RT Embedded http://www.kontronn.com

Android 应用的反编译

徐尤华，熊传玉

(广东松山职业技术学院，广东 韶关 512126)

摘 要：随着计算机软件的广泛应用，反编译已成为软件逆向工程的重要研究领域，文章给出了一种反编译 Android 应用的方法。通过对 Android 应用的反编译，可以推导出他人的思路、原理、结构、算法、处理过程、运行方法等设计要素，作为自己开发软件时的参考，或者直接用于自己的软件产品中。

关键词：Android；反编译；应用

中图分类号：TP393.12 **文献标识码**：A

Decompile of Android Application

XU You- hua，XIONG Chuan- yu

(Guangdong Songshan Polytechnic College, Shaoguan 512126,China)

Abstract：With extensive use of computer software，decompile has become an important research area in the software reverse engineering，this paper presents a way to decompile android applications. Through decompile，we can derive the ideas, principles, structure, algorithms, processes, operating methods and other design elements of others，we can use these as our own reference when developing software，or directly to our software products.

Key words: Android; decompile; application

自从 Android 系统发布以来，网络上出现了大量的基于 Android 系统的应用，这些应用都积累着开发者的设计经验，如果这些应用能够公开源码的话，可以让更多的人加入到应用开发队伍中来，并且能够以更快的速度成长，从而提供更多的优秀的应用产品，这无疑能够很好的推动 Android 应用产业的发展。但是各个厂商和开发者出于各种原因，都不会公开自己应用的源代码，通过对应用的反编译可以达到学习其设计思想的目的。

1 基本方法

学习已有的应用，我们一般需要查看应用的各种 xml 配置文件和各种 java 源文件。通过 xml 文件可以查看到应用的各种配置数据，如 UI 界面的设计；通过 java 源文件可以查看到应用的具体功能的实现。因此通过反编译只要能够得到 xml 文件和 java 文件即可。

以下反编译过程以一个朗读英文文章的应用为例，该应用可以从如下地址获取：http://download.csdn.net/detail/xyh9717/3626207，下载后是一个压缩包 TestSpeechEnglish.rar，解压后在 bin 文件夹下可以找到所需应用：TestSpeechEnglis.apk。

该应用运行界面如下图 1 所示，点击“开始朗读”按钮后开始朗读输入的内容。

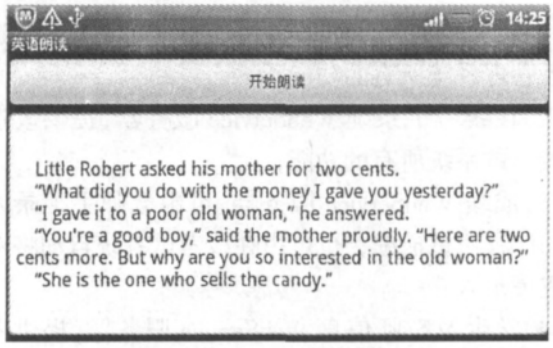

图 1 应用运行界面

2 xml 文件的反编译

要获取到应用中的 xml 文件，需要在如下地址下载 apktool1.4.1.tar.bz2 和 apktool- install- windows- r04-brut1.tar.bz2 两个工具：http://code.google.com/p/android-apktool/downloads/list。下载完成后将两个压缩包中内容解压到同一个文件夹中，本文将这些文件解压到 D:

RT Embedded http://www.kontronn.com

\decompiler 文件夹下。

将 TestSpeechEnglis.apk 也复制到 D:\decompiler 文件夹下，将命令行路径切换到 D:\decompiler 下，执行命令:apktool d TestSpeechEnglis.apk，命令执行完毕后，在 D:\decompiler\TestSpeechEnglis 可以查看所需 xml 文件，通过对比 TestSpeechEnglish.rar 中 xml 文件，内容基本相同，下面给出 main.xml 反编译结果：

```
<?xml version="1.0" encoding="utf- 8"?>
<LinearLayout android:orientation="vertical" android:layout_
width
    ="fill_parent" android:layout_height="fill_parent"
    xmlns:android="http://schemas.android.com/apk/res/an-
droid">
  <Button android: layout_gravity = "center" android:id = "@id/
button1"
    android:layout_width="fill_parent" android:layout_height=
    "wrap_content" android:text=" 开始朗读 " />
  <EditText android:id="@id/editText1" android:layout_width=
"fill_parent" android:layout_height="fill_parent"
    android:hint=" 输入要朗读的英文文章 " />
</LinearLayout>
```

3 java 文件的反编译

java 文件的反编译需要分两步来做：

第一步 将 dex 文件转为 jar 文件。在如下地址下载 dex2jar- 0.0.0.11- SNAPSHOT.zip 工具：http://code.google.com/p/dex2jar/downloads/list，下载完成后解压到 D:\decompiler 中。将 TestSpeechEnglis.apk 用解压软件打开，复制出里面的 classex.dex 文件，在命令行执行：dex2jar classes.dex，可以得到 classes.dex.dex2jar.jar 文件；

第二步 将 jar 文件反编译为 java 文件。在如下地址下载 Java Decompiler 工具：http://laichao.google-code.com/files/jdgui.zip，解压后打开 jd- gui.exe，用该工具打开第一步得到的 jar 文件即可查看到所有 java 文件源码，下面给出 SpeechEnglish.java 反编译后 onCreate () 方法代码:

```
public void onCreate (Bundle paramBundle)
  {
    super.onCreate (paramBundle) ;
    setContentView (2130903040) ;
    Button localButton = (Button) findViewById (2131034112) ;
    this.btn = localButton;
    EditText localEditText = (EditText) findViewById (21310
34113) ;
    this.edit = localEditText;
    this.btn.setOnClickListener (this) ;
     TextToSpeech localTextToSpeech1 = new TextToSpeech
(this, this) ;
    this.speech = localTextToSpeech1;
    this.edit.setText ("...省略 ") ;
     TextToSpeech localTextToSpeech2 = new TextToSpeech
(this, this) ;
    this.speech = localTextToSpeech2;
  }
```

通过对比 TestSpeechEnglish.rar 中 java 文件，内容基本相同，只是 id 号换成了具体的数值，其他差别不大。

4 结束语

本文给出了 Android 应用的反编译方法，通过反编译能够得到应用的 xml 和 java 文件，通过查看这些文件我们可以学习开发者的设计思想，从而快速学习，进而开发出更优秀的 Android 应用。

参考文献：

[1] 王向辉.Android 应用程序开发[M].北京:清华大学出版社，2010.

[2] 林城.Google Android 2.X 应用开发实战[M].北京:清华大学出版社，2011.

[3] ITeye 技术网站[EB/OL].http://www.iteye.com.

[4] Android Developers[EB/OL].http://developer.android.com.

Created in Master PDF Editor

嵌入式资源免费下载

总线协议：

1. 基于 PCIe 驱动程序的数据传输卡 DMA 传输
2. 基于 PCIe 总线协议的设备驱动开发
3. CANopen 协议介绍
4. 基于 PXI 总线 RS422 数据通信卡 WDM 驱动程序设计
5. FPGA 实现 PCIe 总线 DMA 设计
6. PCI Express 协议实现与验证
7. VPX 总线技术及其实现
8. 基于 Xilinx FPGA 的 PCIE 接口实现
9. 基于 PCI 总线的 GPS 授时卡设计
10. 基于 CPCI 标准的 6U 信号处理平台的设计
11. USB30 电路保护
12. USB30 协议分析与框架设计
13. USB 30 中的 CRC 校验原理及实现
14. 基于 CPLD 的 UART 设计
15. IPMI 在 VPX 系统中的应用与设计
16. 基于 CPCI 总线的 PMC 载板设计
17. 基于 VPX 总线的工件台运动控制系统研究与开发

