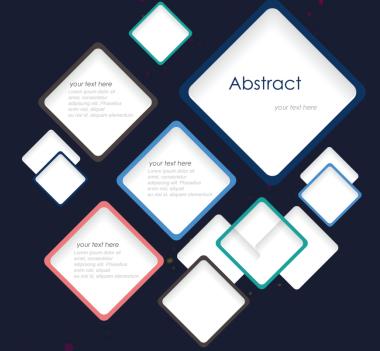
隐私合规测试实践

沈海涛 OPPO子午互联网安全 实验室负责人





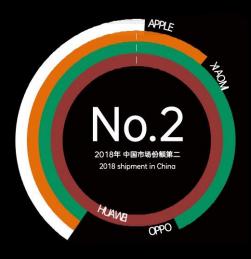
- 1 背景
- 2 技术需求分析
- 3 方案优化演进
- **4** Q&A



背景

背景-业务





Source: 《IDC中国季度手机市场跟踪报告,2018年第四季度》

Market Share, and Year-Over-Year Growth, Calendar Year 2018(shipments in millions of units)

SANATION

SANATION

SANATION

2018年全球市场份額第五 2018 shipment in Global

Top 5 Smartphone Companies, Worldwide Shipments,

Source: IDC Quarterly Mobile Phone Tracker, January 30, 2019

2018年,OPPO取得中国市场份额第2, 世界市场份额第5 In 2018, OPPO's shipment in China ranked No.2 and its shipment in the world No.5

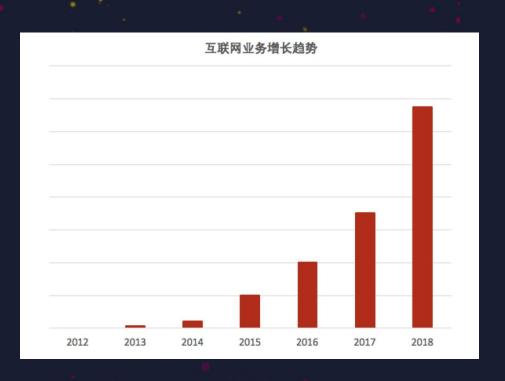
背景-业务

oppo

手机销往全球30+国家和地区

Color OS全球月活用户数3.1亿





背景-法律法规

oppo

一、《欧盟GDPR》

-堪称史上最严格的数据保护条例-

最高处以2千万欧元或上年度全球营业额4%的行政处罚

Google受罚首例。2019年1月,法国数据保护机构CNIL宣布,对Google处以5000万欧元(约合5700万美元)的罚款。机构称,在用户使用Android手机时,Google未能遵守欧盟隐私法——《通用数据保护条例》(GDPR)。Google没有向用户正确披露获取数据的目的、数据的储存期以及哪些数据用于个性化广告等。例如,用户想知道他们的数据如何用于个性化广告,一般需要5或6次点击。CNIL表示,通常很难理解你的数据是如何被使用的,因为谷歌的措辞是广泛而且模糊不清的。

背景-法律法规

oppo

二、《中华人民共和国网络安全法》&《个人信息安全规范》

-《个人信息安全规范》-中国版的GDPR-

虽然《个人信息安全规范》性质上为推荐性国家标准,不具有强制执行力, 但作为《网络安全法》等法律法规的配套技术规范,对于行政主体、司法 机关和企业都具有普遍的适用性。《个人信息安全规范》本身只设定适用 条件和行为模式,并未设定相应的行为后果,但该规范将是行政主体和司 法机关判断事实和构成要件的依据,如果违反其中体现《网络安全法》等 法律关于个人信息保护的强制性要求的,行政主体和法院可以依据相关法 律设定的行为后果作出处罚和判决,企业可能承担相应的民事、行政和刑 事责任。



技术需求分析

隐私合规测试点



隐私政策文本要求

收集使用个人行为信息要求

. . .

. . .

