浅析Android平台漏洞挖掘

蚂蚁金服 巴斯光年实验室

移动安全研究员 超六

Weibo：@SuperSix666

目录

CONTENTS

About Me ?

- 蚂蚁金服移动安全研究员
- 主攻Android平台
  - framework&App漏洞研究
  - 逆向分析
- CTFer，参加过ZCTF final、0ctf final . . .
- CVE-2016-6920、CVE-2017-5351、
  各类app漏洞 . . .

Android平台漏洞综述

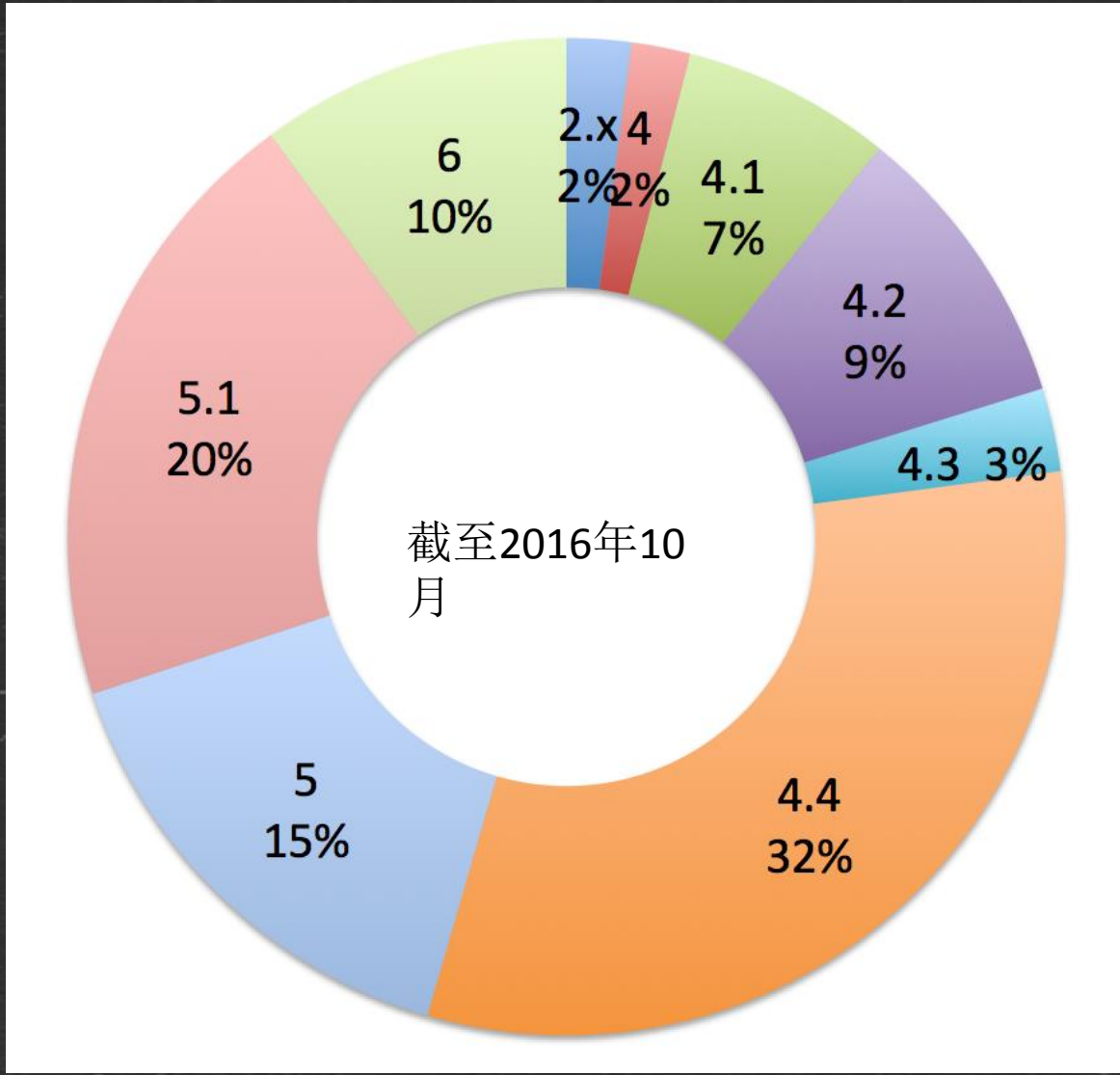
漏洞之王？

Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2016

Go to year: 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	523
2	Debian Linux	Debian	OS	319
3	Ubuntu Linux	Canonical	OS	278
4	Flash Player	Adobe	Application	266
5	Leap	Novell	OS	259
6	Opensuse	Novell	OS	228
7	Acrobat Reader Dc	Adobe	Application	227
8	Acrobat Dc	Adobe	Application	227
9	Acrobat	Adobe	Application	224
10	Linux Kernel	Linux	OS	216
11	Mac Os X	Apple	OS	215

