GIAC

主办方：msup | 架构 ARCHNOTES

GIAC

全球互联网架构大会

GLOBAL INTERNET ARCHITECTURE CONFERENCE

第三方视角下的移动互联网用户隐私风险

王文杰　　众安天下　　合伙人&CTO

一、自我介绍

- 王文杰，“钢铁”直男
- 曾就职于海尔集团、WatchGuard、元心科技、众安天下；
- 熟悉IoT、网络安全、移动安全、安全攻防、安全加固、安全架构、安全体系建相关领域；
- Linux Kernel、libnl、libxml2、SELinux、D-Bus等开源项目的代码贡献者；
- 工作中获得多项国家发明专利，国标《GB/T 34976-2017 信息安全技术 移动智能终端操作系统安全技术要求和测试评价方法》主要起草人之一；

二、关于众安天下

ALLSEC
众安天下·天下众安

- 基于业务视角的安全理念
- 安全众测、安全服务、安全产品
- 服务驱动业务安全发展和安全体系建设
- 让客户的客户更安全

二、关于众安天下

韩国平昌冬季奥运会网络中断

思科高危漏洞攻击

万豪酒店数据库泄露

湖南省儿童医院HIS服务器加密勒索

华大科技**人类遗传基因**数据泄露

上海市医保系统瘫痪近四小时

Facebook用户数据泄露

深圳“恶意差评师”敲诈勒索电商网店近200家

广东揭阳准大学生遭遇电信诈骗

“美版” Quora上亿**数据泄露**

日常工作最高频的词汇

漏洞

+

风险

三、今天的主题 - 关于隐私和风险

基于业务视角提炼安全风险体系

业务安全	Web安全	认证授权	策略安全	接口安全	内容安全	运营安全
	交易安全	供应链安全	风控策略	爬虫对抗	... ...	应用开发
数据安全	接口安全	传输安全	存储安全	交换安全	使用安全	权限审批
	合规安全	权限策略	数据分级	数据恢复	... ...	运行维护
基础架构安全	数据库	操作系统	备份恢复	日志审计	安全策略	制度流程
	访问控制	身份认证	边界防护	异地灾备	... ...	人员意识
						... ...

三、今天的主题 - 关于隐私和风险

三、今天的主题 - 关于隐私和风险

图 - 网络安全法立法进程

第七十六条 （四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

第二十一条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

三、今天的主题 - 关于隐私和风险

在互联网和大数据崛起的新环境下，欧盟认为 95 指令不能切实保护数据主体的权利和自由，也不能对成员国之间的个人数据保护法加以协调。因此，自 2009年开始，欧盟启动个人数据保护框架的改革工作。

1981
- 《1981年个人数据保护公约》

1995
- 《1995 年个人数据保护指令（简称"95指令"）

2012
- 2012年1月正式发布GDPR草案

2016
- 2016年4月欧盟理事会和欧洲议会表决通过了 GDPR

2016
- 2016年5月4日正式在欧盟官方公报发布

2018
- 2018 年 5 月 25 日直接适用于欧盟全体成员国

GDPR

GDPR起源和重要时间节点

General Data Protection Regulation

GDPR中个人数据是指任何指向一个已识别或可识别的自然人的信息。该可识别的自然人能够被直接或间接地识别，尤其是通过参照诸如姓名、身份证号码、定位数据、在线活动识别符，或者是通过参照针对该自然人一个或多个如物理、生理、遗传、心理、经济、文化或社会身份的要素。实践中，个人数据还包括通过任意一种方式被分配或可被分配给某人的所有数据。例如，电话号码、个人的信用卡或人员编号、账户数据、号牌、外貌和客户号或地址，均属于个人数据。

三、今天的主题 - 关于隐私和风险

极客网 首页 深度 智库 自明星 大事件 大奖 行业 企业专栏

极客资讯 > 极客要闻 > 正文

Facebook漏洞或导致300万欧洲用户信息泄露 GDPR规则下罚款高达16亿美元

2018-10-17 发布

极客网·极客要闻10月17日，福无双至，祸不单行。据CNBC报道，美国当地时间周二，爱尔兰数据保护委员会(IDPC)证实，约有300万欧洲用户受到9月份Facebook安全漏洞的影响，用户的个人信息可能被窃取。按照欧盟新颁布的规定，谷歌或因此面临高达16.3亿美元的罚款。

