360 天机移动应用安全加固系统

产品白皮书

北京奇安信科技有限公司

2016-12

目 录

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 1870 邮箱: 360jiagubao@360.cn

1. 背景

移动互联网的迅猛发展，让越来越多的企业投身于移动应用开发中，Android 平台以免费和开源的特点，占据了移动领域的半壁江山。国内应用市场鱼龙混杂，对应用的管理和审核机制缺乏有力的监管与规范，导致 APP 承担了被他人反编译、恶意篡改、二次打包的风险。APP 一旦被破解后植入木马，不仅给开发商带来名誉和金钱损害，APP 玩家隐私也会被窃取。

面对纷乱复杂的 Android 环境，只有提高 APP 自身的安全保护能力，保护 APP 不被非法篡改和二次打包，确保 APP 自身代码的安全，才能从源头杜绝安全风险的发生。在此前提下，360 公司推出移动应用安全保护服务——360 天机移动应用安全加固系统。

2. 功能概述

服务名称：360 天机移动应用安全加固系统

产品简介：360 天机移动应用安全加固系统是基于 360 核心加密技术，给安卓应用进行加密、加壳保护的安全技术产品，可保护应用远离恶意破解、反编译、二次打包，内存抓取等威胁，同时给应用提供数据加密、签名校验、防内存修改、完整性校验、应用安全检测等保护。

此产品采用多项 360 核心加密技术，对应用程序深度加密处理，独有的程序文字信息加密功能，能有效防止应用被反编译和恶意篡改

和，保护应用不被二次打包，保护数据信息不会被黑客窃取。给予官方应用最强保护，从源头消灭恶意盗版应用。

产品特点：

- 加固零成本：无需企业进行二次开发，立刻拥有顶级安全保护
- 应用零风险：防止应用被二次打包、恶意篡改、内存截取等风险
- 大小零增加：独创隐形压缩技术，加固后文件大小零增加
- 使用零影响：完美兼容各版本安卓系统，对应用功能、性能零影响
- 拥有成本低：企业用户在完成正常应用开发后，只需提交该应用到 360 天机移动应用安全加固系统，立即能获得业界最新的加固服务，安全性、兼容性测试报告等，零维护成本。

3. 功能介绍

3.1 APP 应用加固

360天机移动应用安全加固系统提供应用一键加固保护功能。主要原理是将安全性较低的Java程序源代码加密并压缩，存储至安全性更高的Native层，同时对Native层的代码采用自定义Linker方式和基于shellcode的elf文件加密方式进行加密处理；并且在原数据中增加部分垃圾数据，使常规反编译工具失效或无法正常还原源代码，同时还在程序中内置多个内存还原对抗点，防止源代码通过内存截取的方式

泄露。

加固后的应用可防止反编译工具破解和逆向，包括但不限于smali，baksmali,JEB,Dex2jar，jd-gui，BytecodeViewer，AXMLPrinter2,ApkTool工具等，以上工具均无法正常进行应用程序源代码反编译和重打包操作。

加固主要可实现对APP的以下保护：

- 基于虚拟机指令（VMP）的 dex 文件加密保护
- 基于虚拟机指令（VMP）的 so 文件加密保护
- 应用主配文件防篡改保护
- 应用资源文件完整性保护
- 应用数据文件加密保护
- 应用签名校验保护
- 防内存截取攻击保护
- 应用内存非法读取/修改保护
- 防动态注入攻击保护
- dex 文件深度混淆
- Cocos2D 引擎 Lua 脚本保护
- Unity3D 引擎 Dll 脚本保护

3.1.1 基于虚拟机指令（VMP）的 dex 文件加密保护

实现原理：对原应用中 dex 文件采用高压缩及加密变形处理，原始 dex 的关键函数指令采用基于虚拟机指令保护方法，并将指令解释

方案实现在 native 层的保护壳中。反编译软件在对应用进行逆向的时候只能看到加固后新增的保护壳的部份，并不能够逆向出原 dex 中的数据及代码。

3.1.2 基于虚拟机指令（VMP）的 so 文件加密保护

实现原理：对原应用中的 so 文件代码采用自定义 Linker 方式进行加密保护，并且对于壳 so 中的关键函数使用基于虚拟机指令的 so 保护，由于 VMP 的高强度保护方案，以至于调试者或破解者无法获取 Linker 入口从而无法正常反编译 so 文件中代码。同时采用基于动态加载器的 so 保护，增大了壳 so 和第三方 so 的保护强度，保护应用中的 so 的安全性。

