【原创干货】微信小游戏海盗来了源码分析(JAVA 辅助)

作者：relyn

原文链接：https://ld246.com/article/1525115554985

来源网站：链滴

最近很流行的一款微信小游戏《海盗来了》，用来打发时间还不错，就是建岛和转盘太慢了，于是用Fiddler抓了下包，分析了下请求报文，发现所有的请求都需要sign签名，尝试了几次都得不到签名值于是搞了个安卓模拟器，把小游戏的源码拷出来分析了下。

《海盗来了》小游戏的game.js源码

《海盗来了》game.js 格式化后

《海盗来了》未格式化的wxapkg源码

分析源码发现，请求的签名算法就是普通的字典排序，拼成URL后把&符号去掉，再进行MD5签名！

例如：sign=md5(uid=666t=666secret=666)

试了下，还是可以用的，但请求的频率不宜过高，我的一个号就是这样被封了，所以。。。

运行结果：

param >> bet=1&isWxGame=true&secret=2ca123ee4a764293af00b139781c291e&t=15252
8492778&uid=199471083

sign >> 9d1506d57913290ac439dc134990bde4

转盘 >> {"data":{"money":1337034,"maxEnergy":50,"energy":0,"recoverEnergy":6,"timeToReco
er":3135,"shields":2,"wantedCount":0,"ShipwreckCount":0,"cookieCount":0,"potionCount":0,"h
tchCount":0,"hornCount":0,"miniShieldCount":0,"monthCardExpired":0,"gotNewbieGift":false,
gotOccasionalGift":true,"gotDailyShop":true,"allInOnePiece":0,"killTitanCannonBall":30,"summ
nStone":1,"puffer":0,"lolly":0,"guildMedal":0,"doubleMoneyCard":0,"stealIslands":null,"attackTa
get":null,"revengeList":null,"rollerItem":{"index":1,"type":0,"value":48000},"betCount":1,"share
oinFactor":0},"errcode":0,"errmsg":""}

length >> 586

Talk is cheap, show you the code :

