|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 武汉大学国家网络安全学院教学实验报告 | | | | | |
| 课程名称 | 网络对抗演练 | | | 实验日期 | 2024/5/24 |
| 实验名称 | 逆向工程-移动安全 | | | 实验周次 | 第2周 |
| 姓名 | 学号 | | | 专业 | 班级 |
|  |  | | |  |  |
|  |  | | |  |  |
|  |  | | |  |  |
|  |  | | |  |  |
|  |  | | |  |  |
|  |  | | |  |  |
| 1. 实验目的及实验内容   （本次实验所涉及并要求掌握的知识；实验内容；必要的原理分析） | | | | | |
| **实验1和实验2 ，2选1 ，根据学习情况自行选择解答**  **实验目的：**  **掌握移动逆向基础及字节码修改**  **实验环境：**   1. Windows操作系统 2. apktool、AndroidKiller、Jadx、adb   **实验题目1：**  完成逆向题的qiantang apk题目，实现购买成功的功能实现效果   1. 对Android解压，进行文件格式的基本分析   首先使用Android Killer打开钱塘apk文件如下图所示    目录下包含有assets目录，该目录保存应用使用的如文本、音频和视频等格式的原始文件；目录下的lib包含应用使用的本地库文件；original目录包含APK原始签名信息文件，可以用来查看签名详情；res目录包含应用的资源文件，如布局、字符串、图片等，这些文件在APK编译的过程中会被直接编译到resources.arsc中，在这里以原始形式存在；smali目录包含反编译后的smali代码，代表了应用的逻辑和功能；AndroidManifest.xml文件描述了应用的包名、组件（如活动、服务等）、所需权限和其他应用级别的属性。经过 Apktool 反编译后，这个文件应该是以可读的 XML 格式存在，可以查看或修改。  apktool.yml文件是 Apktool 在反编译过程中生成的一个配置文件，包含了反编译时使用的一些设置和 APK 特定的信息，如版本号和编译信息。   1. 静态分析程序   因为本次的试验任务需要修改的内容是对支付功能进行修改，所以在分析程序时主要针对支付功能进行分析  首先使用jadx打开apk文件，因为在上一步中我们已经知道主要的支付功能代码保存到了com.ttzgame.pay目录下，打开该目录的pay文件如下所示    这段代码专门用于处理通过支付宝进行支付的流程。  首先构造函数接收一个Cocos2dxActivity类型的参数（一种Android游戏引擎提供的Activity），并传递给基类构造函数。  然后定义如下5个私有方法  （1）a(String str, String str2, String str3)：  生成支付宝支付请求的参数字符串。  包括商户ID、账户ID、交易编号、商品名称、商品详情、金额、通知URL、服务类型、支付类型、字符集、超时时间和返回URL等。  （2）b(String str)：  通过给定的产品ID来获取完整的支付参数字符串。  遍历预定义的产品数组，匹配产品ID，并使用a()方法生成参数字符串。  （3）c(String str)：  对给定的字符串进行签名（使用SignUtils类的a()方法）。  （4）e()：  生成唯一的交易编号，格式为MMddHHmmss加上随机数，截取前15位。  （5）f()：  返回固定的签名类型字符串，即使用RSA加密。  然后覆盖的公有方法a(final String str)：  接收一个商品ID，生成支付参数和签名，然后通过支付宝SDK（PayTask类）发起支付。使用URLEncoder.encode方法对签名进行URL编码。在子线程中调用支付宝支付功能，处理支付结果。根据支付结果回调，使用a(str, boolean)方法通知支付成功或失败。  然后进行多线程处理  使用new Thread(new Runnable(){...}).start()在新线程中执行支付任务，避免阻塞UI线程。  支付任务完成后，根据返回的结果码（如9000表示支付成功）来处理支付结果。  最后进行错误处理  如果URL编码时出现UnsupportedEncodingException异常，则打印异常堆栈。  总结来说，这段代码的主要功能是封装了支付宝支付的流程，包括生成支付参数、签名处理、调用支付接口，并根据支付结果执行回调。这样的设计使得支付处理与业务逻辑分离，便于维护和扩展。   1. 结合不同逆向工具，分析程序核心算法逻辑   使用上一步中jadx工具获取到的java代码分析代码的核心片段如下    支付片段的核心代码逻辑如下  （1）这里首先初始化变量：  a aVar;：声明一个a类型的变量aVar，即当前类的实例。  