第一个被GDPR罚款20000欧元的德国暧昧聊天平台

在经历过黑客攻击,导致大约808000个电子邮件地址和超过180万的用户名和密码被泄露后，德国的一个社交网络网站被Baden-Württemberg数据保护局罚款20000欧元。

Microsoft is being investigated by European data regulators. CREDIT: REUTERS

监管机构所控诉的内容以微软Word、Excel、PowerPoint和Outlook的日常监控为中心。报道称，相关数据被查出含有微软Word和电子邮件中的语句，疑似是某种检测机制在对特定动作进行自动侦测（例如拼写检查）。

微软称，收集这些数据是为功能和安全的目的。但荷兰司法部并未对此满意，并在报告中称，数据分析显示所收集的数据中包括电子邮件主题内容。司法部表示："来自用户的数据通过Windows 10企业版和微软Office遭到收集，并存储在了美国的一个数据库，这对用户的隐私构成了重大风险。"

代表荷兰政府进行调查的隐私公司也表示，微软正在进行"大规模的、秘密的数据处理"。

微软曾于今年5月宣布表示，将遵守欧盟《通用数据保护条例》。这项法规被认为是欧洲20多年来对数据隐私法规最大的一次调整。为迎合相关法规的要求，微软已经努力将所收集的数据移回欧洲，并在今年10月同意对旗下服务进行改进。

T早报|谷歌违反GDPR 被法国罚款5000万欧元；韬蕴资本计划甩卖易到股权；[redacted]公布"[redacted]漏洞"案件进展

2019年01月22日 08:44 来源于 财新网

【财新网】谷歌因违反GDPR被法国罚款5000万欧元

据《华尔街日报》，法国政府向谷歌开出了一张5000万欧元（5680万美元）的罚单，指控谷歌违反了欧盟于2018年出台的《通用数据保护条例》（GDPR）。这是GDPR生效以来，欧盟政府开出的金额最高的一张罚单。法国数据保护机构指控，谷歌没有清晰向用户解释，他们的信息将如何用于定向广告，并获得用户的许可。谷歌称，正在研究法国政府的决定，以确定如何回应。

三、用户隐私风险 - 隐私泄露的原因

Android系统提供了一整套强大的安全机制，Android平台近几年隐私泄露问题依旧层出不穷。Android用户隐私数据泄露的主要原因是恶意应用程序、Android权限提升漏洞、应用本身对隐私数据的保护不足

应用市场恶意应用程序

第三方应用市场的崛起

权限提升漏洞

OS权限提升导致高权限获取数据

应用对隐私数据保护不足

配置错误、审核不严格、错误的引用

三、用户隐私风险 - 隐私泄露的方式

[应用之间]

I. 提升系统权限获取隐私；
II. 同一个公司开发的软件有相同的签名，从而共享数据来获取隐私；
III. 通过组件 Intent 这种对象传递相关数据来获取数据；
IV. 可以根据一些全局都可读取的文件来获取相关的隐私；
V. 由组件 Content Provider 提供的一些借口去访问其他一些软件的数据；

[应用中]

I. 日志及日志文件；
II. 网络数据包的传输；
III. 安全漏洞和API被动泄露；

[第三方]

I. 合理集成第三方SDK；

三、用户隐私风险 - 聚焦移动互联网隐私

设备隐私

- 系统版本
- 系统名称
- 设备类型
- 设备名称
- 处理器型号
- 基带版本
- 内核版本
- 存储器出厂编号
- 手机号码
- IMEI
- IP地址
- WLAN MAC
- 蓝牙地址
- 序列号
- Android ID等信息
- ……

● Android设备固有的、可能用于标识用户的数据

系统隐私

- Android操作系统网络访问
- 通讯录
- 通话记录
- 拨打电话
- 发送短信
- 短信内容
- 联系人
- 日历日程
- 相片
- 视频
- 录音
- 手机位置数据
- ……

● 用户在使用Android设备时产生的数据

第三方应用产生的隐私

- 身份信息
- 个人账号
- 登录密码
- 聊天记录
- 浏览记录
- 支付记录
- 交易记录
- 购物行为
- 个人偏好
- 行为轨迹
- 运动数据
- 健康数据
- ……

● 用户在使用应用时产生的数据

四、今日要点

第三方视角下的移动互联网用户隐私风险

Q1.什么是用户隐私

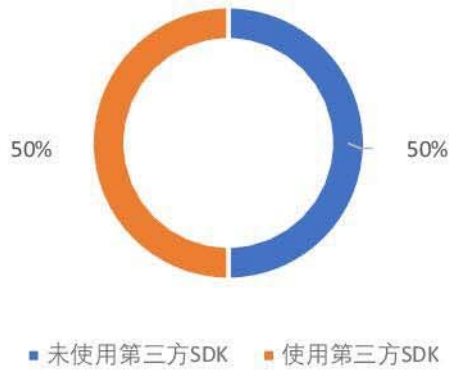
Q2.软件开发人员和安全人员眼中的用户隐私风险

Q3.第三方SDK安全分析

Q4.我们是如何测试的和测试的结论

五、SDK的相关数据 - 第三方SDK集成情况

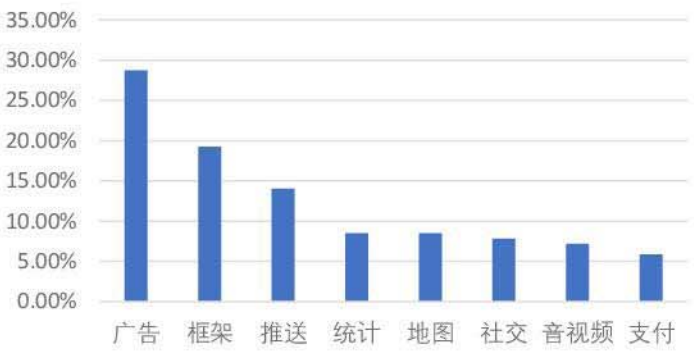
图：267万Android应用集成第三方SDK工具包情况



- 267万Android应用来自于各应用商店、论坛、网盘、企业官方网站；
- 50%左右的应用集成了第三方公司提供的SDK工具包；

五、SDK的相关数据 - 第三方SDK分类和市场占有率

图：414个SDK工具包分类分布



说明：（1）广告类SDK占28.76%；（2）广告 + 框架 + 推送占比超过60%

图：分类SDK市场占有率分布

说明：AdMob、GSON、支付宝、百度地图等SDK在各分类中占有率位居第一

七、SDK还做了什么

编号	检测项	描述
1	android.permission.ACCESS_NETWORK_STATE	允许程序访问有关数据网络
2	android.permission.ACCESS_COARSE_LOCATION	允许一个程序访问CellID或WIFI热点来获取粗略的位置
3	android.permission.WRITE_EXTERNAL_STORAGE	允许程序读写外部存储
4	android.permission.READ_EXTERNAL_STORAGE	允许程序读取外部存储
5	android.permission.ACCESS_WIFI_STATE	允许程序获取无线网络信息
6	android.permission.CHANGE_WIFI_STATE	允许程序改变无线连接状态
7	android.permission.READ_PHONE_STATE	允许程序获取电话状态
	.....	

表：各类被SDK“偷偷”使用的权限

七、SDK还做了什么

编号	检测项	说明
1	检测IMEI获取	国际移动设备识别码（International Mobile Equipment Identity，IMEI）
2	检测android_id获取	设备首次启动时，系统随机生成的64位数字
3	检测IMSI获取	国际移动用户识别码（IMSI：International Mobile Subscriber Identification Number）是区别移动用户的标志，储存在SIM卡中，可用于区别移动用户的有效信息。
4	检测电话号码获取	允许程序获取电话号码
5	检测MAC获取	允许程序获取MAC地址
6	检测IP获取	允许程序获取IP信息
7	检测地理位置获取	允许程序获取设备地理位置
8	检测录音打开	允许程序打开录音
9	检测摄像头打开	允许程序打开摄像头
10	检测彩信读取	允许程序读取彩信
11	检测短信读取	允许程序读取手机短信
12	检测彩信发送	允许程序发送手机彩信
13	检测短信发送	允许程序发送手机短信
14	检测通话记录	允许程序获取手机通话记录
15	检测联系人读取	允许程序读取用户联系人数据
16	检测照片读取	允许程序读取用户照片数据
17	检测健康数据读取	允许程序读取用户健康相关数据

表：SDK获取的各类隐私数据

七、SDK还做了什么

编号	检测内容	说明
1	检测数据传输安全	检测SDK数据传输是否安全
2	检测HTTPS安全	检测SDK是否使用HTTPS进行数据传输
3	检测WebView安全	检测SDK的WebView安全
4	检测存储安全	检测SDK的存储安全
5	检测组件安全	检测SDK的组件安全
6	检测是否远程序更新代码	检测SDK是否存在程序代码后台远程更新
7	检测后台打开WIFI	检测SDK是否存在后台打开WIFI
8	检测后台打开蓝牙	检测SDK是否存在后台打开蓝牙
9	检测后台打开日历	检测SDK是否存在后台打开日历
10	检测后台打开数据网络	检测SDK是否存在后台打开网络

表：SDK本身的安全性、“他们”还可以利用SDK安全弱点做什么

七、SDK还做了什么

```
public synchronized void a(f fVar) {
    Location location = null;
    boolean z = false;
    synchronized (this) {
        e.a(a, "getSystemLocation");
        if (!(fVar == null || this.d == null)) {
            this.e = fVar;
            boolean checkPermission = UMUtils.checkPermission(this.d, "android.permission.ACCESS_COARSE_LOCATION");
            boolean checkPermission2 = UMUtils.checkPermission(this.d, "android.permission.ACCESS_FINE_LOCATION");
            if (checkPermission || checkPermission2) {
                try {
                    if (this.b != null) {
                        boolean isProviderEnabled;
                        if (VERSION.SDK_INT >= 21) {
                            isProviderEnabled = this.b.isProviderEnabled("gps");
                            z = this.b.isProviderEnabled("network");
                        } else {
                            if (checkPermission2) {
                                isProviderEnabled = this.b.isProviderEnabled("gps");
                            } else {
                                isProviderEnabled = false;
                            }
                            if (checkPermission) {
                                z = this.b.isProviderEnabled("network");
                            }
                        }
                        if (isProviderEnabled || z) {
                            e.a(a, "getLastKnownLocation(LocationManager.PASSIVE_PROVIDER)");
                            if (checkPermission2) {
                                location = this.b.getLastKnownLocation("passive");
                            } else if (checkPermission) {
                                location = this.b.getLastKnownLocation("network");
                            }
                        }
                        this.e.a(location);
                    }
```


```
{
 "latitude": 39.95488357543945,
 "longitude": 116.42399597167969,
 "ip": "192.168.3.18",
 "imei": "869963**0095286",
 "model": "FRD-DL00",
 "conn_type": 4,
 "os": 1,
 "os_version": "24",
 "sdk_version": "1.9.*.2",
 "download_sdk_version": "1.9.3.1",
 "app_id": "***"
}
```


七、SDK还做了什么

```
private boolean b(Context context, String str) {
    Iterator it;
    int i = 0;
    int i2 = a;
    i2 = ((((i2 & (--58)) << 1) + ((--58) ^ i2)) - ((-1) ^ -1)) - 1;
    b = i2 % 128;
    switch (i2 % 2 == 0 ? 1 : 0) {
        case 0:
            it = context.getPackageManager().getInstalledPackages(0).iterator();
            break;
        default:
            it = context.getPackageManager().getInstalledPackages(0).iterator();
            break;
    }
    i2 = (a + 88) - 1;
    b = i2 % 128;
    if (i2 % 2 == 0) {
    }
    while (true) {
        switch (it.hasNext() ? 84 : 2) {
```

```
static String getHostString(InetSocketAddress socketAddress) {
    InetAddress address = socketAddress.getAddress();
    if (address == null) {
        return socketAddress.getHostName();
    }
    return address.getHostAddress();
}
```

上报域名：
https://api.tataqou.com.cn

上报内容，包含用户ip地址

```
source=DCYS
appVersion=3.2.0.0
dt=be49725089148da9
deviceId=862525498613116
sv=5041004
pf=ANDROID
v=2.2.5
appDeviceId=111111111111111
tid =
ip=121.71.8.248
pid=65044798
```

```
public static String getImei(Context context) {
    try {
        String imei = ((TelephonyManager) context.getSystemService("phone")).getDeviceId();
        if (Long.parseLong(imei) == 0) {
            return "";
        }
        return imei;
    } catch (Exception e) {
        return "";
    }
}

public static String phoneImei(Context context) {
    String imei;
    try {
        imei = ((TelephonyManager) context.getSystemService("phone")).getDeviceId();
        if (Long.parseLong(imei) == 0) {
            imei = null;
        }
    } catch (Exception e) {
        imei = getAndroidID(context);
    }
    if (!TextUtils.isEmpty(imei)) {
        return imei;
```

