移动应用安全

产品简介

腾讯云

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

产品简介

产品概述

最近更新时间：2023-03-17 16:59:28

移动应用安全（Mobile Application Security，MS）针对移动应用普遍存在的破解、篡改、重打包等各类安全风险，提供 Android 应用加固、iOS 源码混淆、SDK 加固等多种加固技术，已服务于金融、互联网、车联网、物联网，运营商等多个行业。稳定、简单、有效，让移动安全建设不再是一种负担。

注意

- 需上传已签名的安装包。
- 应用加固后需重新签名，否则无法正常安装。

产品优势

最近更新时间：2023-11-20 10:50:32

自研的加固技术

移动应用加固产品采用腾讯自研的安全加固技术，腾讯旗下多款热门应用均采用该加固技术，可帮助开发者从源头上解决应用中存在的安全风险。

稳定性强

移动应用加固产品为内部大量 App 提供安全、有效的加固方案，同时商业化成熟度高，合作案例涵盖泛互联网、金融、汽车等行业，稳定性满足客户需求。

兼容性高

移动应用加固产品采用千余款真机而非虚拟机来验证加固稳定性，确保加固方案在主要机型上的兼容。

灵活配置

操作简单、功能项可以灵活配置；Android 加固支持在线加固及本地工具加固；iOS 源码混淆工具提供本地工具，支持流水线集成。

功能覆盖全面

支持 dex 整体加壳以及 vmp 虚拟化方案结合使用，有效提高应用程序防逆向、破解的难度。

功能介绍

最近更新时间：2023-08-29 11:32:41

Android 应用加固

移动应用安全提供的 Android 应用加固分为基础版和企业版。每个版本对应功能如下表所示：

类别	功能	基础版	企业版
反编译保护	反编译保护	DEX 反编译保护	壳加密算法保护
		–	AndroidManifest.xml 防篡改
		DEX 文件整体加固保护	DEX 文件整体加固保护
		–	DEX 虚拟化加固（VMP）
	SO 反编译保护	–	SO 库加壳保护
		–	SO 库内存动态清除
		–	SO 库与应用绑定保护
		–	高级 SO 混淆保护
		–	SO 库字符串加密
防篡改保护	APK 防篡改保护	–	APK 防二次打包保护
		–	APK 签名文件校验保护
	源代码防篡改保护	DEX 文件防篡改	DEX 文件防篡改
		–	SO 库防篡改
	资源防篡改保护	–	assets 资源防篡改
		–	res 资源防篡改
		–	raw 资源防篡改
		–	配置文件防篡改
防调试保护	防调试保护	–	防模拟器保护
		–	加固壳防动态调试

		–	防线程动态调试保护
		–	防进程动态调试保护
		–	防 JDWP 调试
		–	防注入保护
		–	防内存数据读取
		–	防内存数据修改
数据与资源保护	资源防窃取保护	–	assets 资源防窃取
		–	res 资源防窃取
		–	raw 资源防窃取
		–	SSL 证书防窃取
	本地数据保护	–	本地 databases 目录数据库文件加密
		–	防日志泄漏
价格	–	免费	8万/年/APP
适用范围	–	个人开发者适用	金融 App 及企业适用

iOS源码混淆

常量字符串加密

在源码编译期对常量字符串进行加密，避免攻击者利用常量字符串进行核心代码定位，获取敏感信息。

指令多样化

将某些逻辑指令转换成随机等价的多条逻辑指令组合，增大破解者代码分析的难度，有效隐藏和保护核心算法原始逻辑。

基本块分割

将某个基本块随机分割成多个基本块，并对分割后的基本块进行混排，使控制流更加复杂。

伪控制流

在原有控制流中引入冗余控制逻辑，使应用控制流图复杂化，增大逆向工具分析程序逻辑的难度。

控制流扁平化

遇到循环结构时，会进行结构转换，达到隐藏程序原始逻辑的目的。

应用场景

最近更新时间：2023-03-17 16:59:33

上线前安全加固

App 开发完毕直接上线，可能存在代码泄露风险，通过 dex 整体加壳加固，有效应用代码安全，提高企业 App 被逆向、破解的难度。

防止应用被二次打包

未经安全防护的 App 易被攻击者获取代码信息，制造仿冒应用，采用签名校验、防重打包等加固技术，有效防止应用被二次打包后投放应用市场。

敏感数据保护

敏感数据信息、核心算法逻辑、版本内容等需要进行保护，移动应用安全推出的安全加固支持本地资源加密，有效防止攻击者窃取用户敏感数据。