称多样化，快应用Quick APP（快应用联盟），智能小程序Smart Program（百度），小程序Mini Program（微信）等，各自形成了独立的品牌效应。不同免安装应用采用相对封闭的生态模式，多样化的实现模式一方面促进了免安装应用快速推广和灵活发展，另一方面却加大了统一标准化要求的难度。

针对现阶段免安装应用的生态现状，建议桌面型框架操作系统及免安装应用依据现有原生系统安全标准，提供基本的安全能力；程序型免安装应用框架及上层应用参考原生系统基本要求，依据不同的调用方式和操作敏感程度，制定符合框架实现能力的安全机制，并指导开发者充分利用框架提供的安全能力。

附 录 A
（资料性附录）
常见免安装应用框架

序号	框架	
1	快应用	快应用联盟
2	智能小程序	百度
3	小程序（微信）	腾讯
4	QQ 浏览器小程序	腾讯
5	QQ 小程序	腾讯
6	支付宝小程序	蚂蚁金服

参 考 文 献

[1] 快应用 https://www.quickapp.cn/

[2] 智能小程序 https://smartprogram.baidu.com/developer/index.html

电信终端产业协会研究报告

移动智能终端免安装应用程序安全问题研究

R/TAF 001-2020

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn