研究内容简介：

1. 选题背景

近年来，手机已经成为人们生活中必不可少的工具之一，移动操作系统也备受人们的关注。Android作为几大移动操作系统的佼佼者，在移动平台市场中占据不小的份额。据NET MARKETSHARE的数据显示，Android在2014年7月首次超越IOS跃居市场份额榜首，直至2017年7月，android市场份额占比64.38%[1]。然而由于Android的开放性，安装在Android系统上的诸多app在为用户带来便捷和多种服务的同时，也引入了新的问题 - 个人隐私的泄露。研究表明，乐观估计高达90%的手机应用会访问获取用户的隐私信息[2]。这意味着不仅是恶意软件，合法的手机应用也会借助各种途径获取用户的隐私信息，比如位置信息等。因此，如何有效地检测及防御安卓应用对用户个人隐私信息的窃取，已成为日益关注的热点.

常用的检测隐私信息泄露的方法分为静态分析和动态分析两种，由于静态分析方法不能检测运行时信息，例如当app开发人员使用例如JAVA反射机制，代码加密或者动态加载等技术的代码时静态分析方法就不能很好地起到检测作用。然而由于Google对安卓系统进行了大规模的改动，以往的依赖于Dalvik虚拟机的动态污点分析已经不能满足现在的需求。

除了安卓系统关于运行时的改动外，安卓手机架构的升级同样带来了影响。随着2013年苹果公司推出首个64位架构的A7处理器，64位移动芯片的时代正式开启。ARM公司随后在2014年推出了64位架构的ARMv8-A。与之相应的是，2014年10月Android在新推出的5.0版本中加入了对64位的支持，成为IOS 8之后第二个支持64位的移动操作系统，64位手机芯片成为越来越多的手机厂商的选择。

因此需要结合安卓系统的诸多特性对动态污点技术进行改进完善， 以实现对安卓应用窃取用户隐私信息的检测及防御。

1. 研究内容

本次研究是针对日益严重的安卓应用窃取用户隐私信息的问题，拟采用动态污点分析技术，选定Android 6.0.1系统版本，在AArch64的架构上，结合Android系统新特性，以实现对安卓系统中所有app的动态监测和防御。研究内容主要包括：Arm架构- AArch32（ARM 32-bit Architecture）和AArch64（ARM 64-bit Architecture）在安卓的区别，即arm与arm64的区别，Android运行时的新特性，动态污点分析技术与新特性相结合的具体实现。

2.1 arm vs arm64

Android系统支持arm/arm64/x86/x86\_64/mips/mips64等架构，相比于其他架构相比，Android最早支持ARM，对ARM的支持也最为完善，且主要应用于手机市场；x86/x86\_64架构目前已经支持的比较完善，主要应用于上网本；mips/mips64目前正在移植完善中，主要应用于智能家电/上网本领域。

arm即为ARMv7,32位的架构，支持A32和Thumb指令集，

相比于AArch32而言，AArch64是ARMv8内全新的架构，使用全新的A64指令集。

2.2Android运行时新特性

Google从安卓4.4时引入ART运行时作为一个备选项，在安卓5.0时使用ART彻底替代了Dalvik虚拟机，并且在随后推出的安卓6.0中将默认的编译器后端从Quick模式变为了Optimizing模式，并且支持64位处理器。

论文进展情况：

工作成果：

1. 已完成论文工作内容
2. 阶段性成果
3. 主要创新点

计划及进度安排：

问题及整改方案：

参考文献：

[1]NET MARKETSHARE.Mobile/Tablet Operating System Market Share.http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=8&qpcustomd=1. 2017

[2]Ge Y, Deng B, Sun Y, et al. A Comprehensive Investigation of User Privacy Leakage to Android Applications[C]//Computer Communication and Networks (ICCCN), 2016 25th International Conference on. IEEE, 2016: 1-6.