七、SDK还做了什么

上报字段	返回字段	数据上报方	上报时机	上报数据的目的	对应的功能	是否存在隐私风险	备注	重要字段

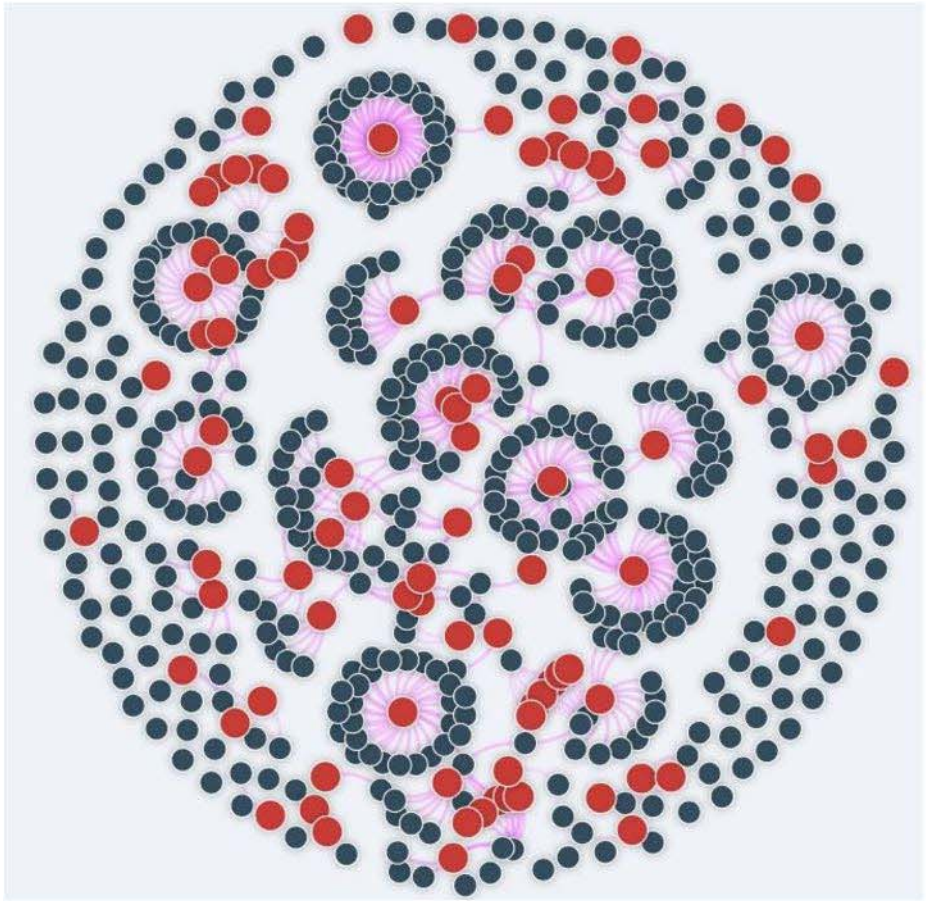
datatype=2&
posh=100&
encext=GJ6APJVjO-ZzLVMIFSsQApNdeu433FKvrPVG-
xq5PQdu9ClkGxdDbKnuoCKmkPt0SKWPjMDCWUFT0shbGRfKzw&
count=1&
er [illegible] =1&
au [illegible] =1&
r=0.56 [illegible] 703999&p [illegible]
ext={"req":{ [illegible] 40741c653 [illegible] 4de92eec0e","m2":"55f2915cc661a43
ed40d68cb1a58 [illegible] ":"da3aa84c [illegible] 23fef555d5da27","m6":"e73c00
dacf2cb1467f98bbc [illegible] ","muidtype": [illegible] 2d540741c653736b00d2de4
de92eec0e","placement_ [illegible] ender_type": [illegible] arrier":2,"loc_src":5,"lat"
:28683854,"lng":116352429," [illegible] ccuracy":40,"s [illegible] op_landing_page":1,
"c_os": [illegible] ","c_osver":"7.0"," [illegible] e":"****","c_de [illegible] RD-
DL00","c_ [illegible] e":1,"c_mf":"HUAW [illegible] ":0,"c_w":108 [illegible] 20,"sdkver":"
4.9.584","jsve [illegible] ","tmpallpt":true,"p [illegible] ":1,"deep_link_v [illegible] "c_sdfre
e":17695322112,"c_ [illegible] 8","c_hl":"zh","go [illegible] 540741c65373b [illegible] de4de9
2eec0e_15466626537 [illegible] ","filterappname":[[illegible] e,"scs":"0001fffc8d1b","ast"
:{"br":"honor","de":"HWFRD","fp":"honor\%2FFRD-
DL00\%2FHWFRD:7.0\%2FHUAWEIFRD-DL00\%2FC0 [illegible] r\%2Frelease-
keys","hw":"hi3650","pr":"FRD-DL00","sr":"NXTDU16811000 [illegible] is_d":true}}
	{"ret":0,
	"rpt":0,
	"msg":"",
	"seq":"47",
	"reqinterval":1740,
	"last_ads":{"responsed_ad_data":"8Q1_qpR5jjA"}
	,
	"data":{
	"9079537218417626401":{
	"ret":0,
	"msg":"",
	"list":[{"cl":"54022290",
	"img":"http://pgdt.ugdtimg.com/gdt/0/DAAOuWQAKAABkAAaBa8RJICM19PKRQ.jpg/0?ck=694416090795429b0413b5967499d614",
	"img_s":"",
	"video":""
		SDK	广告获取	广告获取	广告获取	是	有地理位置	m1:md5(imei)
								m2:md5(mac)
								m3:md5(androidid)
								m4:md5(Google Advertising ID)

