爱加密移动应用安全加固平台彩页

产品概述

移动应用安全加固背景：随着移动互联网产业快速发展，应用呈井喷式爆发，应用开发者从几万迅速增加到几十万，APP 数量更是突破百万，每日新开发的 APP 在以几何级数量递增。移动应用正逐渐取代 PC 端成为黑客攻击的主要对象，超 97%的移动应用遭受盗版侵袭，病毒木马肆虐、流氓软件和钓鱼应用随处可见，严重影响了开发者收益、客户端安全和体验。

移动应用安全加固：为 APP 提供整体安全加固，包括 Android 端加固、IOS 端加固、Web 端加固、变幻加固等功能，从根本上解决移动应用的安全缺陷和风险，使加固后的 APP 具备防逆向分析、防二次打包、防动态调试、防进程注入、防数据篡改、防 OWSAP Top10 漏洞攻击、防自动化工具攻击等安全保护能力。

Android 端加固核心技术

- **防逆向**

通过 DEX 加密、IVMP、源码混淆等加固技术对 DEX 和 SO 文件进行保护。

- **防篡改**

提取 APP 内每个代码、资源、配置文件的特征值，防止 APP 被反编译后植入恶意代码。

- **防调试**

多重加密技术防止代码注入，防 JAVA 层/C 层动态调试、防代码注入和防 HOOK 攻击。

- **数据防泄漏**

多种加密算法，包括国际通用算法及自主研发的加密算法等，保护本地数据的安全。

- **页面数据防护**

应用防劫持、应用防截屏、虚拟键盘 SDK，对输入输出数据进行保护。

- **传输数据防护**

客户端和服务端对数据进行加密，保证通道中传输的数据为高强度加密后的数据。

模块	功能
防逆向	DEX 整体加密保护、DEX 代码分离保护、DEX 混合加密保护、DEX VMP 保护、双重 VMP 保护、Java2CPP、SO 加壳、SO Linker、SO 防调用、SO VMP。
防篡改	DEX 文件防篡改、SO 库文件防篡改、H5 文件防篡改、资源文件防篡改、资源文件加密、签名保护。
防调试	防动态调试、防内存代码注入、防模拟器、防加速器。

模块	功能
数据防泄漏	防内存数据读取、防内存数据修改、防日志泄漏、本地 sharepferences 数据加密、本地 SQLite 数据加密。
页面数据防护	防劫持、防截屏、安全键盘 SDK。
传输数据防护	通信协议加密 SDK、密钥白盒。

IOS 端加固核心技术

- **常量字符串加密**

对字符串采取随机加密，运行时动态解密。

- **基本块分裂**

C/C++/OC/Swift 代码中函数所对应的基本块进行"分裂"变扁，增加破解者分析难度。

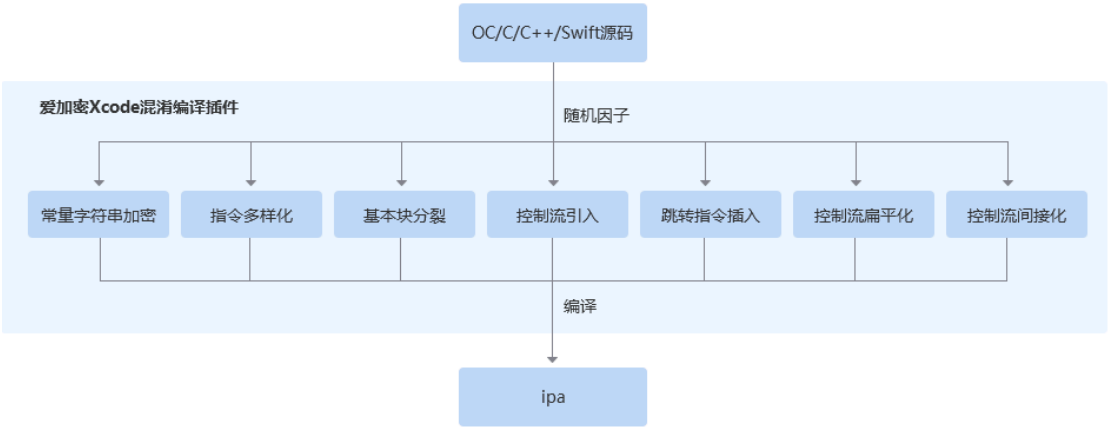
- **指令多样化**

对 C/C++/OC/Swift 代码中每条逻辑指令随机转换成等价的多条逻辑指令组合。

- **控制流保护**

对应用程序逻辑结构进行打乱混排，保证源码可读性降到最低。

根据 iOS 的技术原理和破解原理，在 OC/C/C++/Swift 代码编译的过程中，通过字符串随机加密，指令多样化、基本块分裂、控制流引入、跳转指令插入、控制流扁平化、控制流间接化等核心技术，保护应用免遭破解攻击，并且加密后的 APP 性能和稳定性不受影响。



