移动应用安全加固

技术白皮书

2.0.0 版本

文档版本：V20200408

蚂蚁金服金融科技文档

商标声明

及其他蚂蚁金服金融科技服务相关的商标均为蚂蚁金服所有。

本文档涉及的第三方的注册商标，依法由权利人所有。

免责声明

由于产品版本升级、调整或其他原因，本文档内容有可能变更。蚂蚁金服金融科技保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在蚂蚁金服金融科技授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过蚂蚁金服金融科技授权渠道下载、获取最新版的用户文档。如因文档使用不当造成的直接或间接损失，本公司不承担任何责任。

目 录

1 什么是 MSA

移动应用安全加固（Mobile Security Armor，简称 MSA）是移动开发平台基于阿里集团的移动安全加固技术打造的一款安全应用，该应用能够为为安卓应用（App）提供稳定、简单、有效的安全保护，提高 App 的整体安全水平，力保应用不被逆向破解。

1.1 产品背景

Android 应用的代码一旦分发出去，都会以某种形式处于不可信环境中，难免被有心人分析破解。隐藏在代码中的秘密，无论是私有算法，或是私有协议，或者是加解密秘钥，都可能被攻击者破解出来，然后侵犯原作者的商业利益或知识产权。所以应用被逆向破解是商业风险源头之一。

我们开发安全防护工具的原则是，既要充分提高自身安全能力，增加对手的破解难度和攻击成本，也要尽量降低用户的接入成本，还要兼顾运行效率与体积，尽可能地将更顺滑的服务提供给用户。

1.2 发展现状

MSA 依赖于阿里集团的移动安全加固技术，经历了淘系多个亿级应用的安全性考验，在安全性上具有非常可靠的保障。MSA 的防护能力涵盖核心代码的混淆以及 APK 加壳，能够封杀 Java/Smali 字节码被工具反编译为 Java 源码和 Java/Smali 字节码被直接阅读的风险。

MSA 的使用很简单，只需一个配置文件就可以实现对 APK 文件的一键加固；兼顾了安全性、运行效率和体积上的平衡。

1.3 面临的问题及关键挑战

移动应用安全加固作为一个安全加固产品，面临着自身的安全风险和来自行业高要求的挑战。

自身安全风险

1. 虽然移动应用安全加固在不断地升级自身的安全技术、提高安全系数，已经能够轻松应对绝大多数的安全威胁，但是由于安全产品处在对抗一心谋求不当利益的黑色产业个人或组织的第一线，时刻面临着来自各种各样的攻击和威胁，仍然需要不断的提升自己的安全实力。
2. 随着行业的发展和进步，我们的用户已经具备了日益提高的安全意识，掌握着今非昔比的安全防范技能。但是，我们不能否认依然存在有着较低安全意识的用户，他们的工作环境或生产环境依然处在易攻破、易感染的情况下。因此，提高应用数据的本地存储和通信传输的安全将会是一个长期的发展目标。

行业要求

中国银行发布的〔2019〕237 号文件附件《移动金融客户端应用软件安全管理规范》对客户端应用软件安全提出了明确的要求，在抗攻击能力层面详细列出了基本要求和增强要求。移动应用安全加固作为一款应用安全加固产品，则需要直接应对这些要求，提供完美的解决方案。

以下内容摘自《移动金融客户端应用软件安全管理规范》。

5．3．3 抗攻击能力

基本要求：

a) 客户端应用软件应具备基本的抗攻击能力，能抵御静态分析、动态调试等操作。

b) 客户端代码应使用代码加壳、代码混淆、检测调试器等手段对客户端应用软件进行安全保护。

c) 客户端应用软件安装、启动、更新时应对自身的完整性和真实性进行校验，具备抵御篡改、替换或劫持的能力。

d) 客户端应用软件如使用安全输入控件，该控件应具备抵御一定程度攻击的能力。

增强要求：

客户端应用软件如使用安全输入控件，该控件应具备检测自身是否正在被调试的能力，并采取适当的风控措施，如:给予用户风险提示。

2 产品优势

加固能力全面

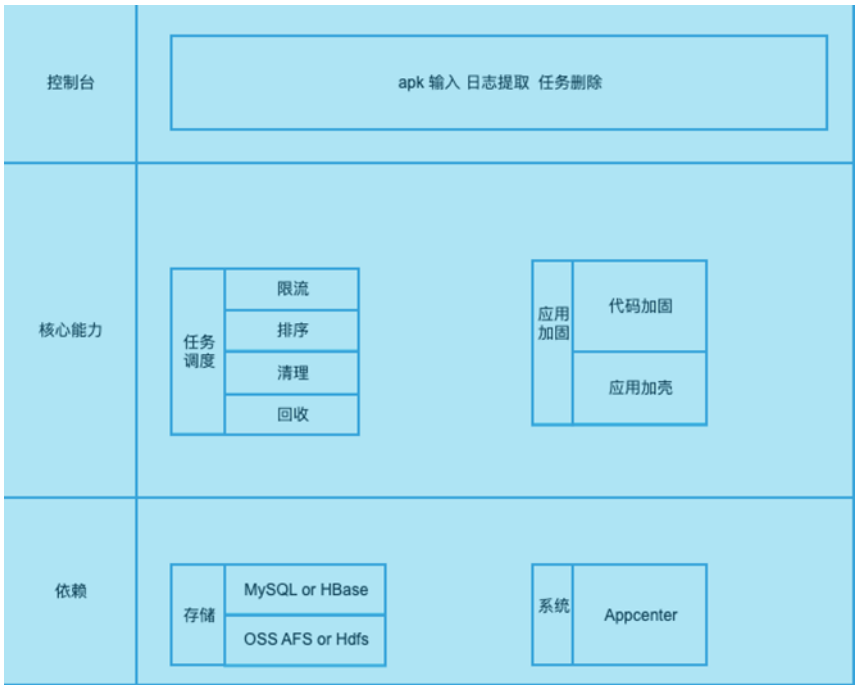
在不改变 Android 应用源代码的前提下，使用移动应用安全加固在 APK 中集成针对各种应用安全缺陷的加固技术，从而提升应用的整体安全水平，力保应用不被盗版侵权。

加固性能优秀

严格控制加固对 APK 体积及性能的影响，在加固前后，应用的体积、性能不会出现显著变化。

3 产品架构

MSA 由任务调度和应用加固两部分组成。任务调度负责任务的排序、清理、限流、回收等工作；应用加固负责应用加壳和代码加固工作。MSA 的系统架构如下图所示。



4 性能指标

在所有类全加固的情况下：

- **运行效率方面**

Java2Java 效率损失小于 10%，Java2C 效率损失小于 50%。

- **体积方面**

Java2Java 膨胀 20%~50%，Java2C 膨胀 2~3 倍。但由于 APK 包含资源文件，体积膨胀比例会被稀释。

一般情况下，我们只需要对核心类进行加固即可满足安全需求。如果对全部类加固会影响 APK 的体积和性能。

5 功能原理

移动应用安全加固通过对 Android 应用重新编译、加壳保护、修改其指令调用顺序等手段来增强应用的反破解能力。在加固过程中，注重加固强度与兼容性并重，避免一般加固功能由于盲目追求加固强度而导致加固后应用完全不可用的问题。

移动应用安全加固采用了自研的 java2java 工具实现了以下加固能力：

- **APK 加固**

  对 APK 整体进行安全保护，提供 APK 防反编译保护、DEX 文件整体加壳保护、DEX 文件防篡改保护、防白盒攻击、壳加密算法保护、防调试保护、防内存篡改保护、防 Hook 保护、防模拟器保护、APK 防重打包保护、防内存 dump 保护。

- **类安全加固**

  对 Java 代码进行混淆，使真实控制流程被隐藏，防止 jadx-gui 反编译。加固后的代码人工难以直接阅读。

- **应用加壳**

  将字节码在 dex 文件中彻底隐藏起来，让普通反编译工具根本找不到字节码所在。


蚂蚁金服
ANT FINANCIAL
金融科技
FINANCIAL TECHNOLOGY