稿号： 2017-70332

文题： 基于扩展权限组合的Android应用程序隐私数据泄露检测方法

详细意见：

论文提出将组合权限判定与动态分析相结合，判定android应用程序是否存在隐私泄漏行为。论文提出了一些新的规则使得具体检测结果相比现有Kirin规则集更准确，但从以下方面仍存在有待改进之处：

1. 与Kirin比较精度，意义有限，因为Kirin针对的是早期android版本；另一方面，本文方法仅改进了规则集，并没有在利用权限组合的方法上有所创新。

2. 实际上本文方法通过先静态分析权限、后用TaintDroid分析的方式，从总体上减少了动态分析的开销，但由于TaintDroid本身不是基于权限的，因而有可能存在这种情况：本文方法的权限组合检测结果显示不存在隐私泄漏的应用（根据本文第2.2节方法不会进入动态分析阶段），这些应用由TaindDroid分析的结论可能是会泄漏隐私的。也就是说本文没有证明用权限组合静态检测的结果是可靠的。因而存在本文方法精度低于TaintDroid分析精度的可能，那么第3.3节仅比较本文工具与TaintDroid的性能就不够，因为一般来讲服务器端的检测不支持用牺牲精度来提升效率。因此，作者需要进一步比较本文工具与TaintDroid的分析精度，看是否有提升。

3. 论文对TaintDroid的动态分析进行的改进，使TaintDroid支持短信发送API作为sink，这一改进也主要是在规则方面，较为平凡，从动态分析方法上并未见明显贡献。

4. 所使用用例集规模较小，难以说明方法优点具有普适性。

关闭窗口