碎片化严重



CVE-2016-5195 dirtycow

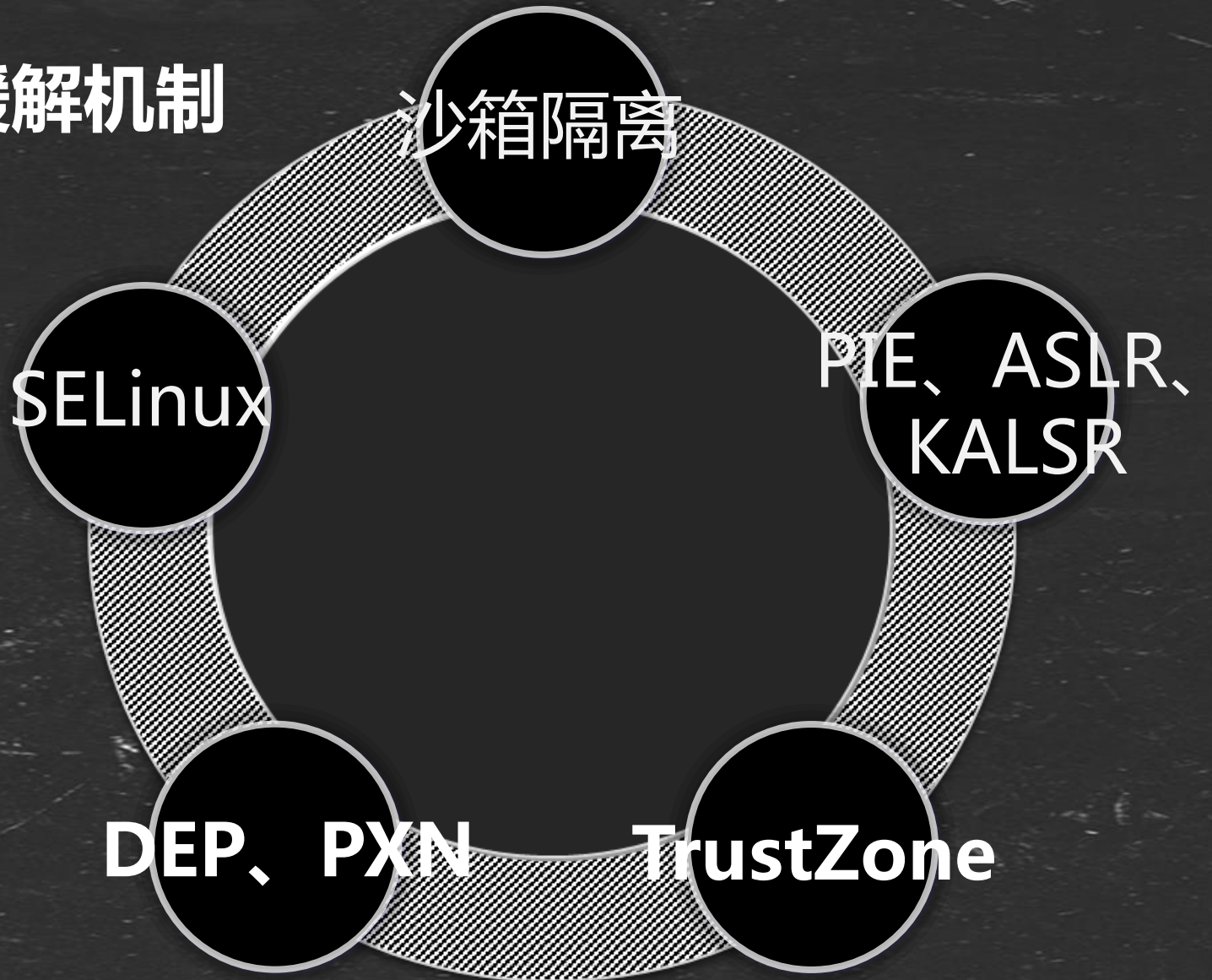
CVE-2015-3636 KEEN TEAM PingPongRoot

Others

- Master Key漏洞
- Stagefright漏洞
- X5内核BadKernel漏洞
- Baidu全系列WormHole漏洞
- 。。。

Android平台下的漏洞缓释技术

漏洞缓解机制



Google Bounty

Severity	Bug Report* + Proof of concept + CTS + patch	Bug Report* + Proof of concept + (CTS or patch)	Bug Report* + Proof of concept
Critical	$8,000	$6,000	$4,000
High	$4,000	$3,000	$2,000
Moderate	$2,000	$1,500	$1,000
Low	$1,000	$500	$333

Samsung Bounty

We are planning to establish a rewards program as a compensation for helping Samsung to improve the security of our products. And we would like to offer you our reward as part of our unofficial pilot program.

Still being a pilot program, please understand that it may take up to 2 months until you receive the reward as we move through our internal process.

If you are interested in this offer, please let us know your acceptance along with attached report form:

Once you accept the reward program, we will ask further document such as bank information for actual payment process.

Thank you.

Very Respectfully,
Samsung Mobile Security Bounty Team

应用层漏洞挖掘


防守
Mark
Black Diamond
VS
进攻
WUHUA
family永恒荣耀
可获取的战利品:
33 199
327 223
2 811
获得战利品:
0
32
0
回放
战果
0%
1x
回营
离回放结束还有:
2分钟 54秒
bbs.duowan.com

- 四大组件
  - export=true
  - registerReceiver

→ 攻击入口

- 高权限代码
  - exec()
  - loadUrl()

→ 缺少校验

- 网络通信
  - https证书未校验
  - 开放端口、协议解析

案例一：信息泄露

```
<activity android:configChanges="keyboardHidden|orientation|screenSize" android:name
    <intent-filter>
        <action android:name="android.intent.action.VIEW" />
        <category android:name="android.intent.category.DEFAULT" />
    </intent-filter>
</activity>
```

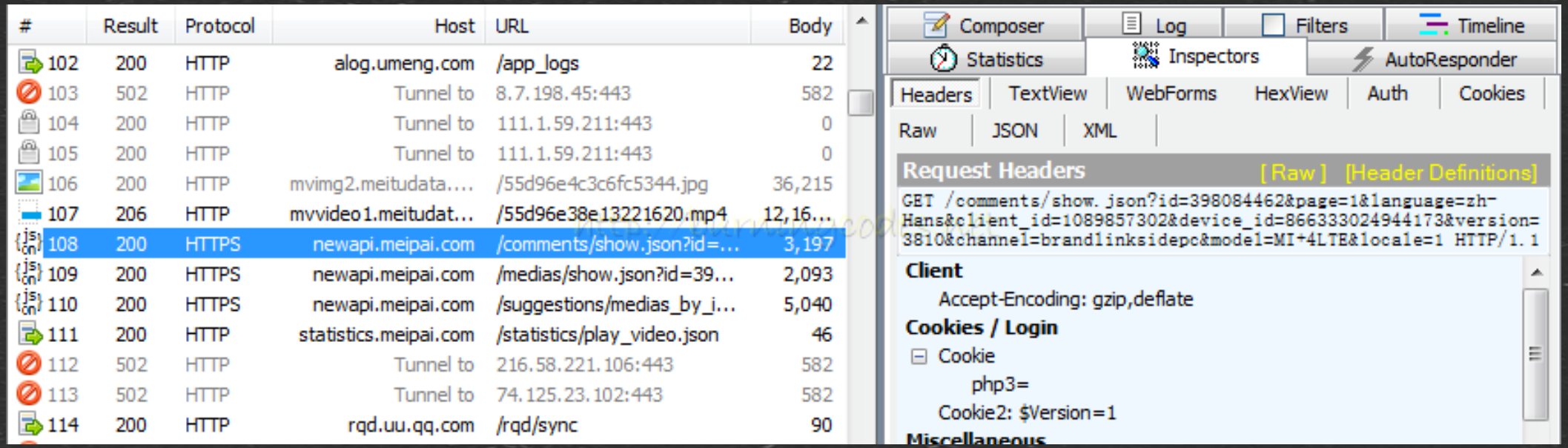
```
protected void safeOnResume() {
    super.safeOnResume();
    if(this.ifRefresh.booleanValue()) {
        this.url = this.getIntent().getStringExtra("url");
        this.mWebView.loadUrl(this.url);
        this.ifRefresh = Boolean.valueOf(false);
    }
```

