学　　号　2015301500150
密　　级

武汉大学本科毕业论文

移动应用的动态行为捕获

院 (系) 名 称:　国家网络安全学院

专 业 名 称:　信息安全

学 生 姓 名:　蹇奇芮

指 导 教 师:　傅建明　教授

二〇一九年五月

BACHELOR'S DEGREE THESIS
OF WUHAN UNIVERSITY

Dynamic behavior capture for mobile apps

School (Department): School of Cyber Science and Engineering

Major: Information Security

Candidate: QiRui Jian

Supervisor: Prof. JianMing Fu

Wuhan University

May, 2019

郑 重 声 明

本人呈交的学位论文, 是在导师的指导下, 独立进行研究工作所取得的成果, 所有数据、图片资料真实可靠. 尽我所知, 除文中已经注明引用的内容外, 本学位论文的研究成果不包含他人享有著作权的内容. 对本论文所涉及的研究工作做出贡献的其他个人和集体, 均已在文中以明确的方式标明. 本学位论文的知识产权归属于培养单位.

本人签名: _____ 日期: _____

摘　　要

智能终端设备的盛行使得移动平台的应用

关键词: 毕业论文; LaTeX; 模板;

ABSTRACT

The prevalence of mobile platforms, the large market share of Android, plus the openness of the Android Market makes it a hot target for malware attacks. Once a malware sample has been identified, it is critical to quickly reveal its malicious intent and inner workings.

In this paper we present DroidScope, an Android analysis platform that continues the tradition of virtualization-based malware analysis. Unlike current desktop malware analysis platforms, DroidScope reconstructs both the OSlevel and Java-level semantics simultaneously and seamlessly. To facilitate custom analysis, DroidScope exports three tiered APIs that mirror the three levels of an Android device: hardware, OS and Dalvik Virtual Machine. On top of DroidScope, we further developed several analysis tools to collect detailed native and Dalvik instruction traces, profile API-level activity, and track information leakage through both the Java and native components using taint analysis. These tools have proven to be effective in analyzing real world malware samples and incur reasonably low performance overheads..

Key words: LaTeX;

目　　录

1 先说重要的

1.1 具体使用步骤

Step 1 进入 includefile 文件夹, 打开 frontmatter.tex, backmatter.tex 这两个文档, 分别填写 (1) 中文摘要、英文摘要, (2) 致谢.

Step 2 打开主文档 Bachelor–template.tex, 填写题目、作者等等信息, 书写正文.

Step 3 使用 XeLaTeX 编译. 具体见 1.2 节.

1.2 编译的方法

默认使用 XeLaTeX 编译, 直接生成 pdf 文件.

若另存为新文档, 请确保文档保存类型为 :UTF-8. 当然目前很多编辑器默认文字编码为 UTF-8. WinEdt 9.0 之后的版本都是默认保存为 UTF-8 的.

1.3 文档类型选择

文档类型有 2 种情形:

`\documentclass{WHUBachelor}`	毕业论文
`\documentclass[forprint]{WHUBachelor}`	毕业论文打印版

相关解释见下节.

1.4 打印的问题

i) 关于文档选项 forprint: 交付打印时, 建议加上选项 forprint, 以消除链接文字之彩色, 避免打印字迹偏淡.

ii) 打印时留意不要缩小页面或居中. 即页面放缩方式应该是 “无”(Adobe Reader XI 是选择 “实际大小”). 有可能页面放缩方式默认为 “适合可打印区域”, 会导致打印为原页面大小的 97%. 文字不要居中打印, 是因为考虑到装订, 左侧的空白留得稍多一点 (模板已作预留).

iii) 遗留问题: 封面需要打印部重新制作. 校内打印部通常有现成的模板. 我们自己做的封面, 打印部不一定好用.

问: 生成 PDF 文件时, 不能去掉目录和文章的引用彩色方框, 请问怎么解决?

答: 方框表示超级链接, 只在电脑上看得见. 实际打印时, 是没有的. 另外, 文档类型加选项 forprint 之后, 这些框框会隐掉的.

本文档下载更新地址: `http://aff.whu.edu.cn/huangzh/`. 使用之前, 请移步查看是否有更新.

问题反馈及建议, 请联系: huangzh@whu.edu.cn.

