第 39 卷 第 5 期
Vol.39 No.5
计 算 机 工 程
Computer Engineering
2013 年 5 月
May 2013

• 安全技术 •
文章编号：1000—3428(2013)05—0144—04 文献标识码：A 中图分类号：TP309.2

基于 Android 平台的访问权限机制优化方案

吴大勇，郑紫微
(宁波大学通信技术研究所，浙江 宁波 315211)

摘 要：为提高 Android 平台访问权限机制的安全性，提出一种基于 Android 平台的访问权限安全优化方案。将应用程序权限定向分为 4 类，获取不同权限组合的种类，量化其权限组合的安全威胁值，同时考虑免费应用程序更有可能是恶意程序的特点，通过应用程序权限安全威胁值判断其安全威胁级别。实验结果表明，该方案能有效区分应用程序的安全威胁级别，准确判断应用程序的安全威胁程度，提高 Android 访问控制安全性。

关键词：Android 平台；访问权限；权限分类；权限组合；安全威胁值；定向分类

Optimization Scheme of Access Permission Mechanism Based on Android Platform

WU Da-yong, ZHENG Zi-wei
(Institute of Communication Technology, Ningbo University, Ningbo 315211, China)

【Abstract】To improve the problem of the security of Android access permission mechanism, this paper proposes an optimization scheme for access permission security based on Android platform. It divides the Android permission into four categories, acquires categories of different permission combination, quantifies the permission combination security threat values and takes fact that free applications are more likely for malicious applications than paid applications into consideration, for judging application security threat level by application access permission security threat value. Experimental results show that the permission access security mechanism can effectively detect security threat level of applications, judge the degree of application security threat more accurately and achieve the goal of enhancing the security of Android access control.

【Key words】Android platform; access permission; permission classification; permission combination; security threat value; directional classification
DOI: 10.3969/j.issn.1000-3428.2013.05.031

1 概述

随着科学技术的发展，移动智能终端的应用在日常生活中越来越普遍，越来越多的人选择智能终端存储和操作个人隐私信息，这使得智能终端的安全问题逐渐成为人们关注的焦点，因此，智能终端安全研究的意义重大。

Android 是一个权限分离的系统[1]，其利用 Linux 已有的权限管理机制，通过为每一个应用程序分配不同的 uid 和 gid，使不同应用程序之间的私有数据访问达到隔离的目的。Android 框架包含许多安全机制，最显著的是沙盒安全机制，以此来强制访问控制组件间通信(Inter-component Communication, ICC)和 Android 核心资源[2]的访问。

Android 还在此基础上进行扩展，提供了权限机制，它主要是用来对应用程序可以执行的某些具体操作进行权限细分和访问控制，旨在允许或限制应用程序访问受限的 API 和资源。在默认情况下，Android 应用程序没有被授予权限，意味着它不能做任何影响用户体验或设备中数据的有害操作。如果某个权限与访问操作和资源对象绑在一起，那么必须获得这个权限才能访问该资源[3]。研发者可以在 AndroidManifest.xml 文件中包含一个或更多<uses-permission>标签来声明此权限，对应用程序授予的安全权限指定程序的保护域，对组件授予的安全权限指定组件的访问策略[4]。

本文介绍 Android 平台权限安全机制研究的进展，分析 ASESD 方案存在的不足，并在此基础上对其进行扩展优化。

基金项目：国家科技重大专项基金资助项目(2011ZX03002-004-02)；浙江省重点科技创新团队基金资助项目(2012R10009-04)；浙江省杰出青年科学基金资助项目(R1110416)；教育部高等学校博士学科点专项科研基金资助项目(20113305110002)；宁波市科技创新团队基金资助项目(2011B81002)
作者简介：吴大勇(1988－)，男，硕士研究生，主研方向：信息安全，数字无线通信；郑紫微，教授
收稿日期：2012-05-28 **修回日期：**2012-07-20 **E-mail：**wudayongwdy@163.com

