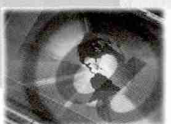



# 一种对 Android 应用资源索引表混淆方案的实现

刘洋,文伟平
(北京大学软件与微电子学院,北京 102600)

**摘　要**:由于 Android 应用具有被逆向、篡改、二次打包等风险,通过对 Android 应用中资源索引表文件进行混淆操作可以加大攻击者对 Android 应用逆向分析的难度。Android 应用中的资源索引表记录着该应用所有的字符串信息。通过对资源文件索引表格式的研究,提出了一种基于字符串置换的混淆方法,实现了对资源文件索引表的混淆,加大了攻击者对 Android 应用逆向分析的难度。

**关键词**:Android;资源文件索引表;混淆
**中图分类号**:TP309　　**文献标识码**:A
**doi:** 10.11959/j.issn.1000-0801.2016252

# An obfuscate implementation for Android resources index table

LIU Yang, WEN Weiping
School of Software and Microelectronics, Peking University, Beijing 102600, China

**Abstract:** Android application has risks of reverse, rewrite and repackage. Obfuscate Android resources index table will increase the difficulty of reverse analysis attack. Resources index table records the strings information in Android App. Through analyzing the structure of resources index table, a new obfuscate method was proposed to achieve obfuscate resources index table and increase the difficulty of reverse Android application.

**Key words:** Android, resources index table, obfuscate

## 1　引言

随着移动互联网时代的到来，传统 PC 设备逐渐退出大众视线，智能移动设备作为 PC 设备的替代品被大多数用户所接受。Android 系统凭借其开源的优势,占据了移动设备操作系统的主要份额。截至 2014 年 11 月,Android 官方应用市场 Google Play 上的应用数量已接近 140 万个[1]。

由于 Android 应用的迅猛发展和安全问题的日益突出与反制措施极不协调[2],大量攻击者将目光转移到逆向 Android 应用。攻击者在对应用实现逆向分析后,一方面可以通过抄袭他人源码窃取劳动成果;另一方面可以通过阅读他人代码逻辑,找寻 Android 应用中的漏洞、修改应用源码、对应用实施攻击。通过对应用中的核心文件进行混淆操作,可有效保护 Android 应用程序开发者的知识产权,在一定程度上避免了 Android 应用程序被逆向分析、盗版以及恶意篡改[3]。

当前对 Android 应用内 dex 文件的混淆技术较为成熟，有多种实现方案，且具有较高的兼容性。但是对于 Android 应用中资源文件索引表文件的混淆研究较少。当前资源文件索引表混淆方法使用范围最广的是由微信团

收稿日期:2016-07-31;修回日期:2016-09-25
基金项目:国家自然科学基金资助项目(No.61170282);信息网络安全公安部重点实验室基金资助项目(No.C14604)
**Foundation Items**: The National Natural Science Foundation of China (No.61170282), The Laboratory of the Ministry of Public Security Information Network (No.C14604)

进行调用时,是通过资源 ID。此类混淆操作影响攻击者对 Android 应用进行逆向的依据来源于,在反编译工具运行时会根据 arsc 文件表恢复资源 key 与资源内容的关系。

AndResGuard 混淆工具相比这种通过修改字符串偏移数组内容完成对于资源 key 的混淆置换的方法对 arsc 文件的修改更大。此类置换混淆方法的欺骗性更强,由于资源 key 的内容均来源于原始的 Android 应用,攻击者在阅读资源 key 时更容易误以为是未进行过混淆的元素。但 AndResGuard 工具可自动实现对应用包混淆后进行二次打包操作,使用起来更方便。

对 arsc 文件进行混淆操作只是对 Android 应用 res 目录下资源文件加固的一种实现方法,对于 res 文件夹下 Bitmap 类型文件的加密和 XML 文件的加密将更有利于对抗攻击者对 Android 应用的逆向分析。

## 参考文献:


[1] AppBrain Stats. Number of available Android applications[EB/OL]. (2015-02-16)[2016-06-13]. http://www.appbrain.com/stats/.

[2] 卿斯汉. Android 安全研究进展 [J]. 软件学报, 2016, 27(1): 45-71.
QING S H. Research process on Android security [J]. Journal of Software, 2016, 27(1): 45-71.

[3] 文伟平, 张汉, 曹向磊. 基于 Android 可执行文件重组的混淆方案的设计与实现[J]. 信息网络安全, 2016(5): 71-77.
WEN W P, ZHANG H, CAO X L. Design and implementation of the scheme of obfuscation based on the recombination of the Android executable file [J]. Netinfo Security, 2016 (5): 71-77.

[4] Shwen. 微信 Android 资源混淆打包工具[EB/OL]. (2015-10-12) [2016-06-30]. http://mp.weixin.qq.com/s?__biz=MzAwNDY 1ODY 2OQ ==&mid =208135658&idx =1&sn =ac9bd6b4927e9e 82f9fa14e396183a8f#rd.
Shwen. A resource obfuscate tool for wechat Android App[EB/OL]. (2015-10-12) [2016-06-30]. http://mp.weixin.qq.com/s?__biz=MzAwNDY1ODY2OQ ==&mid =208135658&idx =1&sn =ac9bd6b4927e9e 82f9fa14e396183a8f#rd.

[5] Beyond702. 手把手教你解析 resources.arsc[EB/OL]. (2016-06-30) [2016-07-01]. http://blog.csdn.net/beyond702/article/details/51744082.
Beyond702. Teach you analyze resources.arsc hand by hand[EB/OL]. (2016-06-30) [2016-07-01]. http://blog.csdn.net/beyond702/article/details/51744082.

[6] 罗升阳. Android 应用程序资源的编译和打包过程分析[EB/OL]. (2013-04-15) [2016-07-01]. http://blog.csdn.net/luoshengyang/article/details/8744683.
LUO S Y. Compiling and packaging process for Android resource program analysis [EB/OL]. (2013-04-15) [2016-07-01]. http://blog.csdn.net/luoshengyang/article/details/8744683.


[作者简介]


刘洋(1992-),女,北京大学软件与微电子学院硕士生,主要研究方向为网络与系统安全。

文伟平(1976-),男,博士,北京大学软件与微电子学院副教授,主要研究方向为网络攻击与防范、恶意代码研究、信息系统逆向工程。