3.1.3 应用主配文件防篡改保护

实现原理：采用哈希技术对主配文件生成文件指纹，指纹信息保存在 dex 文件某处，并在程序运行时对文件指纹进行校验，如发现指纹改变则停止运行。

3.1.4 应用资源文件完整性保护

实现原理：通过快速计算方法，把文件的完整特征存储到源 dex 保护数据中，在运行的时候能够快速判断文件是否被修改，达到保护目的。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 1870 邮箱: 360jiagubao@360.cn

3.1.5 应用数据文件加密保护

实现原理：对应用运行中的产生的数据文件进行加密保护，防止数据文件被窃取和篡改，加密关键信息保存在 Native 层保护壳中。

3.1.6 应用签名校验保护

实现原理：开发者签名信息进行变换存储成特征，把特征存储到源 dex 保护数据中，在运行的时候能够快速判断签名是否被修改，达到保护开发者被二次发布的目的。

3.1.7 防止内存截取攻击

实现原理：动态监控 Android 程序中的内存分布文件，可以随时监控到内存读取等操作，从而保护内存截取攻击。

3.1.8 应用内存非法读取/修改保护

实现原理：动态监控 Android 程序中的内存分布文件，可以随时监控到内存是否被非法第三方程序进行读写操作，从而保护应用运行时的内存数据不被非法读取或修改。

3.1.9 防动态注入攻击保护

实现原理：对应用的关键模块增加反调试技术，从根本上杜绝调试本程序，注入非法代码等操作，保护软件的安全运行。

3.1.10 dex 文件深度混淆

实现原理：对内存中的应用 dex 文件进行混淆处理，使得在 dex 被内存截取的情况下，也只能截取出加固混淆之后的代码，无法还原出原始 dex 文件。

3.1.11 Cocos2D 引擎 Lua 脚本保护

实现原理：对使用 Cocos2D-Lua 的应用，提取出应用包 Lua 脚本文件，经过高强度的算法加密，并打包回原应用包。破解者从应用包中获取到的 Lua 脚本并不能得到直接识别。应用在系统运行加载 Lua 脚本时，会经过加固的代码解密，并正常运行。

3.1.12 Unity 3D 引擎 Dll 脚本保护

实现原理：对使用 Unity3D 的应用，提取出应用包中 Dll 脚本文件，经过高强度的算法加密，并打包回原应用包。破解者从应用包中获取到的 Dll 脚本并不能得到直接识别。应用在系统运行加载 Dll 脚本时，会经过加固的代码解密，并正常运行。

3.2 加固增强服务

360 天机移动应用安全加固系统在加固过程中还提供了多种免 SDK 集成的可选增强服务，具体服务介绍如下：

3.2.1 应用盗版监测

应用盗版监测服务通过对国内外主流应用市场的监测，能帮助开发者发现主流应用市场的应用盗版情况；同时根据 360 智能安全监控系统监控并发现在主流市场渠道之外盗版应用情况，并对盗版应用进行详细分析，可以提供盗版应用的证书情况，应用个数、传播渠道、影响的用户设备数等数据，帮助开发者掌握盗版应用的影响范围。

3.2.2 崩溃日志分析

崩溃日志分析服务为应用提供实时的应用运行崩溃情况统计。该服务无需集成 SDK，就能够全面监控应用的崩溃信息，不论是 Java 层崩溃还是 Native 层崩溃，全部都可以及时抓取到应用异常时的关键信息，方便开发者对问题进行判断还原；同时智能捕捉应用崩溃时的异常类型、异常信息与关键方法，并从崩溃率、影响机型、影响系统等多个维度对异常崩溃信息造成的影响进行统计分析，使开发者能最快了解异常崩溃的情况及影响，及时安排对异常崩溃情况的处理和修复。