2　基于 Android 平台权限的安全机制优化

权限机制是 Android 系统安全最重要的机制之一，某些恶意应用程序滥用访问权限攻击 Android 资源，进行程序保密性、完整性、可用性方面的破坏。

2.1　Android 权限安全的研究方案

针对 Android 权限滥用，Kirin 方案[5]最早的基于权限机制的应用程序认证防御方案，提出使用应用程序的权限来检查声明的权限是否违背了其设定的理想安全权限规则，若应用程序中的访问权限违背了该规则，Kirin 方案就会拒绝安装该应用程序；而 Apex 方案[6]在 Kirin 方案的基础上进行了扩展，用户可根据需要在安装应用程序时为权限设定条件并继续安装，允许用户使用应用程序访问部分终端资源，而限制应用程序访问关键的和代价高的终端资源。文献[7]阐述了 Android OS 对权限的申请、审核以及确认的过程是相当严格的，以此来说明这样的安全机制保障手机中数据的安全性。文献[8]分析了 Android 系统安全机制，指出现有的权限机制的漏洞，修改了 Android 内核，提出强制访问控制安全加固技术，对应用程序实施强制访问控制。文献[9]通过决策树结点对应的权限来判断该应用程序是恶意程序的可能性，指出免费的应用程序更有可能为恶意程序，典型的例子如图 1 所示。其中，P_M 为恶意应用的概率；P_B 为商业应用的概率。

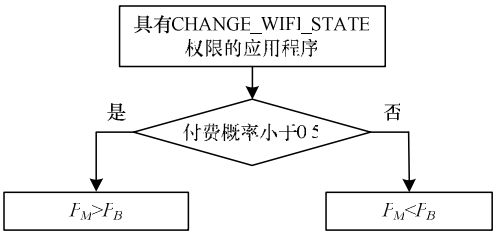


图 1　权限 CHANGE_WIFI_STATE 决策分析流程

在 Android 平台权限分类的决策树结构中，应用程序的访问权限 CHANGE_WIFI_STATE 是决定其是恶意程序最重要的分类权限，因为很多木马应用程序会通过使用 CHANGE_WIFI_STATE 权限以隐秘的方式来发送数据至指定服务器；而使用权限 READ_PHONE_STATE 的应用程序有可能是恶意程序，应用程序可通过该权限了解用户的通话状态及其联系人信息；……按权限分类决策树思想分析，具有不同访问权限的应用程序为恶意程序的概率是不一样的。

若应用程序的权限包含 CHANGE_WIFI_STAT 或者 READ_PHONE_STATE，则其为恶意应用程序的概率比两者都被声明的应用程序小得多，因此，权限安全问题并不在于应用程序获得了哪些安全权限，而在于这些访问权限之间的不同联系。

ASESD 方案[10]阐述了权限之间的联系才是判断一个应用程序是否带有恶意的关键，将应用程序的访问权限安全威胁程度作为量化的指标，通过计算两权限之间的安全威胁值来分析 Android 应用程序为恶意程序的可能性，同时也引用了安全距离，指出封闭的安全距离为这对权限组合的安全威胁不会因为相关组合的出现而增加。ASESD 方案提出了当相关的不封闭的安全距离同时出现时，通过其安全距离的乘积来判断应用程序安全威胁的增加程度，然而这种安全距离的乘积在一定程度上增加了应用程序的安全威胁值，扩大了应用程序安全威胁值的粗粒度。

本文方案改进的重点是减少 ASESD 方案中的安全距离相乘导致应用程序安全威胁值的增加，降低应用程序安全威胁值的粗粒度，提高应用程序安全威胁值的相对准确度。

2.2　ASESD 方案的改进

由于不同权限组合在很大程度上决定了应用程序的安全威胁级别，因此权限的组合不同将直接影响应用程序为恶意程序的概率。

2.2.1　Android 权限的定向分类

为得到权限组合的安全威胁级别，本文在 ASESD 方案基础上进行扩展，其扩展方案流程如图 2 所示。设定应用程序声明的权限为 4 类，将应用程序声明的权限进行定向分类：将与网络交互相关的具有严重安全威胁级别的权限归为一类，如 CHANGE_WIFI_STATE、INTERNET 等；将与用户个人数据相关的具有一般安全威胁级别的权限声明归为一类，如 READ_SMS、READ_CONTACTS 等；将与用户定位等相关的具有没有明显安全威胁级别的权限声明归为一类，如 ACCESS_GPS、ACCESS_FINE_LOCATION 等；将与手机硬件相关的具有无安全威胁的权限声明归为一类，如 BATTERY_STAT、WAKE_LOCK 等。