解释一下，这里用到了一个RelynSpider类，是我自己的爬虫类，其实就是POST请求，用HttpClient可以实现，POST的时候，记得用微信的User-Agent，相关的方法我都贴在最后面了。

```
package com.relyn;

import java.util.HashMap;
import java.util.Map;

public class RelynPirate {

private static RelynSpider relynSpider = new RelynSpider();

public static void start(String userId, String island) {
    String url = "https://pirate-api.hortor002.com/game/entry/wxgame";
    Map<String, Object> map = new HashMap<String, Object>();
    Map<String, String> dataMap = new HashMap<String, String>();
    String t = String.valueOf(System.currentTimeMillis());
    String resp = "";
    String sign = "";
    String param = "";
```

```
String uid = "";

String secret = java.util.UUID.randomUUID().toString().replace("-", "");
System.out.println("secret >> " + secret);

// 基础登录
url = "https://pirate-api.hortor002.com/game/basic/login";
dataMap = new HashMap<String, String>();
dataMap.put("userId", userId);
dataMap.put("isWxGame", "true");
dataMap.put("t", t);
dataMap.put("secret", secret);
param = RelynSpider.formatUrlMap(dataMap, false, false);
System.out.println("param >> " + param);
param = param.replaceAll("&", ""); // 把&去掉
sign = RelynSpider.md5(param);
System.out.println("sign >> " + sign);
map = new HashMap<String, Object>();
map.put("userId", userId);
map.put("isWxGame", "true");
map.put("t", t);
map.put("secret", secret);
map.put("sign", sign);
resp = relynSpider.postWechat(url, map);
System.out.println("基础登录 >> " + resp);
resp = resp.substring(resp.indexOf("uid\":") + 5);
uid = resp.substring(0, resp.indexOf(","));
System.out.println("UID >> " + uid);

// 领取并赠送能量
url = "https://pirate-api.hortor002.com/game/friend/donate";
t = String.valueOf(System.currentTimeMillis());
dataMap = new HashMap<String, String>();
dataMap.put("uid", uid);
dataMap.put("fid", "0");
dataMap.put("isWxGame", "true");
dataMap.put("t", t);
dataMap.put("secret", secret);
param = RelynSpider.formatUrlMap(dataMap, false, false);
System.out.println("param >> " + param);
param = param.replaceAll("&", ""); // 把&去掉
sign = RelynSpider.md5(param);
System.out.println("sign >> " + sign);
map = new HashMap<String, Object>();
map.put("uid", uid);
map.put("fid", "0");
map.put("isWxGame", "true");
map.put("t", t);
map.put("secret", secret);
map.put("sign", sign);
resp = relynSpider.postWechat(url, map);
System.out.println("领取并赠送能量 >> " + resp);

// 金矿
```

```
url = "https://pirate-api.hortor002.com/game/island/collect";
t = String.valueOf(System.currentTimeMillis());
dataMap = new HashMap<String, String>();
dataMap.put("uid", uid);
dataMap.put("isWxGame", "true");
dataMap.put("t", t);
dataMap.put("secret", secret);
param = RelynSpider.formatUrlMap(dataMap, false, false);
System.out.println("param >> " + param);
param = param.replaceAll("&", ""); // 把&去掉
sign = RelynSpider.md5(param);
System.out.println("sign >> " + sign);
map = new HashMap<String, Object>();
map.put("uid", uid);
map.put("isWxGame", "true");
map.put("t", t);
map.put("secret", secret);
map.put("sign", sign);
resp = relynSpider.postWechat(url, map);
System.out.println("金矿 >> " + resp);

// 转盘
int length = 100;
while (length > 34) {
    t = String.valueOf(System.currentTimeMillis());
    url = "https://pirate-api.hortor002.com/game/roller/roll";
    dataMap = new HashMap<String, String>();
    dataMap.put("uid", uid);
    dataMap.put("bet", "1");
    dataMap.put("isWxGame", "true");
    dataMap.put("t", t);
    dataMap.put("secret", secret);
    param = RelynSpider.formatUrlMap(dataMap, false, false);
    System.out.println("param >> " + param);
    param = param.replaceAll("&", ""); // 把&去掉
    sign = RelynSpider.md5(param);
    System.out.println("sign >> " + sign);
    map = new HashMap<String, Object>();
    map.put("uid", uid);
    map.put("bet", "1");
    map.put("isWxGame", "true");
    map.put("t", t);
    map.put("secret", secret);
    map.put("sign", sign);
    resp = relynSpider.postWechat(url, map);
    System.out.println("转盘 >> " + resp);
    length = resp.length();
    System.out.println("length >> " + length);
    if (length > 600) {
        if (resp.indexOf("stealIslands\":null") != -1) {
            resp = resp.substring(resp.indexOf("uid\":") + 5);
            String puid = resp.substring(0, resp.indexOf(","));
            // 攻击
            t = String.valueOf(System.currentTimeMillis());
```

```
            System.out.println("[*] 攻击");
            url = "https://pirate-api.hortor002.com/game/pvp/attack";
            dataMap = new HashMap<String, String>();
            dataMap.put("uid", uid);
            dataMap.put("puid", puid);
            dataMap.put("building", "3");
            dataMap.put("isWxGame", "true");
            dataMap.put("t", t);
            dataMap.put("secret", secret);
            param = RelynSpider.formatUrlMap(dataMap, false, false);
            System.out.println("param >> " + param);
            param = param.replaceAll("&", ""); // 把&去掉
            sign = RelynSpider.md5(param);
            System.out.println("sign >> " + sign);
            map = new HashMap<String, Object>();
            map.put("uid", uid);
            map.put("puid", puid);
            map.put("building", "3");
            map.put("isWxGame", "true");
            map.put("t", t);
            map.put("secret", secret);
            map.put("sign", sign);
            resp = relynSpider.postWechat(url, map);
            System.out.println("攻击 >> " + resp);
        } else {
            // 盗窃
            t = String.valueOf(System.currentTimeMillis());
            System.out.println("[*] 盗窃");
            url = "https://pirate-api.hortor002.com/game/pvp/steal";
            dataMap = new HashMap<String, String>();
            dataMap.put("uid", uid);
            dataMap.put("idx", "1");
            dataMap.put("isWxGame", "true");
            dataMap.put("t", t);
            dataMap.put("secret", secret);
            param = RelynSpider.formatUrlMap(dataMap, false, false);
            System.out.println("param >> " + param);
            param = param.replaceAll("&", ""); // 把&去掉
            sign = RelynSpider.md5(param);
            System.out.println("sign >> " + sign);
            map = new HashMap<String, Object>();
            map.put("uid", uid);
            map.put("idx", "1");
            map.put("isWxGame", "true");
            map.put("t", t);
            map.put("secret", secret);
            map.put("sign", sign);
            resp = relynSpider.postWechat(url, map);
            System.out.println("盗窃 >> " + resp);
        }

    }
}
```

```
    // 许愿瓶
    // url = "https://pirate-api.hortor002.com/game/annual/open-lucky-box";
    // dataMap = new HashMap<String, String>();
    // dataMap.put("uid", uid);
    // dataMap.put("useFree", "false");
    // dataMap.put("isWxGame", "true");
    // dataMap.put("t", t);
    // dataMap.put("secret", secret);
    // param = formatUrlMap(dataMap, false, false);
    // System.out.println("param >> " + param);
    // param = param.replaceAll("&", ""); //把&去掉
    // sign = md5(param);
    // System.out.println("sign >> " + sign);
    // map = new HashMap<String, Object>();
    // map.put("uid", uid);
    // map.put("useFree", "false");
    // map.put("isWxGame", "true");
    // map.put("t", t);
    // map.put("secret", secret);
    // map.put("sign", sign);
    // resp = relynSpider.postWechat(url, map);
    // System.out.println("HTML >> " + resp);

    // 建造
    for (int building = 0; building < 5; building++) {
        for (int level = 1; level < 6; level++) {
            t = String.valueOf(System.currentTimeMillis());
            url = "https://pirate-api.hortor002.com/game/island/build";
            dataMap = new HashMap<String, String>();
            dataMap.put("uid", uid);
            dataMap.put("island", island);
            dataMap.put("building", String.valueOf(building));
            dataMap.put("level", String.valueOf(level));
            dataMap.put("t", t);
            dataMap.put("secret", secret);
            param = RelynSpider.formatUrlMap(dataMap, false, false);
            System.out.println("param >> " + param);
            param = param.replaceAll("&", ""); // 把&去掉
            sign = RelynSpider.md5(param);
            System.out.println("sign >> " + sign);
            map = new HashMap<String, Object>();
            map.put("uid", uid);
            map.put("island", island);
            map.put("building", building);
            map.put("level", level);
            map.put("t", t);
            map.put("secret", secret);
            map.put("sign", sign);
            resp = relynSpider.postWechat(url, map);
            System.out.println("建造 >> " + resp);
        }
    }
}
```

```
public static void main(String[] args) {
    // TODO Auto-generated method stub
    userId = "";
    island = ""; // 当前建造第几座岛屿，第一座是0，依次类推
    start(userId, island);

}

}
```

