通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

杨欢1,张玉清1, 2,胡予濮1,刘奇旭2.基于权限频繁模式挖掘算法的Android恶意应用检测方法[J].通信学报,2013,(Z1):106~115

基于权限频繁模式挖掘算法的Android恶意应用检测方法

Android malware detection method based onpermission sequential pattern mining algorithm

投稿时间： 2013-07-03

DOI：10.3969/j.issn.1000-436x.2013.Z1.014

中文关键词：频繁模式 数据挖掘 恶意应用检测 权限特征 Android系统

英文关键词:sequential pattern mining data mining malware detection permission feature Android OS

基金项目:国家自然科学基金资助项目（61272481）；中国博士后科学基金资助项目（2011M500416，2012T50152）；北京市自然科学基金资助项目(4122089)；国家发改委信息安全专项基金资助项目（发改办高技[2012]1424）

作者	单位
杨欢1，张玉清1, 2，胡予濮1，刘奇旭2	1. 西安电子科技大学 综合业务网理论及关键技术国家重点实验室，陕西 西安 710071；2. 中国科学院大学 国家计算机网络入侵防范中心 北京 100190

中文摘要:

Android应用所申请的各个权限可以有效反映出应用程序的行为模式，而一个恶意行为的产生需要多个权限的配合，所以通过挖掘权限之间的关联性可以有效检测未知的恶意应用。以往研究者大多关注单一权限的统计特性，很少研究权限之间关联性的统计特性。因此，为有效检测Android平台未知的恶意应用，提出了一种基于权限频繁模式挖掘算法的Android恶意应用检测方法，设计了能够挖掘权限之间关联性的权限频繁模式挖掘算法—PApriori。基于该算法对49个恶意应用家族进行权限频繁模式发现，得到极大频繁权限项集，从而构造出权限关系特征库来检测未知的恶意应用。最后，通过实验验证了该方法的有效性和正确性，实验结果表明所提出的方法与其他相关工作对比效果更优。

英文摘要:

The permissions requested by Android applications reflect the behavior sequence of the application. While a generation of malicious behavior usually requires the cooperation of multiple permissions, so mining the association between permissions can effectively detect unknown malicious applications. Most researchers concerned the statistical properties of a single permission, and there was little researchers studying the statistical properties of the association between permissions. In order to detect unknown Android malwares, an Android malware detection method based on permission sequential pattern mining algorithm was proposed. The proposed method design a permission sequential pattern mining algorithm PApriori to dig out permissions association. PApriori algorithm could discover permission sequential pattern from 49 malware families and build the permissions association dataset to detect malware. The experiment results prove that it performs better than other related work in efficiency and accuracy.

查看全文 查看/发表评论 下载PDF阅读器

关闭