用户权利的保障

日志

隐私合规测试点

个人信息使用加密协议传输(如https等)

通信

个人敏感信息(身份证号码、银行卡号等)传输时要实施内容加密。

存储

使用

需求点

oppo

能够分析SSL/TLS 加密流量 能够识别流量中的 个人敏感数据



现状分析

oppo

手机: 最新出货版本

系统: android 9

权限: adb root

权限:修改系统文件难度较大

技术方案选型

oppo



Xposed + ustTrustMe

Frida + by vass.js +Burp



方案优化演进





Frida bypass 脚本
https://codeshare.frida.re/browse
针对具体情况可能要有一些定制原则是尽量hook系统底层

# •	Host				Method	URL	Params	Edit
2424	https://a	ıpi.map.ba	idu.cor	n	POST	/geocoder/v2/	✓	
4								
	Υ_							
Requ	est Resp	onse						
Raw	Params	Headers	Hex					
		/v2/ HTT	P/1.1					
test:	0000	annliant	ion/r	-www-form-urlence	odod			
						PBDM00 Build/OPM1.171019.026)		
Host:	api.map.	baidu.co		, - ,	,	,		
	tion: cl		J-61.					
	t-Encoain t-Length	g: gzip, : 295	deila	ate				
						=4.9E-324%2C4.9E-324&output=js		
110088	bulld=/2	1&OS=And	roid2	/&1me1=869166030	496458&M	o=PBEM00&from=BaiduNLP&languag	e=zn-CN&	rang



开发: 我不走系统代理, 看你怎么抓包

```
HttpURLConnection:

URL url = new URL(urlStr);
urlConnection = (HttpURLConnection) url.openConnection(Proxy.NO_PROXY);

OkHttp:

OkHttpClient client = new OkHttpClient().newBuilder().proxy(Proxy.NO_PROXY).build ();
```



oppo

攻防:我有hook大法,想抓就抓

try {

```
var URL = Java.use("java.net.URL");
    URL.openConnection.overload('java.net.Proxy').implementation = function()
        return this.openConnection();
} catch(e) {
    console.log("" + e);
try {
    var Builder = Java.use("okhttp3.0kHttpClient$Builder");
    var mybuilder = Builder.$new();
    Builder.proxy.overload('java.net.Proxy').implementation = function(arg1)
        return mybuilder;
} catch(e) {
    console.log("" + e);
```



oppo

开发:让你找不到hook的点,且每次变,看你咋办

```
end color.support
e com
dalvik.system
io.protostuff
javax.annotation
H libcore
d okhttp3
 internal
    HttpUrl
     Protocol
    TIsVersion
▼ G a
      ₫ 1: HttpUrl
     ₫ o: 5
      b: س کے
      : List
      List : سر 🏗

▲ : ProxySelector

     Proxy : و

▲ : HostnameVerifier

     g: و 🚣
```

```
package okhttp3;
import a.a.a.cga;
import java.net.Proxy;
import java.net.ProxySelector;
import java.util.List;
import javax.annotation.Nullable;
import javax.net.SocketFactory;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.SSLSocketFactory;
import okhttp3.HttpUrl.Builder;
/* compiled from: Address */
public final class a {
    final HttpUrl 1;
    final o <;</pre>
    final SocketFactory >;
    final b >:
    final List<Protocol> /":
    final List<k> >;
    final ProxySelector @;
    @Nullable
    final Proxy >;
    @Nullable
    final SSLSocketFactory *;
    @Nullable
    final HostnameVerifier 
    @Nullable
    final a :
```



攻防:看来只能降维打击了

使用 iptables 转发应用流量:

iptables -t nat -A OUTPUT -p tcp -m owner --uid-owner 应用uid -j DNAT --to-destination ip:端[

同时需要设置 burp 透明代理



ו־ (II OWI	ופונ	iiu-owii	61 V	У П Jui	u -j D	INAI -	-to-ut	estiliatio	II ih				
Burp	Intruder Rep	oeater Wind	ow Help											
Targ	et Proxy	Spider Sca	nner Intruder	Repeate	r Sequence	er Decoder	Comparer	Extender	Project options	User				
Intercept HTTP history WebSockets history Options														
?	Proxy List Burp Proxy		rs to receive inc	oming H	ITP requests	s from your	browser. You	ı will need t	o configure your l	orowse				
	Add Running		Interface	Invisible	Redirect		Certificate							
	Edit	V	192.168.0.18:	8080	✓		ı	Per-host						
	Luit		0 0			Edit proxy listener								
	Remove		Binding Reque	est handl	ing Certific	cate								
These settings control whether Burp redirects requests received by this listener.														
	Each installation of Bu another installation of		Redirect t	o host:										
			Redirect t	o port:										
	Import / 6	export CA	☐ Force use of SSL											
?	Intercept	Client F	Invisible proxy support allows non-proxy-aware clients to connect directly to the listener.											
Use these settings to Intercept requests			Support invisible proxying (enable only if needed)											
								•						
						-			-					

oppo

开发:哎呦,不错哦。那我们走TCP/UDP吧



```
String message = "Hello IdeasAndroid udp!";
int server port = 12345;
DatagramSocket s = null;
try {
    s = new DatagramSocket():
} catch (SocketException e) {
    e.printStackTrace():
InetAddress address = null;
    address = InetAddress.getByName("192.168.0.8");
} catch (UnknownHostException e) {
    e.printStackTrace();
int msg_length = message.length();
byte[] messageByte = message.getBytes();
DatagramPacket p = new DatagramPacket(messageByte, msg length, address, server port):
trv {
    s.send(p):
} catch (IOException e) {
    e.printStackTrace();
```



