数字货币钱包安全审计报告

Loopr 钱包（Android）

SECBIT

2018 年 12 月 15 日

1. 综述

Loopr 钱包（Android）是一款数字货币钱包应用。安比（SECBIT）实验室于 2018 年 11 月 16 日至 2018 年 11 月 26 日对 Loopr 钱包（Android）进行审计。审计过程从**数字钱包资产安全**，**应用常规风险**和**服务端应用安全风险**三个维度对钱包进行分析。审计结果表明，Loopr 钱包（Android）并未发现致命的安全漏洞，安比（SECBIT）实验室给出了如下几点功能实现安全隐患，发行风险提示以及优化建议项（详见第 4 章节）。

风险类型	描述	风险级别
钱包资产安全	明文保存助记词	中
应用常规风险	AndroidMainfest.xml 配置有安全风险	中
钱包资产安全	在日志中打印助记词等敏感信息	中
服务端通信风险	H5DexWebActivity 使用 http 协议通信	低
应用常规风险	敏感信息输入和显示界面没有防止信息泄露的保护措施	低
应用常规风险	没有弱口令密码检测和错误输入次数检测	低
应用常规风险	存储文件没有对文件内容进行加密	低
应用常规风险	打包 APK 没有对代码进行混淆和加固	低
应用常规风险	APK 未进行完整性校验	低
钱包资产安全	通过无密码的助记词导入的钱包没有任何密码保护	低
钱包资产安全	Android 创建钱包时生成私钥的过程和 iOS 不一致	低
钱包资产安全	没有及时抹除保存私钥变量的内容	提示
风险提示	Android 和 iOS 的 Loopr 钱包未提示用户丢失密码后，无法从助记词中恢复用户私钥	提示

2. 钱包信息

该部分描述了 Loopr 钱包（Android）的基本信息。

应用名称	Loopr 钱包（Android）
应用类型	Android
是否上架	否
文件来源	Github
文件类型	源码、官网 APK 文件
代码路径	https://github.com/Loopring/loopr-android
commit id	145bdb011e0f6037abd0828ae3a13e700c8b8dbc
支持币种	ETH、ERC20 Token

3. 钱包分析

该部分针对钱包审计范围的主要功能和主要特性进行了详细分析，从实现的相关功能和安全两部分来进行说明。

3.1 相关功能

Loopr 钱包（Android）作为一款加密数字货币钱包，针对数字货币部分的主要功能分为四个部分：创建钱包，钱包导入，密钥管理和转账收款。

- 创建钱包
    - 创建一个或者多个钱包
    - 用户创建钱包可以跳过校验助记词
- 导入钱包
    - 用户可以根据助记词、Keystore、私钥导入钱包
- 密钥管理
    - 修改钱包名称
    - 导出 Keystore 文件
- 转账收款
    - 支持对 ETH、ERC20 Token 进行收款和转账

3.2 安全分析

- 随机数的生成
  - 使用了 SecureRandom 的安全随机源
- 助记词的生成
  - 代码实现遵循了 BIP39 规范，暂未发现安全问题
- 密钥派生
  - 使用 BitcoinJ 的开源库实现的密钥派生，目前该库未暴露出安全问题。并且按照 BIP44 标准派生密钥，coin type 正确。
- 密钥存储
  - 使用 Web3J 开源库生成 Keystore 文件进行保存，该文件根据用户密码将私钥进行加密后存储，不直接泄露用户私钥。
  - 存在助记词明文保存的情况，有一定的安全隐患。
- 密钥管理
  - 仅提供 Keystore 格式的密钥导出，且需要输入密码才能导出，导出过程安全
- 敏感信息输入
  - 未使用自绘安全键盘
  - 使用了弱密码
- 服务器通信安全
  - 未发现上传私钥信息
  - 使用了不安全的 http 协议
- Android 常规安全
  - AndroidMainfest.xml 配置存在安全风险
- 防截屏
  - 没有防截屏措施（部分已修复）

4. 审计详情

该部分描述钱包审计流程和详细结果，并对发现的问题（数字钱包资产安全，应用常规风险和服务端应用安全风险），数字货币钱包发行的风险点进行详细的说明。

4.1 审计过程

本次审计工作，严格按照安比（SECBIT）实验室审计流程规范执行，从钱包资产安全、应用常规安全、服务器风险三个维度进行全面分析。审计流程大致分为四个步骤：

- 各审计小组根据审计内容对钱包应用进行审计
- 各审计小组对钱包应用的漏洞和风险进行评估
- 审计小组之间交换审计结果，并对审计结果进行逐一审查和确认
- 审计小组配合审计负责人生成审计报告

4.2 审计结果

本次审计首先经过安比（SECBIT）实验室内部工具和外部开源工具的检查，检查结果由审计小组成员详细确认。审计小组成员对钱包应用源码进行检查，汇总审计结果。审计内容总结为如下。