案例一：信息泄露

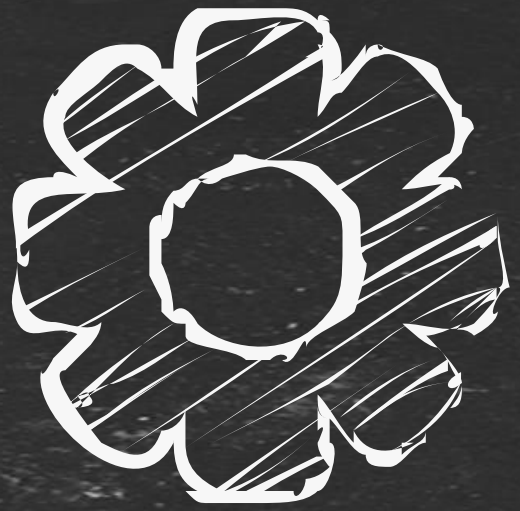
```
Intent i = new Intent(Intent.ACTION_VIEW);

i.putExtra("extrakey_url","file:///data/data/xxx");
```

案例二：https中间人攻击

```
private HttpClient a() {
    KeyStore v0 = KeyStore.getInstance(KeyStore.getDefaultType());
    v0.load(null, null);
    l v1 = new l(v0);
    ((SSLSocketFactory)v1).setHostnameVerifier(SSLSocketFactory.ALLOW_ALL_HOSTNAME_VERIFIER);
    BasicHttpParams v0_1 = new BasicHttpParams();
    HttpProtocolParams.setVersion(((HttpParams)v0_1), HttpVersion.HTTP_1_1);
```



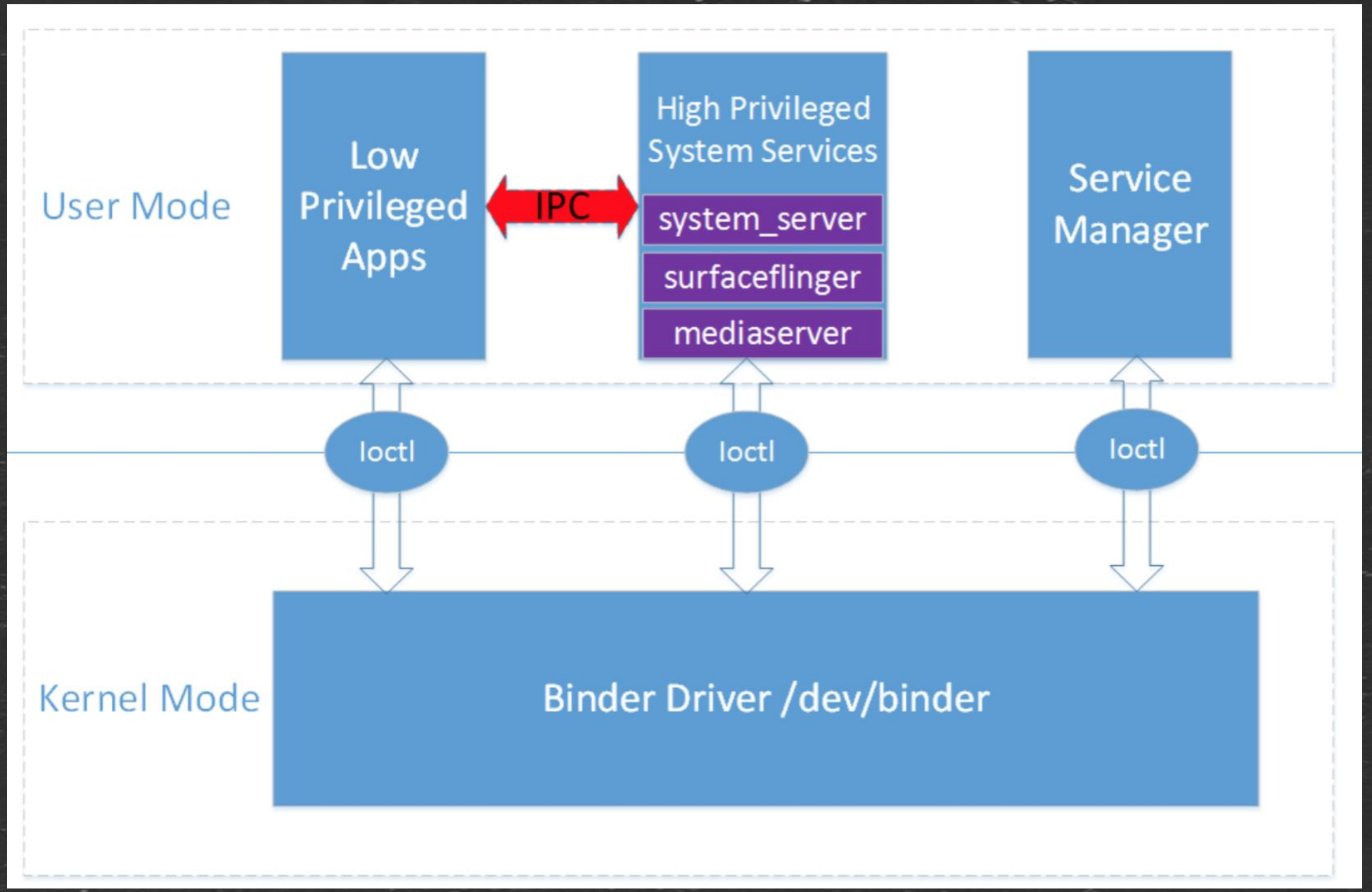
- Drozer
- JEB
- 学习一门脚本，推荐python
- 学习历史漏洞



