iResearch
艾 瑞 咨 询

中国移动应用安全服务行业白皮书

2017年

开篇摘要

发展驱动力

- 移动应用安全市场整体处于发展初期阶段。
- 移动应用安全市场发展主要驱动力：其一，政策落地，对移动应用市场的安全等问题作出明确规定；其二，市场恶意软件泛滥，为移动应用安全防护市场带来机遇；其三，移动网民的持续增加与移动生活在在人们生活的不断渗透推动移动应用安全市场发展。

市场发展

- 安全检测：人工渗透测试和自动化检测是目前常用的两种检测手段。
- 安全加固：将dex文件进行加密处理，并将目标程序的入口指向壳程序是dex文件加固的原理，目前的加固技术是初级加固技术与虚拟机加固技术配合进行。
- 安全监测：渠道管理、识别仿冒程序以及大数据分析是安全监测的常用手段。

市场格局

- 国内移动应用安全市场中，主要存在互联网企业背景和垂直移动安全企业两大类主要玩家。
- 移动应用安全市场集中度相对偏高，中等偏大企业进入市场较早，客户群体覆盖比较广，但整个市场的准入度较高。
- 移动应用安全市场未来将在复杂应用的加固保护方案和恶意应用攻击向底层渗透这两个方面发力。

发展趋势

- 人工智能、机器学习将深度应用至安全检测，有效提升安全检测的质量与效率。
- 移动应用安全企业开始注重安全服务生态圈，安全服务将覆盖至整个产业链上下游。

艾瑞研究院自主研究绘制。

定义

针对移动应用生命周期可能出现的隐患提供的解决方案

目前业界还没有针对移动应用安全服务给出权威的定义，本文的移动应用安全服务指的是针对移动应用的开发、发布、分发以及安装使用等全生命周期阶段提供的开发咨询服务、安全咨询及安全保障等服务。

移动应用开发的生命周期的简单示意图

开发者

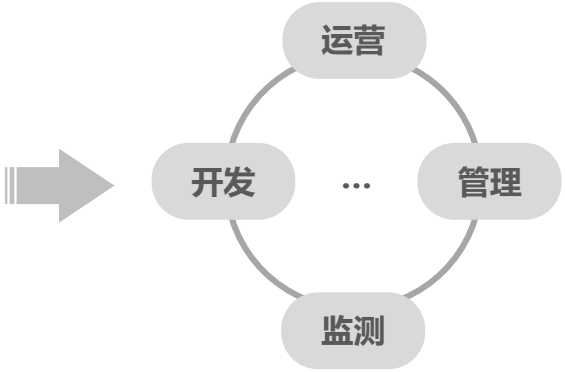
移动应用开发者在开发者平台上开发应用并将最终开发好的应用发布到各应用商店。

应用商店

应用商店将开发者开发的应用整合分类，并利用分发渠道将开发者发布的应用分发/推送给用户。

用户

用户从应用商店或者官网上下载应用，并安装应用。



提供安全服务的各个方面

来源：艾瑞研究院自主研究绘制。

Android平台的结构及特点

平台整体为层次结构，且各层功能分明

Android移动设备平台的软件层次结构自上而下分别为：Application（应用程序）、 Application Fraework（应用程序框架层）、系统运行是的各种类库和Android运行环境层以及Linux Kernel（Linux内核层）。其中Dalvik虚拟机位于安卓运行环境中，它主要是通过解释dex文件来执行由Java字节码转换而来的Davilk字节码，从而达到运行Android程序的作用。

Android平台系统架构图

来源：艾瑞研究院自主研究绘制。

Android平台的不足

平台架构及运营模式的不足造成移动应用安全受威胁

虽然Android平台本身有比较规范的安全机制，如应用层引用签名机制、应用权限控制机制保护程序的安全；内核层通过沙箱机制隔离不同进程的资源，并辅助独特的内存管理机制和进程间通信机制等。但是由于Android本身的开源性、推广的开放性等因素，安卓平台在自身架构、架构的安全机制以及平台的运营模式等方面均存在一定的不足，这些问题一旦被攻击者利用，用户的利益将受到侵害。

Android平台的不足

平台架构

Linux提权攻击风险

Root是Linux的最高权限，攻击者一旦拥有Root权限就可以对系统和文件进行肆意修改。

非法系统篡改

原生Android系统缺乏对系统镜像加载过程的安全防护，攻击者可以在系统内植入或安装非法程序。

APK逆向破解

Android采用Dalvik虚拟机进行代码执行，由于解释语言的机制会导致Android应用容易被攻击者通过反编译的手段进行逆向分析，进而恶意修改代码后二次打包，损害用户利益。