2 杂七杂八的话

2.1 Readme

模板文件的结构, 如下表所示:

Bachelor-template.tex		主文档. 在其中填写正文.
includefile 文件夹	frontmatter.tex	郑重声明、中英文摘要.
	backmatter.tex	致谢.
figures 文件夹		存放图片文件.
WHUBachelor.cls		定义文档格式的 class file. 不可删除.

无需也不要改变、移动上述文档的位置.

如果不习惯用 `\include{ }` 的方式加入 “子文档”, 当然可以把它们合并在主文档, 成为一个文档. (但是这样并不会给我们带来方便.)

利用 WinEdt 的 Project tree, 可以方便地管理这些文件:

- 点击 WinEdt 窗口的 Project Tree 按键;
- 再点击 WinEdt 窗口的 Set Main File 按键;

接下来的管理, 已经清楚地展示在跳出的窗口中了. 再去处理其他的文件时, 还要点击 WinEdt 窗口的 Remove Main File 按键.

2.2 更新记录

2016 年 06 月更新: 正文字体为小四号; 英文字体为 Times New Roman; 修订图表标题的字体、字号; 修订目录的字号; 修订附录章节编号的问题. 非常感谢武汉大学数学与统计学院 2012 级张仕俊、林颖倩、宋[illegible]辰等同学.

2016 年 05 月更新: 参考文献加到目录. 感谢武汉大学经济与管理学院的郑中天同学. [上次修订使用的版本有误, 非常抱歉.]

2016 年 02 月更新: 调整为适应 TeX Live 2015 的版本.

2014 年 06 月更新: 修改章节标题、声明标题、图表标题的字体和大小. 再次感谢孙启航同学.

2014 年 05 月更新: 参考文献加到目录. 感谢武汉大学计算机学院孙启航同学、数学与统计学院李振坤同学指出这个纰漏.

2013 年 12 月更新: 加上英文封面. 教务部的写作规范中的附例, 并没有英文封面. 但是遇到很多同学说要加上.

2.3 字体调节

`\songti`	宋体
`\heiti`	**黑体**
`\fangsong`	仿宋
`\kaishu`	楷书

2.4 字号调节

字号命令: `\zihao`

\zihao{0} 初号字 English

\zihao{-0} 小初号 English

\zihao{1} 一号字 English

\zihao{-1} 小一号 English

\zihao{2} 二号字 English

\zihao{-2} 小二号 English

\zihao{3} 三号字 English

\zihao{-3} 小三号 English

\zihao{4} 四号字 English

\zihao{-4} 小四号 English

\zihao{5} 五号字 English

\zihao{-5} 小五号 English

\zihao{6} 六号字 English

\zihao{-6} 小六号 English

\zihao{7} 七号字 English

\zihao{8} 八号字 English

2.5 已加入的常用宏包

cite 参考文献引用, 得到形如 [3-7] 的样式.

color,xcolor 支持彩色.

enumerate 方便自由选择 enumerate 环境的编号方式. 比如

\begin{enumerate}[(a)] 得到形如 (a), (b), (c) 的编号.

\begin{enumerate}[i)] 得到形如 i), ii), iii) 的编号.

另外要说明的是, itemize, enumerate, description 这三种 list 环境, 已经调节了其间距和缩进, 以符合中文书写的习惯.

2.6 标点符号的问题

建议使用半角的标点符号, 后边再键入一个空格. 特别是在英文书写中要注意此问题!

双引号是由两个左单引号、两个右单引号构成的: `` ''. 左单引号在键盘上数字 1 的左边.

但是, 无论您偏向于全角或半角, 强烈建议您使用实心的句号, 只要您书写的是自然科学的文章. 原因可能是因为, 比如使用全角句号的句子结尾处的 "x。" 容易误为数学式 x_0(`$x_0$`) 吧.

2.7 引用的问题

2.7.1 参考文献的引用

参考文献的引用, 用命令 `\cite{ }`. 大括号内要填入的字串, 是自命名的文献条目名.

比如, 通常我们会说:

关于此问题, 请参见文献 [2]. 作者某某还提到了某某概念[1].

上文使用的源文件为:

```
关于此问题, 请参见文献 \cite{r2}. 作者某某还提到了某某概念 \upcite{r1}.
```

其中 `\upcite` 是自定义命令, 使文献引用呈现为上标形式.

(**注意**: 这里文献的引用, 有时需要以上标形式出现, 有时需要作为正文文字出现, 为什么?)