系统层漏洞挖掘


内核
第三方
厂商代码
Android
Framework

- Binder体系的java服务(有Stub接口,也就是AIDL封装)
- Binder体系的Native服务
- socket体系的init服务(通常见于init.rc)
- 其他服务

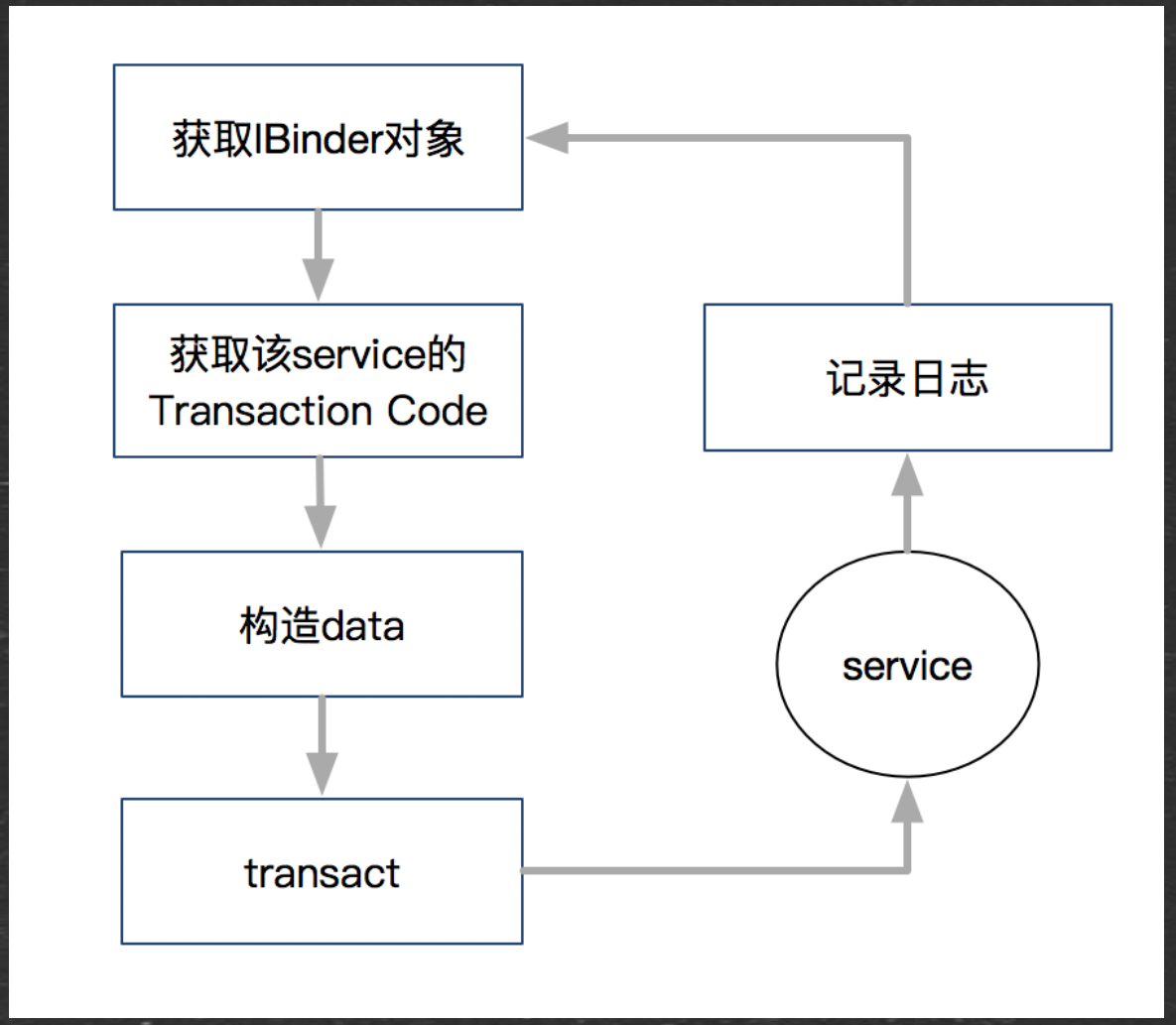

User Mode
Low Privileged Apps
IPC
High Privileged System Services
system_server
surfaceflinger
mediaserver
Service Manager
Ioctl
Ioctl
Ioctl
Kernel Mode
Binder Driver /dev/binder

```
[burningcodes:~$ adb shell service list
Found 182 services:
0       hermesservice: [com.samsung.android.hermes.IKerykeion]
1       AtCmdFwd: [com.qualcomm.atfwd.IAtCmdFwd]
2       sip: [android.net.sip.ISipService]
3       carrier_config: [com.android.internal.telephony.ICarrierConfigLoader]
4       phone: [com.android.internal.telephony.ITelephony]
5       isms: [com.android.internal.telephony.ISms]
6       iphonesubinfo: [com.android.internal.telephony.IPhoneSubInfo]
7       simphonebook: [com.android.internal.telephony.IIccPhoneBook]
8       telecom: [com.android.internal.telecom.ITelecomService]
9       isub: [com.android.internal.telephony.ISub]
10      secontroller: [com.samsung.android.nfc.mpos.IMPOSAdapter]
11      nfccontroller: [com.gsma.services.nfc.INfcController]