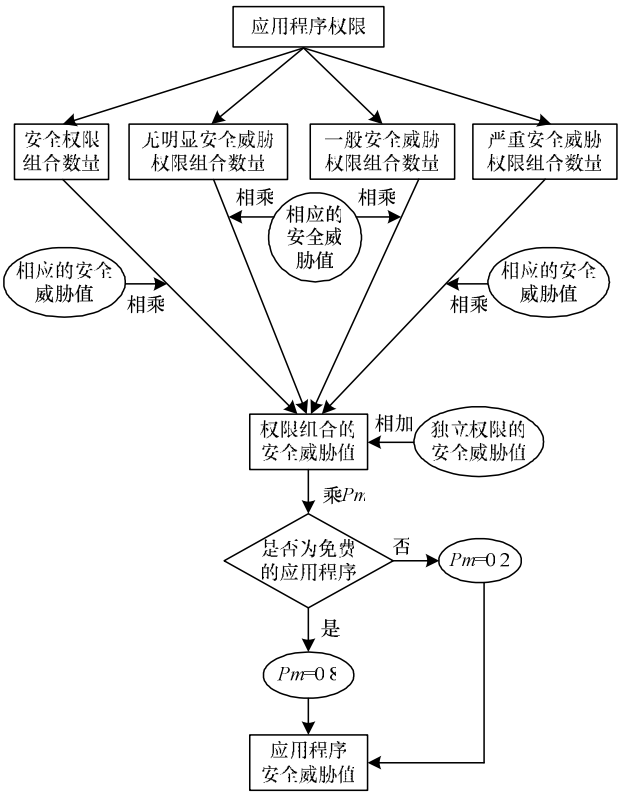


图 2　ASESD 方案的扩展优化

2.2.2 Android 权限威胁级别

为形象地将上述 Android 应用程序权限组合进行分类统计，本文将上述 4 类权限分别以 $\Phi_1 \sim \Phi_4$ 符号来代替，其权限的组合种类达到如下 11 种：$\Phi_1\ \Phi_2$，$\Phi_1\ \Phi_3$，$\Phi_1\ \Phi_4$，$\Phi_2\ \Phi_3$，$\Phi_2\ \Phi_4$，$\Phi_3\ \Phi_4$，$\Phi_1\ \Phi_2\ \Phi_3$，$\Phi_1\ \Phi_2\ \Phi_4$，$\Phi_1\ \Phi_3\ \Phi_4$，$\Phi_2\ \Phi_3\ \Phi_4$，$\Phi_1\ \Phi_2\ \Phi_3\ \Phi_4$。应用程序的权限组合会直接影响到程序的安全性，当应用程序权限组合复杂度越高，其安全威胁级别越高。

为反映应用程序的安全威胁值，本文拟设定 4 种不同应用程序权限组合安全威胁值：安全威胁值为 0、1、6、12 分别代表安全的权限组合，无明显安全威胁的权限组合，一般安全威胁级别的权限组合和具有安全威胁的权限组合。同时，本文也设定了不同应用程序单个权限的安全威胁值：安全威胁值为 0、1、2、3 分别代表安全的权限、无明显安全威胁的权限、一般安全威胁级别的权限和具有安全威胁的权限。

本文方案将应用程序权限组合的安全威胁值与单独权限安全威胁值相结合，便可得到 Android 应用程序所声明的安全威胁值，以此来判断该应用程序的安全威胁级别。

3 算法改进及仿真结果分析

综上所述，本文采取通过计算应用程序安全威胁值来分析应用程序为恶意程序的可能性。在应用程序安装前，可从程序安装器获得应用程序安装包的路径，通过 PackageManager 和 PackageInfo 接口获取到应用程序所声明的权限，对这些应用程序所声明的权限进行归类，计算出应用程序的安全威胁值，并将结果返回给程序安装器，程序安装器就将该应用程序的安全威胁值展现给用户。