Web 端加固核心技术

- **常量字符串/常数加密**

对常量字符串、常数进行混淆加密，降低代码可读性。

- **变量名混淆**

将函数名称、变量名称进行混淆，使处理后的 JavaScript 代码不具备可识性。

- **控制流保护**

结合不透明表达式，引入多余控制流，进行扁平化处理，使 JavaScript 代码可读性变差。

- **二元表达式加密**

对 JavaScript 中的二元表达式转换成等价函数调用形式，增大破解者分析难度。

- **防调试**

防止JavaScript在未知环境中执行，或者被调试工具调试。

- **域名绑定**

防止 JavaScript 代码运行在非授权的网络域名。

- **JS 加壳**

通过对整体代码进行加壳处理，隐藏整体代码结构。

- **多态变异模式**

采用一次一密模式，使每次加密后的代码都不相同。

加固项目	Web 页面	APP H5 文件	微信小程序
流平坦化	支持	支持	支持
垃圾指令注入	支持	支持	支持
常量字符串加密	支持	支持	支持
常数加密	支持	支持	支持
二元表达式加密	支持	支持	支持
代码压缩	支持	支持	支持
函数变量名混淆	支持	支持	支持
禁止控制台输出	支持	不支持	不支持
JS 加壳	支持	支持	不支持
防调试	支持	不支持	不支持
JS 域名绑定	支持	不支持	不支持
流平坦化	支持	支持	支持
垃圾指令注入	支持	支持	支持
OWASP Top10 漏洞防护	支持	支持	支持

变幻加固核心技术

- **验证变幻**

通过主动下发验证代码在客户端环境中执行，验证是真人还是自动化工具。

- **令牌变幻**

防止 JavaScript 代码运行在非授权的网络域名。

- **代码变幻**

对应用服务器返回页面实时变幻算法进行处理，返回到客户端的页面源码不具可识别性。

- **表单变换**

对用户的 POST 请求信息和文本型返回信息实时变幻算法混淆，防中间人。

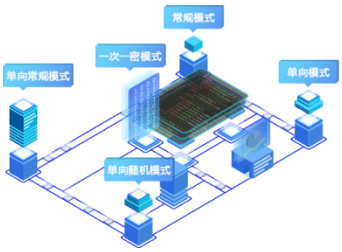
模块	功能
令牌变幻	通过对访问页面的请求授予在实时变幻的令牌，并每次验证令牌合法性，保证访问页面请求不可不可直接构造，也不可被重放。
验证变幻	在网页内插入对客户端环境的动态验证代码，验证终端访问行为，验证客户端操作行为，实时区分是真人操作还是自动化工具操作。
代码变幻	无论人还是工具，都无法看到页面的表单、Javascript 代码、href 链接等信息，成功地隐藏了可攻击的入口。另一方面，没有这些信息，攻击者及其自动化工具便无法判断应用程序的后续逻辑，无法预测应用服务器行为。
表单变幻	攻击者可能会通过流量劫持或缓存投毒等方式对受害者发起中间人攻击，请求数据被混淆后，攻击者即便截获数据包也无法看懂、篡改。

型号规格

机型	软件版	标准硬件版	高配硬件版
尺寸	/	90×450×680mm (H*W*D)	90×450×680mm (H*W*D)
CPU	16C	20C	40C
内存	32G	32G	64G
硬盘	/	1T	2T
网卡	/	1Gps 电口（含 Bypass） × 4 1Gps 电口（不含 Bypass） × 2	10Gps 光口（含 Bypass） × 4 1Gps 电口（不含 Bypass） × 2
网络层吞吐量（双向）	≥1.6Gbps	≥1.8Gbps	≥8Gbps
HTTP 吞吐量（双向）	≥600Mbps	≥800Mbps	≥4Gbps
HTTP 最大请求速率	≥12000 请求/秒	15000 请求/秒	22000 请求/秒
HTTP 最大并发连接数	≥60 万	≥80 万	≥200 万

机型	软件版	标准硬件版	高配硬件版
HTTP 最大新建连接数	≥9000 连接/秒	≥10000 连接/秒	≥35000 连接/秒

产品优势

	➢ 最新第六代高级双重 VMP 加密技术 ➢ 6 种加密方式满足不同用户、行业的使用需求 ➢ 加密后包增量大小不超过原包“±5%” ➢ 兼容性高达 99%，实现 ART 全面兼容 ➢ 交付方式灵活，支持本地部署或者云部署 ➢ 通过密钥白盒技术实现最强的加密强度
	➢ 支持 ARM/ARM64/i386/x86_64 等所有常见处理器平台 ➢ 可无缝替换的 Xcode 自带编译器，完美支持命令行方式 xcodebuild ➢ 保证加密后的 APP 性能和稳定性不受影响 ➢ 根据客户需求，区别关键代码和次要代码，通过传入不同的参数达到不同强度的混淆
	➢ 产品领先 国内唯一实现移动终端 H5 和浏览器 Web 应用加固技术，为 Web 应用提供安全保护 ➢ 多层防护：为开发者提供三种不同的安全策略，实现对平台、代码等方面进行保护 ➢ 一键防护：操作方式简便、一键式提交，不需要开发者参与，实现全过程自动混淆加密 ➢ 兼容性 :加密后，HTML5 网页兼容 Android、iOS、WP、Windows、MacOS 等主要操作系统
	➢ 常规模式：支持 AES 算法和 SM4 算法，同一个数据多次加密后的密文数据是一样的。 ➢ 一次一密模式：支持 AES 算法和 SM4 算法，同一个数据多次加密后的密文数据是随机的。 ➢ 单向模式 :客户端的方法不能相互加解密，只能和服务端相互加解密；服务端的方法不能相互加解密，只能和客户端相互加解密。