安全机制

伪造应用签名

Android的签名机制保证应用的安全性，但今年来暴露的签名漏洞使得攻击者利用恶意程序伪造合法应用而绕过验证机制。

模糊的权限声明

用户安装应用时无法通过阅读权限说明明确应用的真实意图，进而无法对用户决策产生有效支持。

作用受限的数据保护机制

Android仅采用了基于文件系统的加密技术保障数据安全，一旦设备正常运行，数据将暴露与系统的明文空间内，则其数据保护作用将受限。

运营模式

版本碎片化

由于Android采用完全开源及开放的推广态度，故市场上运行的安卓版本众多。版本过度分散会导致系统漏洞修复迟滞，一旦谷歌停过之对某个版本前的漏洞修复，用户利益将受威胁。

第三方Rom良莠不齐

Android系统的开放性使得第三方Rom市场繁荣，但由于第三方Rom的水平良莠不齐，可能会导致系统漏洞暴露，给攻击者带来可乘之机。

应用市场多样化

用户主要从第三方应用市场下载应用，而Android应用市场多，且缺乏审核监管机制，因此恶意软件泛滥，Android生态环境较差。

来源：艾瑞研究院自主研究绘制。

移动应用安全所处的政策驱动力

政策助力移动应用安全行业发展规范化、制度化

移动互联网的发展和智能手机的普及使得手机上网越来越流行，移动互联网时代的爆发更是带动移动端设备趋于全能化的发展，而与此同时，手段安全隐患越来越多、问题越来越突出。因此从2016年全国人大、网信办、公安部、工信部出台了多条相关的法律法规，净化网络空间安全、打击网络违法犯罪，助力安全市场发展。

2017年中国移动应用安全行业的政策环境

法律法规	主要内容	主要意义
移动互联网应用程序信息服务管理规定 2016年8月1日起施行	主要涵盖了关键信息基础设施保护、网络数据和用户信息保护、网路安全应急与监测等领域，并加强了个人信息保护要求，加大了对网络诈骗等不法行为的打击力度。	首次明确了国家网信办作为移动应用程序信息服务的主管单位，针对应用程序市场中的问题，如过度收集用户信息、恶意扣费等安全问题，都给出了明确规定，加强了APP信息服务规范管理，使得网民利益遭受侵害时有法可依，且投诉便捷、高效。
关于促进移动互联网健康有序发展的意见 2017年1月1日起施行	完善了市场准入制度，提升网络安全保障水平，维护用户合法权益、打击网络违法犯罪、增强网络管理能力，防范移动互联网安全风险。	《意见》提到将加大对移动互联网技术、商业模式等创新成果的知识产权保护，研究完善法律法规，规范网络服务秩序，提高侵权代价和违法成本；对完善移动互联网用户信息保护制度，严格规范个人信息收集，严查造谣诽谤等行为。
中华人民共和国网络安全法 2017年6月1日起施行	主要涵盖了关键信息基础设施保护、网络数据和用户信息保护、网路安全应急与监测等领域，并加强了个人信息保护要求，加大了对网络诈骗等不法行为的打击力度。	构建了我国首部网路空间管辖的基本法律法规，网络参与者提供普遍法律准则和依据，推动全社会网络安全意识的提升和网络安全保障水平的发展。

来源：艾瑞研究院自主研究绘制。

移动应用安全所处市场驱动力

市场恶意软件泛滥，移动应用安全市场亟待解决

根据《YD/T2439-2012移动互联网恶意程序性描述格式》，移动互联网恶意程序行为属性包含以下8类：恶意扣费、信息窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈和流氓行为。

2017年中国移动应用常见的恶意软件分类及其行为

恶意扣费 在用户不知情或未授权的情况下，通过隐蔽执行、欺骗用户点击等手段，订购各类收费业务或使用移动终端支付，导致用户经济损失。

在用户不知情或未授权的情况下，获取涉及用户个人隐私信息的行为。 **信息窃取**

远程控制 在用户不知情或未授权的情况下，能够接受远程控制端指令并进行相关操作。

自动通过复制、感染、投递、下载等方式将自身、自身衍生物或其他恶意代码进行扩散。 **恶意传播**

资费消耗 在用户不知情或未授权的情况下，通过自动拨打电话、发送短信、彩信、邮件、频繁链接网