攻防:还真的有点难住我了。。。

嗯,burp 抓不到,直接 Frida hook 打印出来好啦。



```
[*] Intercepting on ddns.android.netcapture (pid:23245)...
[-] OpenSSLSocketImpl pinner not found
org.conscrypt.Platform not found!
com.android.org.conscrypt.NativeSsl not found!
org.conscrypt.NativeSsl not found!
Hello IdeasAndroid tcp!
```



开发:换个思路,流量任你抓吧,让你看不懂总行了吧

POST /update/v3/check HTTP/1.1 host: i

```
sign: 7455120284fb14603072f4312efc12e9
Accept: application/x-protobuff; charset=UTF-8
Content-Type: application/x-protobuff; charset=UTF-8
Content-Length: 5148
Connection: close
Accept-Encoding: gzip, deflate
                                             .UpgradeRequyqfds
com.android.browser
                         ( com.
com.android.calendar �
                                                           UpgradeReg
            hemespace �0 (�)com.c
                     🖪 rom 🍪 '
```





Protobuf 是 google 开源的一种平台无关、语言无关、可扩展且轻便高效的序列化数据结构的协议,可以用于网络通信和数据存储。

其具有体积小、序列化和传输速度快、维护简单的特点,被越来越多的安卓 APP 使用。

Burp插件: https://github.com/nccgroup/blackboxprotobuf



```
Request
     Params Headers Hex Protobuf
                                                                        Validate
                                                                      Save Type
     "1": "qqqqqqqqqqwqwqc
     "2": 32011144444444.
                                                                      Load Type
     "4": 122222222332333333,
                                                                       Edit Type
     "127":
                                                                        Reset
                                 "UpgradeReguygfds"
     "2": 301,
      4": 0,
     "1": "com.android.browser",
     "2": 50400,
```

oppo

开发: 真是拿你没办法, 埋个坑送给你。

于是开发将不同出货区域、不同定制版集成到了同一个 app 中。

意味着:不同的环境会触发不同的代码分支,可能会携带不同的数据请求不同的域名。进行隐私合规测试的时候,需要模拟大量的环境,且不能保证没有遗漏。

oppo

攻防: 嗯,干得漂亮。。。

不过,我们还有一招:基于污点的静态分析。



```
String imei = telephonyManager.getDeviceId();
switch (areaType) {
    case CHINA:
       Log. d( tag: "neixiao_log", imei):
        break:
    case INDIA:
       Log. d( tag: "waixiao_log", imei); Path0:
        break:
    case FRANCE:
        Log. d( tag: "gdpr_log", imei);
        break
```

- -> <ddns. android. privacytest. MainActivity: void onCreate(android. os. Bundle)>
 - -> \$r6 = virtualinvoke \$r3. <android.telephony.TelephonyManager: java.lang.String getDeviceId()>()
- -> <ddns. android. privacytest. MainActivity: void onCreate(android. os. Bundle)>
 - -> staticinvoke <android.util.Log: int d(java.lang.String, java.lang.String)>("gdpr_log", \$r6)

Path1:

- -> <ddns. android. privacytest. MainActivity: void onCreate(android. os. Bundle)>
 - -> \$r6 = virtualinvoke \$r3. <android.telephony.TelephonyManager: java.lang.String getDeviceId()>()
- -> <ddns. android. privacytest. MainActivity: void onCreate(android. os. Bundle)>
 - -> staticinvoke <android.util.Log: int d(java.lang.String, java.lang.String)>("waixiao_log", \$r6)

Path2:

- -> <ddns. android. privacytest. MainActivity: void onCreate(android. os. Bundle)>
 - -> \$r6 = virtualinvoke \$r3. <android.telephony.TelephonyManager: java.lang.String getDeviceId()>()
- -> <ddns. android. privacytest. MainActivity: void onCreate(android. os. Bundle)>
 - -> staticinvoke <android.util.Log: int d(java.lang.String, java.lang.String)>("neixiao_log", \$r6)