编号	分类	结果
1	助记词的创建和存储过程风险检测	通过
2	私钥的创建和存储过程风险检测	通过
3	本地敏感信息的保存风险检测	通过
4	钱包导入过程风险检测	通过
5	钱包口令风险检测	通过
6	数字货币交易风险检测	通过

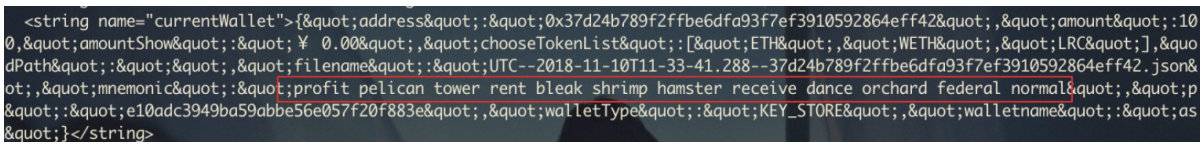
7	密码算法，随机数算法风险检测	通过
8	业务逻辑流程风险检测	通过
9	用户权限划分风险检测	通过
10	数字货币钱包 App 运行环境风险检测	通过
11	数字货币钱包 App 开发合规性风险检测	通过
12	数字货币钱包 App 组件风险检测	通过
13	数字货币钱包 App 本地存储及缓存文件风险检测	通过
14	钱包应用与服务器端通信风险检测	通过

4.3 问题列表

问题是明显存在的安全隐患，安比（SECBIT）实验室在对 Loopr 钱包（Android）应用风险进行评估以后，指出钱包存在如下问题点，并根据问题提出一些规避方案，具体描述如下：

1. 明文保存助记词

- 风险级别：**中**
- 问题类型：
  - 助记词的创建和存储过程风险检测
- 问题描述：



  用户生成私钥的助记词明文保存在 `shared_pref/share_data.xml`。

  同时，`leaf.prod.app/files/keystore/mnemonic.txt` 里面存放了最近一次的助记词缓存。

  使得用户的私钥在设备丢失的情况下，有较大的安全风险。

- 影响结果：

  使用户私钥在特定情况下，容易泄漏

- 规避方案：
    - 不保存助记词或者加密保存
    - 不缓存助记词

  对于加密保存助记词，可以参考 Keystore 文件生成过程，使用用户密码对助记词进行加密，具体过程描述如下：

    - 使用 `PBKDF2-SHA-256` 算法 或者 `Scrypt` 算法，对用户密码进行派生，得到派生密钥
    - 以派生密钥作为 Key，使用 AES 算法加密助记词，得到密文
    - 保存密文和 AES 运算过程中生成的 iv 变量

  同时可以参照 `7. 存储文件没有对文件内容进行加密` 中提到的规避方案，对整个 SharedPreference 文件内容进行加密。
- 修改结果：
    - 不再使用 `mnemonic.txt` 保存助记词，同时删除了该文件
    - 对助记词进行了加密存储

2. AndroidMainfest.xml 配置有安全风险

- 风险级别：**中**
- 问题类型：
    - 数字货币钱包 App 运行环境风险检测
- 问题描述：
    - `android:allowBackup=true` 允许用户导出所有 App 数据
    - `android:exported=true` 大部分 Activity 都是暴露出来的
- 影响结果：

  使 App 更容易被分析和调试
- 规避方案：
    - 不允许用户导出所有 App 数据，即配置 `android:allowBackup=false`
    - 将不需要暴露的 Activity 设置为 `android:exported=false`
- 修改结果：
    - 已经将不需要暴露的 Activity 设置为 `android:exported=false`

3. 在日志中打印助记词等敏感信息

- 风险级别：**中**
- 问题类型：
    - 数字货币钱包 App 开发合规性风险检测

- 问题描述：
  - 使用 `LyqbLogger.log()`在多处打印助记词、用户密码等敏感信息。例如：`GenerateWalletActivity.java` 中 378 行打印了用户助记词。
- 影响结果：
  - 导致用户私钥泄露。
- 规避方案：
  - 检查并删除所有使用 `LyqbLogger.log()` 打印用户敏感信息的代码。

4. H5DexWebActivity 使用 http 协议通信

- 风险级别：**低**
- 问题类型：
  - 钱包应用与服务器端通信风险检测
- 问题描述：

```
e R.id.dapp_layout:
 getOperation().addParameter("url", "http://embeddex.upwallet.io/#/auth/tpwallet");
 getOperation().forward(H5DexWebActivity.class);
 break;
e R.id.p2p_layout:
 getOperation().addParameter("url", "http://embeddex.upwallet.io/#/face2face");
```