12      nfc: [android.nfc.INfcAdapter]
```

Service潜在问题

- Java层服务
  - 权限泄露。 比如锁屏绕过
  - 本地DOS。 导致手机重启等
- Native层服务
  - 堆栈溢出。权限提升
  - 整数溢出、race等

Java层service fuzz



- 从ServiceManager获取Ibinder对象
- 反射Stub类获取Code
- 反射Stub类获取参数类型
- 构造data发送畸形数据
- 日志监控

CVE-2017-5351 (SVE-2016-7650)

```
3108  3108 I ServiceManager: service 'persona_policy' died
3108  3108 I ServiceManager: service 'sdp_log' died
3108  3108 I ServiceManager: service 'dlp' died
3108  3108 I ServiceManager: service 'log_manager_service' died
3108  3108 I ServiceManager: service 'enterprise_license_policy' died
3108  3108 I ServiceManager: service 'application_policy' died
3108  3108 I ServiceManager: service 'wifi_policy' died
3108  3108 I ServiceManager: service 'phone_restriction_policy' died
3108  3108 I ServiceManager: service 'remoteinjection' died
3108  3108 I ServiceManager: service 'knox_ucsm_policy' died
3108  3108 I ServiceManager: service 'edm_proxy' died
3108  3108 I ServiceManager: service 'mum_container_policy' died
3108  3108 I ServiceManager: service 'enterprise_billing_policy' died
```

THANKS

蚂蚁金服 巴斯光年实验室

移动安全研究员 超六

Weibo：@SuperSix666

yaoguang.cyg@antfin.com