逆向微信小红书小程序并获得x-sign算法

免责声明

以下内容仅用于逆向学习和技术验证，如果侵犯了利益，请联系我删除v:feilang235。

硬件准备

一台 root 好的手机

Mac or win 电脑

提取小程序包

清除历史缓存的小程序包

微信的小程序是在第一次打开的时候就会进行下载一个 wxapkg 的包并且缓存到手机里面。以后再使用的时候就不用下载了，只需要检测有没有更新就行了。我们这边先删除历史中存在的所有缓存文件。

使用 adb 链接手机进入目录：/data/data/com.tencent.mm/MicroMsg/{user}/appbrand/pkg

{user} 是自己的 UserID。

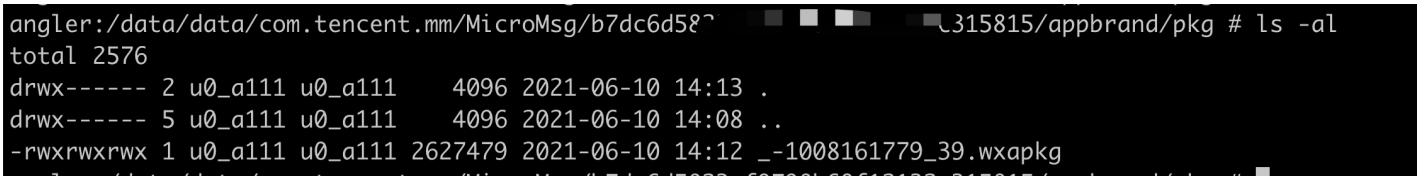
在这个目录下删除所有的后缀为 wxapkg 的包。

微信中打开小程序

清理所有缓存小程序包之后，重新打开微信，然后搜索小红书APP找到小程序。点击后打开小红书小程序。你会发现这个时候第一次特别慢，因为微信需要重新去下载小红书小程序的包。相当于就是下载app 并安装，但是小程序没有app那么大，而且安装更快。

等重新打开小程序后，随便点击几下，确认运行正常。

这个时候在 /data/data/com.tencent.mm/MicroMsg/{user}/appbrand/pkg 查看是否有一个新文件。



如上截图，多了一个 _-1008161779_39.wxapkg 这个包就是小红书的微信小程序内容了。

提取微信小程序包到电脑

使用 adb pull进行复制。

这里有个坑。直接从 /data/data/com.tencent.mm/MicroMsg/{user}/appbrand/pkg/_-1008161779_39.wxapkg 这里复制可能会没有权限。

可以先把 _-1008161779_39.wxapkg 复制到 /data/local/tmp 路径下。并且

chmod 777 _-1008161779_39.wxapkg 给予最高权限。

然后在 adb pull /data/local/tmp/_-1008161779_39.wxapkg ~/projects/

进行复制。这样就可以将小红书的包下载到 mac 的~/projects/ 文件夹下面了。

反编译小程序包

上面虽然下载到了小程序的包，不过后缀是 wxapkg 这个还是微信生态圈的内容。需要对这个包进行反编译获得 js 文件。并且可以对其进行调试。

这里推荐一个神器。上 github 地址。

https://github.com/xuedingmiaojun/wxappUnpacker

我们也会用到 wxappUnpacker 进行反编译。github 上面已经有详细的使用教程了。而且还提供了一个

wxappUnpacker 配置

wxappUnpacker 配置依赖了 nodejs 和 npm 不懂的请自行 google。

Shell

```
git clone https://github.com/xuedingmiaojun/wxappUnpacker.git
cd wxappUnpacker

npm install # 安装依赖

# 安装其他需要的包
npm install esprima
npm install css-tree
npm install cssbeautify
npm install vm2
npm install uglify-es
npm install js-beautify
```