  使用 http 协议通信容易被中间人攻击。
- 影响结果：

  攻击者可以伪造 H5 页面，可能造成用户的财产损失或者信息泄露。
- 规避方案：
  - 使用 https 进行通信
- 修改结果：
  - 关键数据信息的通信使用了安全的 https

5. 敏感信息输入和显示界面没有防止信息泄露的保护措施

- 风险级别：**低**
- 问题类型：
  - 钱包口令风险检测
  - 助记词的创建和存储过程风险检测
- 问题描述：

  用户在输入密码、助记词等敏感信息界面上没有防止截屏、录屏以及安全自绘键盘的保护措施
- 影响结果：

导致用户隐私信息被泄露

- 规避方案：
  - 做防截屏、录屏的保护。主要有以下几个部分需要做防截屏处理：
    - 钱包创建时的助记词显示和用户密码的输入界面
    - 导出钱包的私钥和助记词显示界面
    - 通过助记词或者私钥导入钱包的界面和用户密码的输入界面
    - 交易过程中用户密码的输入界面，尤其是弹框界面
  - 使用自绘输入键盘代替系统键盘
- 修改结果：
  - 在创建钱包、导出钱包时，进行了防截屏、录屏处理。

6. 没有弱口令密码检测和错误输入次数检测

- 风险级别：**低**
- 问题类型：
  - 钱包口令风险检测
- 问题描述：

  输入密码没有对弱密码进行检测，也没有对错误输入进行限制。
- 影响结果：

  用户密码更容易被暴力破解，造成用户资产的损失。
- 规避方案：
  - 提示用户输入强度高的密码
  - 对错误输入次数进行限制
- 修改结果：
  - 对弱密码进行了提示

7. 存储文件时没有对文件内容进行加密

- 风险级别：**低**
- 问题类型：
  - 本地敏感信息的保存风险检测
  - 数字货币钱包 App 本地存储及缓存文件风险检测
- 问题描述：

  Android 设备中用户存储在本地的文件更加容易被窃取。没有对文件内容加密，使黑客更加容易获取用户的敏感信息。
- 影响结果：

可能会造成用户隐私的泄漏或者数字资产的损失。

- 规避方案：

  对于存储的 SharedPreference 和 本地文件（例如：Keystore ）的内容进行加密，具体方案描述如下：

  - 对于SharedPreference，可以参考使用 secure-preferences https://github.com/scottyab/secure-preferences 的方案。对 SharedPreference 的 Key 和 Value 进行加密存储。
  - 对于本地文件，建议基于 C++ 编写 Native code 实现的 AES 加密算法对存储的内容进行加密：
    - 使用 Native 代码编写生成的 so 文件相对于 Java 更难以被逆向，同时更容易做加固。
    - Native 代码中使用 AES 算法加解密文件时，不要直接使用硬编码的密钥，应该使用函数动态生成密钥的方式来增加逆向成本。
    - So 文件中的加解密函数被调用时，动态获取 Android 运行时上下文环境，判断是否在安全的上下文中运行（例如：调用当前加密函数的App包名是否为指定包名），提高被动态调试破解的成本。
  - 为了提高 Keystore 文件存储的安全性，建议在用户设置钱包密码的时候，要求用户输入强度高的密码。这样可以增加 Keystore 文件被窃取之后暴力破解出私钥的难度。

8. 打包 APK 没有对代码进行混淆和加固

- 风险级别：**低**
- 问题类型：
  - 数字货币钱包 App 运行环境风险检测
- 问题描述：

  没有对 APK 进行加固，很容易逆向破解。同时打包时没有做代码混淆，使得逆向反编译的代码很容易阅读。

- 影响结果：

  使攻击者更加容易分析 App 的行为和发现潜在的漏洞，造成开发者或者用户的损失。

- 规避方案：
  - 在打包 APK 时编写 `proguard-rules.pro`对代码进行混淆，尤其是涉及到助记词、私钥部分的代码
  - 上线 APK 前使用付费或者免费的加固服务对 APK 文件进行加固

9. APK 未进行完整性校验

- 风险级别：**低**
- 问题类型：
  - 数字货币钱包 App 运行环境风险检测
- 问题描述：

  APK 没有进行签名完整性校验，重新签名后仍可以安装。

  APK 没有对文件进行完整性检查。反编译后修改文件后重新签名，程序仍可运行。
- 影响结果：

  攻击者可以通过篡改客户端后重新打包篡改客户端行为。
- 规避方案：
  - 运行时对 APK 进行签名完整性校验
  - 可以通过常规完整性校验算法（CRC、MD5）对 classes.dex 以及整个 APK 文件进行校验。