RelynSpider类中的postWechat方法：

```
/**

 * 微信POST请求
 * @param url
 * @return
 */
public String postWechat(String url, Map<String, Object> map) {
    String respString = "";
    try {
        HCB hcb = HCB.custom()
                // .proxy(proxyArray[0], proxyPort) //代理
                .timeout(30000) // 超时
                .pool(100, 10) // 启用连接池，每个路由最大创建10个链接，总连接数限制为100个
                .sslpv(SSLProtocolVersion.SSLv3) // 设置ssl版本号，默认SSLv3，也可以调用sslpv("TLS
1.2")
                .ssl() // https，支持自定义ssl证书路径和密码，ssl(String keyStorePath,
                       // String keyStorepass)
                .retry(5); // 重试5次
        HttpConfig config = HttpConfig.custom()
                  //.headers(headers)    //设置headers，不需要时则无需设置
                  .url(url)    //设置请求的url
                  .map(map)    //设置请求参数，没有则无需设置
                  //.encoding("utf-8")//设置请求和返回编码，默认就是Charset.defaultCharset()
                  .client(hcb.setUserAgent("MicroMessenger/6.6.6.1300(0x26060636) NetType/WIFI
anguage/zh_CN").build())    //如果只是简单使用，无需设置，会自动获取默认的一个client对象
                  //.inenc("utf-8") //设置请求编码，如果请求返回一直，不需要再单独设置
                  //.inenc("utf-8")    //设置返回编码，如果请求返回一直，不需要再单独设置
                  //.json("json字符串")    //json方式请求的话，就不用设置map方法，当然二者可以共用

                  //.context(httpCookies.getContext()) //设置cookie，用于完成携带cookie的操作
                  //.out(new FileOutputStream("保存地址"))       //下载的话，设置这个方法,否则不要
置
                  //.files(new String[]{"d:/1.txt","d:/2.txt"})    //上传的话，传递文件路径，一般还需map
置，设置服务器保存路径
                  ;
        respString = HttpClientUtil.post(config);
    } catch (HttpProcessException e) {
        // TODO Auto-generated catch block
        e.printStackTrace();
    }
    return respString;
```

```
}
```