wxappUnpacker 工具说明

Shell

```
node wuConfig.js <files...>

# 将 app-config.json 中的内容拆分到各个文件对应的 .json 和 app.json , 并通过搜索 app-config.json 所在文件夹下的所有文件尝试将 iconData 还原为 iconPath 。

node wuJs.js <files...>

# 将 app-service.js (或小游戏中的 game.js ) 拆分成一系列原先独立的 javascript 文件，并使用 Uglify-ES 美化，从而尽可能还原编译前的情况。

node wuWxml.js [-m] <files...>

# 将编译/混合到 page-frame.html ( 或 app-wxss.js ) 中的 wxml 和 wxs 文件还原为独立的、未编译的文件。如果加上-m指令，就会阻止block块自动省略，可能帮助解决一些相关过程的 bug 。**

node wuWxss.js <dirs...>

# 通过获取文件夹下的 page-frame.html ( 或 app-wxss.js ) 和其他 html 文件的内容，还原出编译前 wxss 文件的内容。

node wuWxapkg.js [-o] [-d] [-s=] <files...>

# 将 wxapkg 文件解包，并将包中上述命令中所提的被编译/混合的文件自动地恢复原状。如果加上-o指令，表示仅解包，不做后续操作。如果加上-d指令，就会保留编译/混合后所生成的新文件，否则会自动删去这些文件。同时，前面命令中的指令也可直接加在这一命令上。而如果需要解压分包，请先解压主包，然后执行node wuWxapkg.js [-d] -s=<subPackages...>，其中Main Dir为主包解压地址。除-d与-s外，这些指令两两共存的后果是未定义的（当然，是不会有危险的）
```

wxappUnpacker 反编译小红书小程序

终于到了最激动人心的步骤了。

Apache

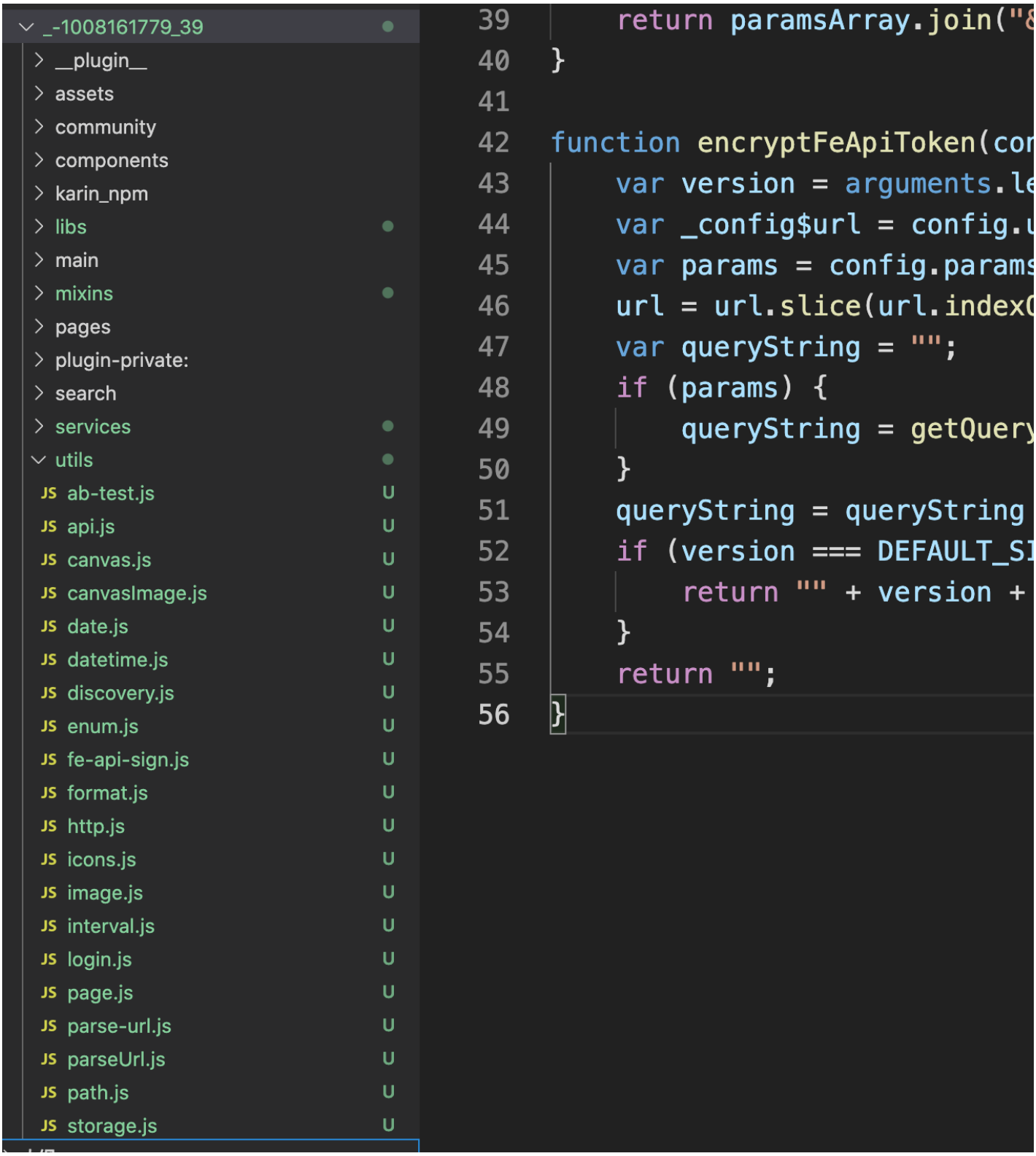
```
node wuWxapkg.js _-1008161779_39.wxapkg
```

```
➜  wxappUnpacker git:(master) ✗ node wuWxapkg.js _-1008161779_39.wxapkg
Unpack file _-1008161779_39.wxapkg...

Header info:
  firstMark: 0xbe
  unknownInfo:  0
  infoListLength:  6843
  dataLength:  2620622
  lastMark: 0xed

File list info:
  fileCount:  131
Saving files...
Unpack done.
Split app-service.js and make up configs & wxss & wxml & wxs...
deal config ok
deal js ok
deal wxss.js ok
deal css ok
============================================================
这个小程序采用了分包
子包个数为:  5
```

```
Save wxss...
saveDir: /Users/lgq/projects/study/wxappUnpacker/_-1008161779_39
Split and make up done.
Delete files...
Deleted.

File done.
Total use: 5.142s
```