密文	密文，解密后 {"ret":0,"seq":48,"setting":{"app":"eyJkb3dubG9hZF9jb25maXJtIjozLCJkb3dubG9hZF9wYXVzZSI6MCwicHMiOnsiNDA0MDQzMzI1MTg0MzUwNiI6eyJwb3NpZCI6NDA0MDQzMzI1MTg0MzUwNiwic3RvcCI6MCwidGVzdGFkIjowLCJkb3dubG9hZF9jb25maXJtIjoxLCJvdmVybGFwX2NoZWNrX3JhdGUiOjAsImV4cG9zdXJlX3RpbWVfY2hlY2tfcmF0ZSI6MCwicmVxdWlyZV93aW5kb3dfZm9jdXMiOjEsImZvcmNlX2V4cCI6MCwic2hvd19sb2dvIjoxfSwiODU3NTEzNDA2MDE1MjEzMDg0OS	SDK	事件上报，程序开启、得到广告、点击、消息等	统计信息并获得相应配置	统计信息并获得相应配置	是	使用http协议，固定密钥加密，容易被破解	解密： {"suid":"fd3b0664-df15-4e1a-abbb-2208efc9dc8e","sid":"","sig":{"app":"n1lfmjRoraoU6IRHR8y4Qd1V6MTem8RZySafq3+6nJq+VY0deUervwbN3dAOi7wjG1Mb5fHg7FyaQy0n0UXMaC7baKO5uuvZJ1NzFxcGV/xgRk0Osor2qe8nALD5pBLbxcpJ5nfAiQRH1bWjwzGi48hrLkeYvF+TbOGCsRsgxPC4=","sdk":"PYat7Lg4biPBBxVURe+o0oFOciWD59RugSPx66LOXwv5f9pYP9fhmpFnLeLKwheVZFwJQOlaqiIVOSAJNAtzQcgHJubEIVWHhjd6515cCXl8qcCclOTAzlvhsRx7BQltkWzj
actionid=5&targettype=6&tagetid=801097412&sellerid=801097412&clickid=jc7e4xg2aaako7p [illegible]	0	SDK	事件	事件跟踪	事件统计	是		
conv_type=" [illegible] ing.valueOf(arg8)).append("&imei").append("=").append(v0).append("&ap [illegible] nd("=").append("ANDROID").append("&client_ip").append("=").append(v [illegible] "conv_time").append("=").append(v2).append("&pkg_name").append("=").ap [illegible] end("&click_id").append("=").append(arg9);		SDK	用于点击广告事件分析	用于点击广告事件分析	用于点击广告事件分析	否	IMEI、IP数据被上传，且使用http协议	