更多优化 - 效率



				- 4		F 10							
	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	SSI	L	IP
kanaamaa com	GET	/index.php?q=index/indexnew	✓		200	1742	JSON	php					22
k.nearme.com	POST	/index.php?q=index/subfeed	✓		200	447	JSON	php		13330994619 13252054003			22
pp emebile.com	GET	/generate_204			204	323							14
du.com	POST	/			302	1212	HTML		•				14
ers.google.cn	GET	/generate_204			204	102							20
k. 1	GET	/index.php?q=index/feedbacktype	✓		200	504	JSON	php					22
k.neame.co.n	GET	/index.php?q=index/indexnew	✓		200	1742	JSON	php					22
k.n eanmeesen 1	GET	/index.php?q=index/comquedetail&ci	✓		200	2182	JSON	php					22
.baidu.com	POST	/statloc	✓		200	159	JSON						16
o.baidu.com	POST	/geocoder/v2/	✓		200	5301	script			001003289013420	,	✓	16
K. Tearma com	GET	/index.php?q=index/indexnew	✓		200	1742	JSON	php					22
k.n	GET	/index.php?q=index/indexnew	✓		200	1742	JSON	php					22
1	GET	/index.html			200	11024	HTML	html					22
k.n .cu.mercen 1	GET	/index.html			200	11024	HTML	html					22
ou.com	POST	/q	✓		404	184	HTML						11
finz.cppemoh	POST	/api/pin/v1/reset-pin	✓		200	719	JSON			001003289013420	,	√	22
o.baidu.com	POST	/sdk.php	✓		200	540	text	php			,	✓	16
o.baidu.com	POST	/sdk.php	✓		200	540	text	php			,	✓	16
finz. czpamab	POST	/api/pin/v1/rule-check	✓		200	738	JSON			001003289013420	,	✓	22
o.baidu.com		/sdk.php	✓		200	540	text	php			•	✓	16
o.baidu.com		/sdk.php	✓		200	540	text	php			,	✓	16
com	POST	/			302	366	HTML		30				18
promobile	GET	/generate_204			204	325							14
ogle.cn	GET	/generate_204			204	102							20
.baidu.com	POST	/statloc	✓		200	159	JSON						16
f inzioppomob	GET	/favicon.ico			404	747	HTML	ico	40		,	✓	22
f inanoppomob	GET	/static/icon_remove.png			200	2376	PNG	png			,	✓	22
f inz.eppemeb	GET	/static/shouqi.png			200	755	PNG	png			,	✓	22
fi nz oppomob	GET	/static/js/views/resetPassAuth.39a56			200	29582	script	js	ſ		一 ,	✓	22
f	GET	/views/resetPassAuth.html?target=_bl	✓		200	2591	HTML	html	åį.	001003289013420	,	✓	22
ppomobile sum	GET	/generate_204			204	203				001003289013420			12
Г	POST	/api/auth/identify/v1/four-element	✓		200	1500	JSON			æ ¬è¾°ä¾ 13330994619 00100328901342	0 ,	✓	22
.baidu.com	POST	/sdk.php	✓		200	540	text	php				V	16

更多优化 - 覆盖率

oppo

静态污点分析:

Source不仅要覆盖系统函数(IMEI、GPS、电话号码等),还要覆盖用户输入的信息(身份证号码、地址等)。

Sink要尽可能的覆盖全,如日志打印、各种网络请求



oppo

04 章节 **PART**

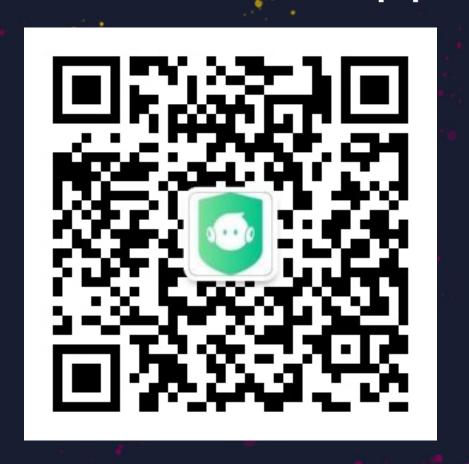
Q&A

子午互联网安全实验室

oppo

专注于隐私保护、IoT安全、红 蓝对抗等领域的安全技术研究。





OGeek oppo



your text here

Abstract

your text here

your fext here
Lorem ipsum dolor sit
amet, consectetur
adipiscing elit. Phaselius
enim nist, aliquet
eu nisi id, aliquam elementu

your text here