VxWorks：

1. 基于 VxWorks 的多任务程序设计
2. 基于 VxWorks 的数据采集存储装置设计
3. Flash 文件系统分析及其在 VxWorks 中的实现
4. VxWorks 多任务编程中的异常研究
5. VxWorks 应用技巧两例
6. 一种基于 VxWorks 的飞行仿真实时管理系统
7. 在 VxWorks 系统中使用 TrueType 字库
8. 基于 FreeType 的 VxWorks 中文显示方案
9. 基于 Tilcon 的 VxWorks 简单动画开发
10. 基于 Tilcon 的某武器显控系统界面设计
11. 基于 Tilcon 的综合导航信息处理装置界面设计

Created in Master PDF Editor

12. VxWorks 的内存配置和管理
13. 基于 VxWorks 系统的 PCI 配置与应用
14. 基于 MPC8270 的 VxWorks BSP 的移植
15. Bootrom 功能改进经验谈

Linux：

1. Linux 程序设计第三版及源代码
2. NAND FLASH 文件系统的设计与实现
3. 多通道串行通信设备的 Linux 驱动程序实现
4. Zsh 开发指南-数组
5. 常用 GDB 命令中文速览
6. 嵌入式 C 进阶之道
7. Linux 串口编程实例
8. 基于 Yocto Project 的嵌入式应用设计

Windows CE：

1. Windows CE.NET 下 YAFFS 文件系统 NAND Flash 驱动程序设计
2. Windows CE 的 CAN 总线驱动程序设计
3. 基于 Windows CE.NET 的 ADC 驱动程序实现与应用的研究
4. 基于 Windows CE.NET 平台的串行通信实现
5. 基于 Windows CE.NET 下的 GPRS 模块的研究与开发
6. win2k 下 NTFS 分区用 ntldr 加载进 dos 源代码
7. Windows 下的 USB 设备驱动程序开发
8. WinCE 的大容量程控数据传输解决方案设计
9. WinCE6.0 安装开发详解
10. DOS 下仿 Windows 的自带计算器程序 C 源码
11. G726 局域网语音通话程序和源代码
12. WinCE 主板加载第三方驱动程序的方法
13. WinCE 下的注册表编辑程序和源代码
14. WinCE 串口通信源代码
15. WINCE 的 SD 卡程序[可实现读写的源码]
16. 基于 WinCE 的 BootLoader 研究

Creator Master PDF Editor

PowerPC：

1. Freescale MPC8536 开发板原理图
2. 基于 MPC8548E 的固件设计
3. 基于 MPC8548E 的嵌入式数据处理系统设计
4. 基于 PowerPC 嵌入式网络通信平台的实现
5. PowerPC 在车辆显控系统中的应用
6. 基于 PowerPC 的单板计算机的设计
7. 用 PowerPC860 实现 FPGA 配置

ARM：

1. 基于 DiskOnChip 2000 的驱动程序设计及应用
2. 基于 ARM 体系的 PC-104 总线设计
3. 基于 ARM 的嵌入式系统中断处理机制研究
4. 设计 ARM 的中断处理
5. 基于 ARM 的数据采集系统并行总线的驱动设计
6. S3C2410 下的 TFT LCD 驱动源码
7. STM32 SD 卡移植 FATFS 文件系统源码
8. STM32 ADC 多通道源码
9. ARM Linux 在 EP7312 上的移植
10. ARM 经典 300 问
11. 基于 S5PV210 的频谱监测设备嵌入式系统设计与实现

Hardware：

1. DSP 电源的典型设计
2. 高频脉冲电源设计
3. 电源的综合保护设计
4. 任意波形电源的设计
5. 高速 PCB 信号完整性分析及应用
6. DM642 高速图像采集系统的电磁干扰设计
7. 使用 COMExpress Nano 工控板实现 IP 调度设备

Created in Master PDF Editor

Created in Master PDF Editor