String str3;：声明一个字符串变量str3，用于存储商品ID。  boolean z = true;：声明一个布尔变量z，初始值为true，用于表示支付是否成功。  （2）然后发起支付并获取结果：  new PayTask(a.this.d()).pay(str2, true)：通过PayTask类的实例发起支付宝支付，传入支付参数字符串str2和true表示使用异步方式支付。  new c(...).a()：使用c类（可能是用于签名的辅助类）对支付结果进行处理，返回一个表示支付结果的字符串。  （3）之后根据支付结果进行处理：  if (TextUtils.equals(a2, "9000")) { ... }：如果支付结果为"9000"，表示支付成功。  将当前实例赋值给aVar。  将商品ID赋值给str3。  else if (TextUtils.equals(a2, "8000")) { return; }：如果支付结果为"8000"，表示支付结果待确认，这里直接返回，不做处理。  else { ... }：如果支付结果不是"9000"或"8000"，表示支付失败。  将当前实例赋值给aVar。  将商品ID赋值给str3。  将支付状态标记z设置为false，表示支付失败。  （4）最后执行支付结果回调：  aVar.a(str3, z);：调用当前实例的a()方法，传入商品ID和支付状态，以便通知支付结果给调用者。   1. 利用程序逻辑逆向分析支付功能的具体实践 2. 实现具体功能的patch，得到购买成功的效果   首先检索“9000”字段    打开含有pay字段的部分    获取到该部分的源码如下    将跳转指令删除    保存之后编译    编译成功    之后打开游戏界面，这里因为是第二次截图所以游戏内金币并不是原始的20，点击皮肤选择购买    在弹出的支付界面选择一个选项    成功弹出充值成功界面      重启游戏后发现成功实现充值    **实验题目2：**  1、完成逆向题的seh.apk题目，实现购买成功的功能实现效果   1. 对Android解压，进行文件格式的基本分析 2. 静态分析程序 3. 结合不同逆向工具，分析程序核心算法逻辑 4. 利用程序逻辑逆向支付功能的具体实践 5. 实现具体功能的patch，得到购买成功的效果   实验要求：   1. 实验的关键步骤需要截图，并将相应代码粘贴至报告中。 2. 报告中的代码使用等宽字体，对齐使用四个空格，禁止使用tab或双空格。   **实验3 选做，根据学习情况自行选择解答**  **实验目的：**   * + 学会基本的Windows程序逆向分析方法，结合多种逆向框架进行基础的逆向分析，算法还原，得到re.exe的flag   + RE\_Cirno题目的分析   **实验题目：**  1、完成逆向题的RE\_Cirno题目，拿到flag字符串   1. binwalk分析提取程序 2. 静态分析程序 3. 结合不同逆向工具，分析程序核心算法逻辑 4. 利用程序逻辑逆向写出求解算法程序 5. 利用逆向求解算法拿到flag   jpg  binwalk  binwalk -e  exe打开  放到die中打开看架构  用ida打开  main函数  空格 F5没有异或操作  ghidra打开，程序codebrowser  search for string ->all blocks  找到异或操作  按g跳到0x00040f43e异或操作  选中异或操作右侧代码可以识别出来  最后将得到的代码逆向 | | | | | |
| 1. 实验步骤   （每道题具体的实验步骤，关键步骤需截图） | | | | | |
|  | | | | | |
| 1. 实验过程分析   （记录实验过程中遇到问题，进行问题分析，说明问题解决过程及方法。） | | | | | |
|  | | | | | |
| 1. 实验结果总结   （实验的完成情况，所遇到的难点，对实验的修改建议） | | | | | |
|  | | | | | |
| 1. 各人实验贡献与体会（每人各自撰写，每人在实验中所做的贡献度与体会） | | | | | |
| 同学：XXX  ……  同学：XXX  …… | | | | | |
| 1. 教师评语 | | | | | |
|  | | | | | |
| **教师评分（请填写好姓名、学号）** | | | | | |
| 姓名 | | 学号 | 分数 | | |
|  | |  |  | | |
|  | |  |  | | |
|  | |  |  | | |
|  | |  |  | | |
|  | |  |  | | |
|  | |  |  | | |
| 教师签名：  年 月 日 | | | | | |