出现上面的内容就表示反编译成功了。现在已经获得了小红书小程序客户端的全部内容了。

使用 vscode 打开看看。



逆向小红书小程序x-sign 算法

通过抓包可以知道小红书小程序使用的是 x-sign 字段进行验证。

既然我们这里已经获得了完整的客户端代码了。要找到 x-sign 签名算法，那还不件非常简单的事情。直接搜索 x-sign 差不多就定位了。

这里将签名算法接个图。

```
function encryptFeApiToken(config) {
    var version = arguments.length > 1 && arguments[1] !== undefined ? arguments[1] : DEFAULT_SIGN_VERSION;
    var _config$url = config.url, url = _config$url === undefined ? "" : _config$url;
    var params = config.params, _config$transform = config.transform, transform = _config$transform === undefined ? false :
    url = url.slice(url.indexOf(DEFAULT_SIGN_API_PATH), url.length);
    var queryString = "";
    if (params) {
        queryString = getQueryByParams(params, transform);
    }
    queryString = queryString ? "?" + queryString : "";
    if (version === DEFAULT_SIGN_VERSION) {
        return "" + version + (0, _md2.default)(url + queryString + SECRET_KEY);
    }
    return "";
}
```

简单的说就是

md5(DEFAULT_SIGN_VERSION + url + queryString + SECRET_KEY)

详细代码就不编写了。如果需要可以私聊v：feilang235 .

以上就是最详细的逆向小红书小程序并且获得 x-sign 算法的全流程了。

参考内容

https://www.ddosi.com/weixin-pkg/

https://github.com/xuedingmiaojun/wxappUnpacker