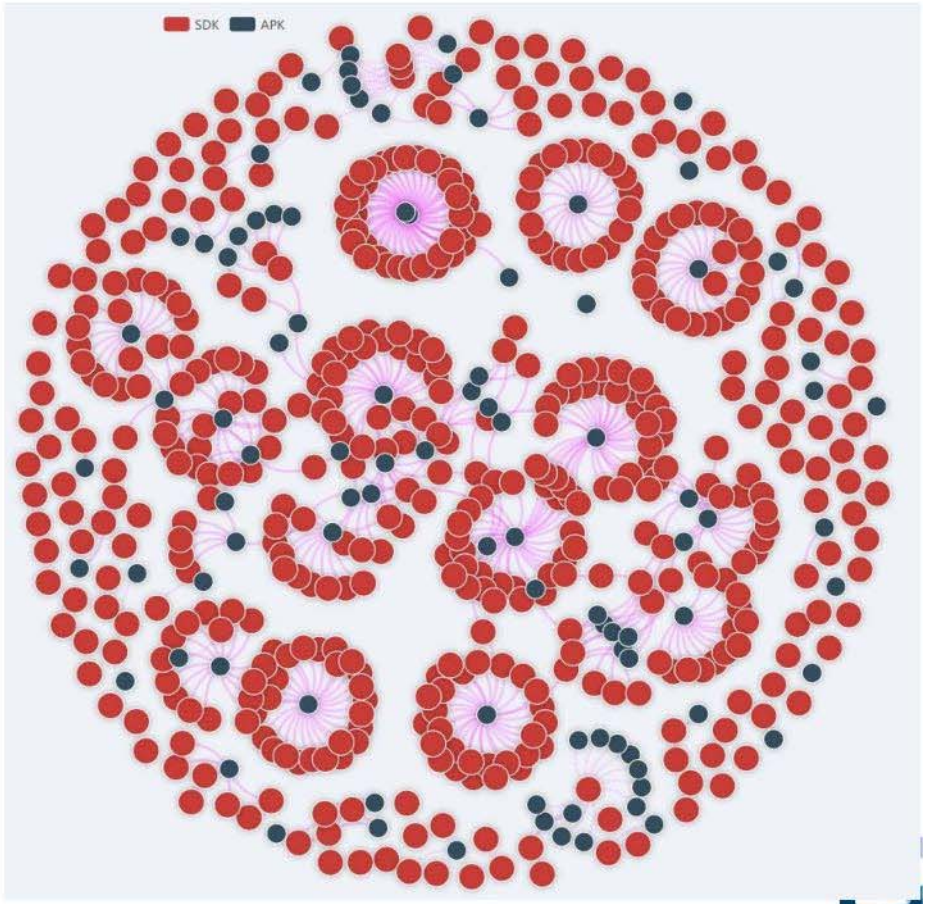
七、SDK还做了什么 - 一些“有趣”的行为

- 每6小时定时获取手机上的应用列表并回传；
- DexClassLoader类用来加载外部的DEX或者JAR文件，远程代码执行；

八、用户隐私风险态势 - SDK/APK关联关系



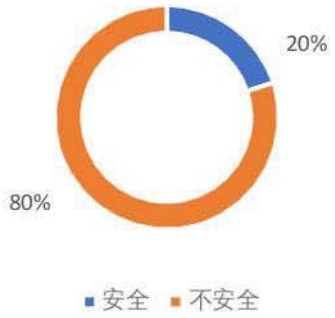
图：APK - SDK关系图



图：SDK - APK关系图

八、用户隐私风险态势 - 总览

图：第三方SDK隐私泄露和安全性情况



I. 80% = 40% + 40%；

II. 知名SDK的情况；

III. 国内SDK vs 国外SDK；

IV. 开源SDK的情况；

八、用户隐私风险态势 - 典型问题

01

隐私数据TOP5

1. 设备信息
2. 应用列表
3. 广告播放情况
4. 应用崩溃信息
5. 获取配置信息

02

SDK安全隐患TOP4

1. 未使用HTTPS安全传输
2. HTTPS未进行强校验
3. WebView安全隐患
4. 后台可远程更新代码

03

最值得关注的问题TOP2

1. 后台静默上传
2. 代码远程执行

九、一点建议

I. 尽可能减少不必要的第三方SDK的使用；

II. 审计有无集成但未调用的第三方SDK；

III. 关注第三方SDK“还”做了哪些事情；

IV. 关注第三方SDK本身的安全性；