相比于 ASESD 方案采取的是两权限之间的安全威胁值，本方案将应用程序的权限定向分为 4 类，ASESD 方案采取的计算公式为：

$$R = (\sum d_c + \sum d_{ij} \times d_{jk}) \times G \tag{1}$$

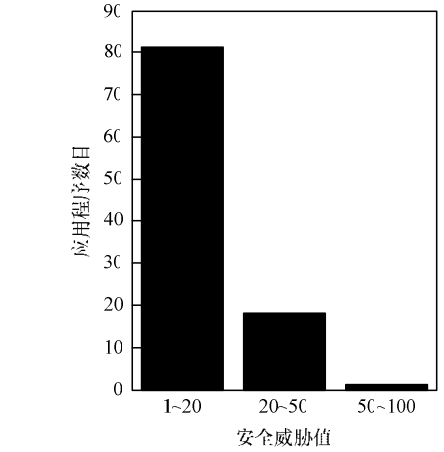
在式(1)中，d_c 是程序封闭的安全距离，d_{ij} 和 d_{jk} 是程序中相关的非封闭安全距离，其中，下标 j 代表 d_{ij} 和 d_{jk} 共享的安全权限；下标 i 和 k 代表 d_{ij} 和 d_{jk} 不同的安全权限；G 是程序安全权限类别的数量，R 是最后的程序威胁值。

而在本文方案中，本文提出的基于多种权限组合的访问控制方案，其权限组合种类最多可包含 11 种，且考虑了免费应用程序比付费的应用程序更有可能为恶意程序的事实，优化后的算法为：

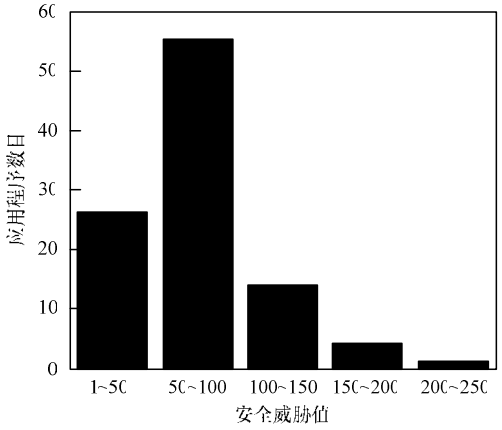
$$T = \left[\sum R_0 \times K_0 + \sum R_1 \times K_1 + \sum R_2 \times K_2 + \sum R_3 \times K_3\right] \times Pm \tag{2}$$

其中，T 代表该应用程序的安全威胁值；R_0 代表其单独权限的安全威胁值；R_1 代表其 2 类权限组合时的安全威胁值；R_2 代表其 3 类权限组合时的安全威胁值；R_3 代表其 4 类权限组合时的安全威胁值；K_0 代表单独权限安全威胁值对应的数量；$K_i(i=1,2,3)$ 代表其权限组合安全威胁值所对应的数量；p_m 代表其是否为免费应用程序的概率：若该应用程序是免费的应用程序，则 p_m 的值为 0.8；若该应用程序是付费的应用程序，则 p_m 的值为 0.2。

本文在 Android 应用商店中随机选取商用、游戏、系统工具、购物和娱乐 5 类，共 100 个应用程序，在安装这些应用程序时，可通过程序安装器获得其访问权限，将其权限按 ASESD 方案和本方案规则进行分类，分别使用式(1)和式(2)，得到应用程序的安全威胁值，通过仿真统计出应用程序安全威胁值分布情况，其结果如图 3 所示。



(a)ASESD 方案



(b)采用权限定向分类优化后的情况

图 3 权限安全威胁值分布情况

在图 3 中，可以清楚地看到，本文提出的基于应用程序安全威胁值权限定向分类的方案，大部分应用程序安全威胁值都集中在 0~150 之间，而只有少量应用程序安全威胁值超过 150，若应用程序安全威胁值超过 150，用户则需慎重考虑，此时应用程序有可能为恶意程序，若其安全威胁值超过 200，此时的应用程序极有可能为恶意程序。而在 ASESD 方案中，其应用程序安全威胁值比较集中，主要集中在 1~20 之间。就仿真结果而言，相比于 Kirin 方案，本文提出的基于权限机制防御方案量化了其权限的安全威胁

值；相比于 ASESD 方案，本文方案将应用程序安全威胁区域分为五大类，比 ASESD 方案更准确地确定应用程序的安全威胁程度，更有效、全面地判别出应用程序存在安全威胁的可能性。

4 结束语

本文提出一套基于 Android 平台访问权限的安全优化方案，通过量化其权限组合安全威胁值来分析 Android 应用程序为恶意程序的可能性。本文方案提出的基于多种权限组合的访问控制，其权限组合种类最多可包含 11 种，且考虑了免费应用程序比付费应用程序更有可能为恶意程序的事实，能更有效地反映出应用程序的安全威胁值，从而更可靠地分析出应用程序为恶意程序的可能性。下一步研究工作将根据应用程序运行时权限的使用情况，实时监控权限的不正常使用，动态地授权应用程序的权限，提高 Android 访问控制的安全性。

参考文献

[1] Shabtai A, Fledel Y, Kanonov U, et al. Google Android: A Comprehensive Security Assessment[J]. IEEE Trans. on Security Privacy, 2010, 8(2): 35-44.

