

主 题:	《一种Android应用程序隐私数据泄露检测方法》 外审退稿信	
发件人:	"yutong@ustb.edu.cn" <yutong@ustb.edu.cn>	2017-10-16 16:41:22
收件人:	casun@ustb.edu.cn	

尊敬的孙昌爱 先生/女士:

您好!  
您的文章《一种Android应用程序隐私数据泄露检测方法》没有通过我刊评审, 建议另投他刊。感谢您对《工程科学学报》的关注和支持!

以下是外审专家的审稿意见供您参考:

审稿专家返回审稿意见1:  
文章利用短信泄露隐私数据的危险权限组合对Kirin安全规则集进行扩展, 提出首先利用静态分析解析Android 应用程序的配置文件申请的访问权限集合, 识别存在隐私数据泄露风险的危险权限组合; 然后采用动态污点分析监控隐私数据的处理过程, 检测隐私数据泄露问题, 并开发了相应的支持工具DroidProtector。文章结构清晰完整, 思路较为明确。存在以下几个问题: 1.在2.2.3中语义表达不清, 对隐私数据动态跟踪过程描述不清, 且隐私数据源、隐私数据污点源、隐私数据污点、隐私数据标签、污点标签、隐私数据污点标记等术语未解释其含义及区别。 2.文章是对TaintDroid 架构进行扩展, 提出一个面向Android 应用程序的隐私数据泄露的检测框架, 但在实验部分尚未给出TaintDroid对194个应用程序的检测结果, 未看出DroidProtector大幅度提高应用程序的隐私数据泄露的检测能力。 3.全文出现了4次“误点”, 是与污点语义相同, 还是新的名词? 4.表2和表3中对于权限NA和N/A的含义未给出, 二者是否一致? 5.在2.3部分倒数第三行, 应把“TainDroid”改为“TaintDroid”。 6.在1.2已有研究工作中, 静态分析和动态检测的方法仅仅针对一个研究者的工作总结的, 是否充分?

《工程科学学报》编辑部  
(原北京科技大学学报)