另外, 要得到形如 [1, 3, 4, 5] 的参考文献连续引用, 需要用到 cite 宏包 (模板已经加入), 在正文中使用 `\cite{r1,r3,r4,r5}` 的引用形式即可. 或者, 连续引用的上标形式: 使用 `\upcite{r1,r2,r3}`, 得到[1, 2, 3].

2.7.2 定理和公式的引用

定理 2.7.1 **(谁发现的)** 最大的正整数是 1.

证明 要找到这个最大的正整数, 我们设最大的正整数为 x, 则 $x \geqslant 1$, 两边同时乘以 x, 得到

$$x^2 \geqslant x. \tag{2.1}$$

而 x 是最大的正整数, 由 (2.1) 式得到

$$x^2 = x.$$

所以

$$x = 1. \qquad \square$$

定理 2.7.1 是一个重大的发现.

定义 2.7.1 (**整数**) 正整数 (例如 1, 2, 3)、负整数 (例如 −1, −2, −3) 与零 (0) 合起来统称为**整数**.

注 2.7.1 整数集合在数学上通常表示为 Z 或 $\mathbb{Z}$, 该记号源于德语单词 Zahlen(意为 “数”) 的首字母.

性质 2.7.1 任意两个整数相加、相减、相乘的结果, 仍然是整数.

例 2.7.1 $1 + 2 = 3$.

推论 2.7.1 在整数集合内, 相加、相减、相乘运算是封闭的.

2.8 图形与表格

支持对 eps, pdf, jpg 等等常见图形格式.

再次澄清一个误会: LaTeX 支持的图形格式绝非 eps 这一种. 无需特意把图片转化为 eps.

用形如 `\includegraphics[width=12cm]{Daisy.jpg}` 的命令可以纳入图片.

如图 2.1 是一个纳入 jpg 图片的例子.

表格问题, 建议使用 “三线表”, 如表 2.1.

图 2.1　一个彩色 jpg 图片的例子

表 2.1　一般三线表

123	4	5	123	4	5123	4	5	123	4	5
67	890	13	123	4	5123	4	5	123	4	5
67	890	13	123	4	5123	4	5	123	4	5
67	890	13	123	4	5123	4	5	123	4	5

3 其他事项

以下是广告时间, 插播一段广告:

- 插图的制作, 建议用 pgf, 也叫 tikz. pgf 的长处是源文件直接植入 TEX 文档, 管理起来非常方便. 这里有我写的一个关于初次使用 pgf 的帖子:
  http://bbs.ctex.org/forum.php?mod=viewthread&tid=30480.
- 生成参考文献, 建议使用 BibTeX. 这里有我写的一个文档:
  http://bbs.ctex.org/forum.php?mod=viewthread&tid=26056.

  使用 BibTeX 做参考文献时, 借助 EndNote 或者 NoteExpress, 可以非常漂亮简单地解决 bib 文件的录入问题. NoteExpress 在校图书馆网站有正版软件提供下载. 当然 EndNote 本身就是 Thomson Corporation 推出的 (和 SCI 搜索引擎是同一家公司), 和多个重要文献搜索引擎有良好的功能配合.

  Google 学术搜索也提供了文献的 bib 格式. 录入参考文献时, 偶尔用一用 Google 学术搜索, 还可以核查或减少录入的错误, 并减少录入的工作量.
- 幻灯片的制作, 建议使用 Beamer. 这里有我写的一个模板, 谨供参考:
  http://bbs.ctex.org/forum.php?mod=viewthread&tid=27695.

参考文献

[1] 作者. 文章题目 [J]. 期刊名, 出版年份，卷号 (期数): 起止页码.

[2] 作者. 书名 [M]. 版次. 出版地：出版单位，出版年份：起止页码.

[3] 邓建松等, 《LaTeX 2ε 科技排版指南》, 科学出版社.

[4] 吴凌云, 《CTeX FAQ (常见问题集)》, Version 0.4, June 21, 2004.

[5] Herbert Voß, Mathmode, `http://www.tex.ac.uk/ctan/info/math/voss/mathmode/Mathmode.pdf`.

致　　谢

感谢你, 感谢他和她, 感谢大家.

附录 A　测试

A.1　第一个测试

测试公式编号

$$1+1=2. \tag{A.1}$$

表格编号测试

表 A.1　测试表格

11	13	13	13	13
12	14	13	13	13

附录 B　附录测试

测试

附录 C　附录测试

测试