[2] Bugiel S, Davi L, Dmitrienko A, et al. Practical and Lightweight Domain Isolation on Android[C]//Proc. of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. [S. l.]: ACM Press, 2011.

[3] 廖明华, 郑力明. Android 安全机制分析与解决方案初探[J]. 科学技术与工程, 2009, 26(3): 6351-6354.

[4] Enck W, Ongtang M, McDaniel P. Understanding Android Security[J]. IEEE Security & Privacy, 2009, 7(1): 50-57.

[5] Enck W, Ongtang M, McDaniel P. On Lightweight Mobile Phone Application Certification[C]//Proc. of ACM Conference on Computer and Communications Security. Chicago, USA: ACM Press, 2009.

[6] Nauman M, Khan S, Zhang Xinwen. Apex: Extending Android Permission Model and Enforcement with User-defined Runtime Constraints[C]//Proc. of the 5th ACM Symposium on Information, Computer and Communications Security. [S. l.]: ACM Press, 2010.

[7] 宋 杰, 党李成, 郭振朝, 等. Android OS 手机平台的安全机制分析和应用研究[J]. 计算机技术与发展, 2010, 20(6): 152-155.

[8] 屯聚虎, 周学海, 余艳玮, 等. Android 安全加固技术[J]. 电信科学, 2011, 20(10): 74-77.

[9] McLeese L, Watkins J, Cole J, et al. Permission System Evaluation on the Android Mobile Platform[EB/OL]. http://salsahpc.indiana.edu/test_page/I399-12/Collect-ion/2011/security1/Final%20Research%20Paper.do.

[10] Tang Wei, Jin Guang, He Jiaming. Extending Android Security Enforcement with a Security Distance Model[C]//Proc. of iTAP'11. Wuhan, China: [s. n.], 2011.

编辑 金胡考

(上接第 143 页)

5 结束语

本文对 GSI 中基于 PKI 认证机制的缺点进行分析，提出了基于 Kerberos 和 HIBC 的身份认证模型，对域内认证、域间认证、PKG 之间的认证机制进行阐述，分析结果表明，本文模型具有较高的安全性和效率，优于原有的认证机制，而且能较好地满足网格的自治性。

参考文献

[1] Foster I, Kesselman C. The Grid: Blueprint for a New Computing Infrastructure[M]. New York, USA: Morgan Kaufmann, 1999.

[2] 朱彦霞, 谭玉波, 华 南. 基于 Hash 算法的网格安全认证模型[J]. 现代电子技术, 2010, 33(1): 75-77.

[3] 赵会洋, 王 爽, 魏士伟. 网格安全模型中认证策略的研究[J]. 计算机技术与发展, 2010, 20(4): 171-174.

[4] Welch V, Foster I, Kesselman C. X.509 Proxy Certificates for Dynamic Delegation[C]//Proceedings of the 3rd Annual PKI R&D Workshop. [S. l.]: IEEE Press, 2004.

[5] 于代荣, 杨 扬. 基于分层身份的电子政务网格认证模型研究[J]. 计算机科学, 2008, 35(12): 55-61.

[6] Boneh D, Franklin M. Identity Based Encryption from the Weil Pairing[J]. SIAM Journal on Computing, 2003, 32(3): 586-615.

[7] Gentry C, Silverberg A. Hierarchical ID-based Cryptography[C]//Proceedings of the 8th International Conference on the Theory and Application of Cryptology and Information Security. Queenstown, New Zealand: [s. n.], 2002.

[8] 邢国稳, 薛胜军, 焦 峰, 等. 网格安全认证机制的研究与实现[J]. 武汉理工大学学报, 2010, 32(16): 169-172.

[9] 路晓明, 冯登国. 一种基于身份的多信任域网格认证模型[J]. 电子学报, 2006, 34(4): 577-582.

[10] 张红旗, 张文波, 张 斌, 等. 网格环境下基于身份的跨域认证研究[J]. 计算机工程, 2009, 35(17): 160-162.

编辑 金胡考