10. 通过无密码的助记词导入的钱包没有任何密码保护

- 风险级别：**中**
- 问题类型：
  - 钱包口令风险检测
  - 钱包导入过程风险检测
- 问题描述：

  用户通过助记词导入钱包时，导入未使用密码的助记词（例如：导入 imToken App 生成钱包的助记词），导入后钱包没有任何密码保护，他人可以随意发起转账。而且保存用户私钥的 Keystore 文件加密的密码为空，使用户私钥更容易被盗取。
- 影响结果：

  造成用户资产损失。
- 规避方案：

  在导入时，对于导入未使用密码的助记词，提供额外的密码保护。
- 修改结果：
  - 修改为导入助记词的时候，必须要输入助记词密码作为钱包的密码。

11. Android 创建钱包时生成私钥的过程和 iOS 不一致

- 风险级别：**提示**
- 问题类型：
  - 助记词的创建和存储过程风险检测

    - 私钥的创建和存储过程风险检测
- 问题描述： iOS 实现的 BIP39 使用了用户输入的密码作为助记词密码，而 Android 未使用助记词密码。导致两者在创建钱包时，即使生成的助记词相同，派生出的私钥 Seed 也不相同。
- 影响结果：

  两个平台上创建生成的钱包，互相导入时过程不一致。
- 规避方案：

  经沟通，iOS 和 Android 统一使用用户输入密码作为助记词密码生成用户私钥。Android 需要进行修改，创建钱包时私钥 Seed 的生成过程中使用用户输入的密码作为助记词密码。
- 修改结果：
    - 修改为 Android 钱包使用助记词密码作为钱包密码。经测试，相同助记词和用户密码生成钱包地址一致。

12. 没有及时抹除保存私钥变量的内容

- 风险级别：**提示**
- 问题类型：
    - 私钥的创建和存储过程风险检测
- 问题描述： 使用 String、Credential 中的 BigInteger 等对象类型保存用户私钥。对象类型的变量在堆上分配，依赖于 GC 进行垃圾回收，在非常极端的情况下，可以通过 Dump Heap 获得用户私钥。
- 影响结果：

  用户私钥泄漏，造成用户资产的损失。
- 规避方案：

  使用 `[]bytes` 保存用户私钥，并且在使用后及时抹除变量的内容。参考代码如下：

```
bytes[] privKey = genPrivateKey();
for (i:=0;i < privKey.length; i++){
    privKey[i] = 0;
}
```

4.4 风险提示

风险点是在用户使用过程中，或者是在产品设计逻辑下可能存在的安全风险。安比（SECBIT）实验室在对 Loopr 钱包（Android）应用风险进行评估以后，指出钱包存在如下风险项：

Android 和 iOS 的 Loopr 钱包未提示用户丢失密码后，无法从助记词中恢复用户私钥

- 风险级别：**提示**
- 问题类型：风险提示
- 风险描述：

  Android 和 iOS 的 Loopr 钱包使用了助记词密码。如果用户忘记密码，仅通过助记词也无法恢复出私钥。而且常规钱包应用都仅提示用户保管好助记词，并且支持从助记词中恢复私钥，容易对使用 Loopr 钱包用户带来认知偏差，造成用户不必要的资产损失。

- 规避方案：

  在创建钱包过程中，通过弹框告知用户，该钱包使用用户输入的密码作为助记词密码生成钱包账户，并强调用户需要保管好自己输入的密码，否则密码丢失后无法通过助记词或者 Keystore 文件恢复出自己的钱包账户，并待用户点击确认该信息后才可以使用钱包。

5. 结论

Loopr 钱包（Android）钱包根据标准协议规范 BIP32、BIP39、BIP44 实现了数字货币钱包的基本功能（创建账户、密钥管理、转账收款等）并在此基础上进行了其他功能的扩展。安比（SECBIT）实验室在对 Loopr 钱包（Android）进行分析后，发现并未致命的缺陷和漏洞。在钱包资产安全、手机端和服务器端上存在的问题和风险，上文均已给出具体的分析说明。

免责声明

SECBIT 数字货币钱包安全审计从账户安全、资产安全和钱包发行风险等方面对钱包应用的正确性、安全性、可执行性进行审计，但不做任何和代码的适用性、商业模式和管理制度的适用性及其他与数字货币钱包适用性相关的承诺。本报告为技术信息文件，不作为投资指导。

附录

漏洞风险级别介绍

等级	描述
高	可以严重损害用户数字资产安全的缺陷，能够允许攻击者盗取用户数字资产，或者无法使用数字资产等缺陷。
中	在一定限制条件下能够损害数字资产安全的缺陷，造成某些参与方利益损失的缺陷。
低	并未对数字资产安全造成实质损害的缺陷。
提示	不会带来直接的风险，但与数字资产安全实践或数字货币钱包合理性建议有关的信息。

安比（SECBIT）实验室致力于参与共建共识、可信、有序的区块链经济体。

https://secbit.io
audit@secbit.io
@secbit_io