4. 兼容性情况

4.1 完善的兼容性保障服务

（1） **全自动兼容性测试系统：**360 天机移动应用安全加固系统拥有自动化兼容性测试系统，可自动完成上百款主流 Android 机型的兼容

性测试，覆盖当前 Android 用户 90%以上

（2） **与手机厂商紧密合作**：与华为、INTEL、MTK 等多家手机设备制造商紧密合作，从系统底层解决加固兼容性与安全性问题

（3） **紧密追踪 Android 系统更新变化**：360 天机移动应用安全加固系统以平均每月升级 1 次的速度，快速适配 Android 系统的更新升级，目前是国内第一家实现 Android N 系统兼容的加固产品。上线至今，累计加固后应用已成功运行在超过 8 亿的用户设备上。

4.2 兼容的 Android 系统版本

Android 2.1、2.2.X、3.X、4.0.X、4.1.X、4.2.X、4.3.X、4.4.X、5.0.X、5.1.X、6.0，7.0 包括 davilk 模式和 ART 模式。

4.3 兼容 X86 架构安卓手机

与 INTEL 公司深度合作，加固应用可兼容 X86 架构的 Android 手机。

5. 360 天机移动应用安全加固系统优势介绍

5.1 专业源代码保护方案

360 天机移动应用安全加固系统采用独有的程序文字信息加密，可有效的防止应用被静态破解和动态攻击。

360 天机移动应用安全加固系统对 dex 源文件、so 源文件、应用主配文件、应用资源文件、应用数据文件都有高强度的加密保护方案；同时对每个文件做了完整性保护，并对整体应用进行了签名校验保护，

彻底防止应用被破解和二次打包的可能。

加固还采用了内存打散加密技术，可真正防止应用源代码以内存截取的方式被还原，同时可防止其他程序在内存中的扫描与篡改动作，保护应用不被动态注入攻击。

5.2 多维度的安全保护

360 天机移动应用安全加固系统区分在线大众版提供更多维度的安全加密保护：

功能项	专业版	定制版
基于虚拟机指令（VMP）的 dex 文件加密保护	√	√
应用签名校验保护	√	√
防止内存截取攻击	√	√
应用内存非法读取/修改保护	√	√
基于虚拟机指令（VMP）的 so 文件加密保护		√
应用主配文件防篡改保护		√
应用资源文件完整性保护		√
应用数据文件加密保护		√
防动态注入攻击保护		√
dex 文件深度混淆		√

5.3 最优的加固性能

360 天机移动应用安全加固系统拥有独立自主产权的“隐形加固”技术，是目前唯一能实现加固后应用大小零增加的加固类产品。经产品测试 90%的应用在加固后，应用大小会会减小 50k~300k。市面上其他加固类产品平均增加 300k-500k。

加固后应用启动时间平均只增加 0.3 秒，使用基本无感知。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 1870 邮箱: 360jiagubao@360.cn

5.4 系统兼容性

360 天机移动应用安全加固系统经过严格的兼容性测试，真机测试超过 1000 款，涵盖安卓 2.1 以后所有版本操作系统，覆盖国内所有主流机型与定制 rom，加固后的应用兼容性得到完美的保证。

5.5 客户端兼容性

360 天机移动应用安全加固系统的加固方案适用于所有安卓客户端，使用无差异。

5.6 专业的团队支持

360 天机移动应用安全加固系统拥有单独的企业安全支持团队，负责全程配合技术和商务上的相关问题解决，为企业客户提供最贴心的安全服务。

5.7 同类产品对比

功能	功能描述	同类产品对比	
		360 天机移动应用安全加固系统	其他
高强度 VMP 加密保护方案	采用最高强度的 VMP 加密方案，同时对 dex 文件和 so 文件进行加密保护	VMP 方案	其他方案
加固应用大小优化	加固应用同时对应用原程序中的 dex 文件进行加密压缩，保护源代码同时可优化应用体积大小	加固后应用增量小于 100K	加固后应用平均增加 300K 以上
源代码优化	加固同时对源码进行优化、	支持	不支持

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 1870 邮箱: 360jiagubao@360.cn

	Log输出清除等功能优化		
应用安全检测	利用 360 安全病毒库，对加固前的应用进行安全检测，检测是否含有风险代码或不必要的敏感权限	支持	不支持
加固增强服务功能丰富	除应用加固之外，还可提供“应用盗版监测”、“崩溃日志分析”、“应用升级通知”、“应用数据分析”等多种增强服务，所有服务均无需二次开发，与加固服务完美整合	支持多种增强服务	无增强服务 或 服务需人工参与