RelynSpider类中的formatUrlMap方法：

```
/**
 *
 * 方法用途: 对所有传入参数按照字段名的 ASCII 码从小到大排序（字典序），并且生成url参数串<b
>
 * 实现步骤: <br>
 *
 * @param paraMap
 *          要排序的Map对象
 * @param urlEncode
 *          是否需要URLENCODE
 * @param keyToLower
 *          是否需要将Key转换为全小写 true:key 转化成小写，false:不转化
 * @return
 */
public static String formatUrlMap(Map<String, String> paraMap, boolean urlEncode, boolean
keyToLower) {
    String buff = "";
    try {
        List<Map.Entry<String, String>> infoIds = new ArrayList<Map.Entry<String, String>>(pa
aMap.entrySet());
        // 对所有传入参数按照字段名的 ASCII 码从小到大排序（字典序）
        Collections.sort(infoIds, new Comparator<Map.Entry<String, String>>() {
            @Override
            public int compare(Map.Entry<String, String> o1, Map.Entry<String, String> o2) {
                return (o1.getKey()).toString().compareTo(o2.getKey());
            }
        });
        // 构造URL 键值对的格式
        StringBuilder buf = new StringBuilder();
        for (Map.Entry<String, String> item : infoIds) {
            if (StringUtils.isNotBlank(item.getKey())) {
                String key = item.getKey();
                String val = item.getValue();
                if (urlEncode) {
                    val = URLEncoder.encode(val, "utf-8");
                }
                if (keyToLower) {
                    buf.append(key.toLowerCase() + "=" + val);
                } else {
                    buf.append(key + "=" + val);
                }
                buf.append("&");
            }

        }
        buff = buf.toString();
        if (buff.isEmpty() == false) {
            buff = buff.substring(0, buff.length() - 1);
        }
```

```
    } catch (Exception e) {
        return null;
    }
    return buff;
}
```

RelynSpider类中的md5方法：

```
/**
 * md5加密方法
 * @param text
 * @return
 */
public static String md5(String text) {
    String result="";
    try {
        MessageDigest md = MessageDigest.getInstance("MD5");
        md.update(text.getBytes("UTF-8"));
        byte b[] = md.digest();
        int i;
        StringBuffer buf = new StringBuffer("");
        for (int offset = 0; offset < b.length; offset++) {
            i = b[offset];
            if (i < 0)
                i += 256;
            if (i < 16)
                buf.append("0");
            buf.append(Integer.toHexString(i));
        }
        result = buf.toString();
    } catch (NoSuchAlgorithmException e) {
        e.printStackTrace();
    } catch (UnsupportedEncodingException e) {
        e.printStackTrace();
    }
    return result;
}
```