

遵守国家信息安全法律法规，
仅限个人学习使用！！！！

内部学习资料，请勿随意传播！

ANDROID安全与防护

钱 权

qqian@shu.edu.cn

上海大学计算机学院

2025年5月

主要内容

- ❖ 一、Android安全基本原理
- ❖ 二、Android安全威胁与应对
- ❖ 作业（研讨内容）

（1）查阅文献就一种具体的移动系统（安卓、鸿蒙或者IOS）安全，给出其威胁原理描述和相应的防御措施；

（2）针对一种具体的移动系统安全方法（登录系统、数据安全、应用安全等），进行程序模拟和实现；

注：以上内容2选1，鼓励选2



Android市场占有率

- ❖ IDC报告显示，预计2019年Android智能手机平均销售额将增长3.2%至263美元，高于2018年的254美元。到2023年，安卓智能手机设备的出货量将达到13亿。

IDC新报告：2019年安卓手机占87%市场份额，iPhone仅占13%



超能网

发布时间：19-09-10 15:23 | 广州超能网络科技有限公司

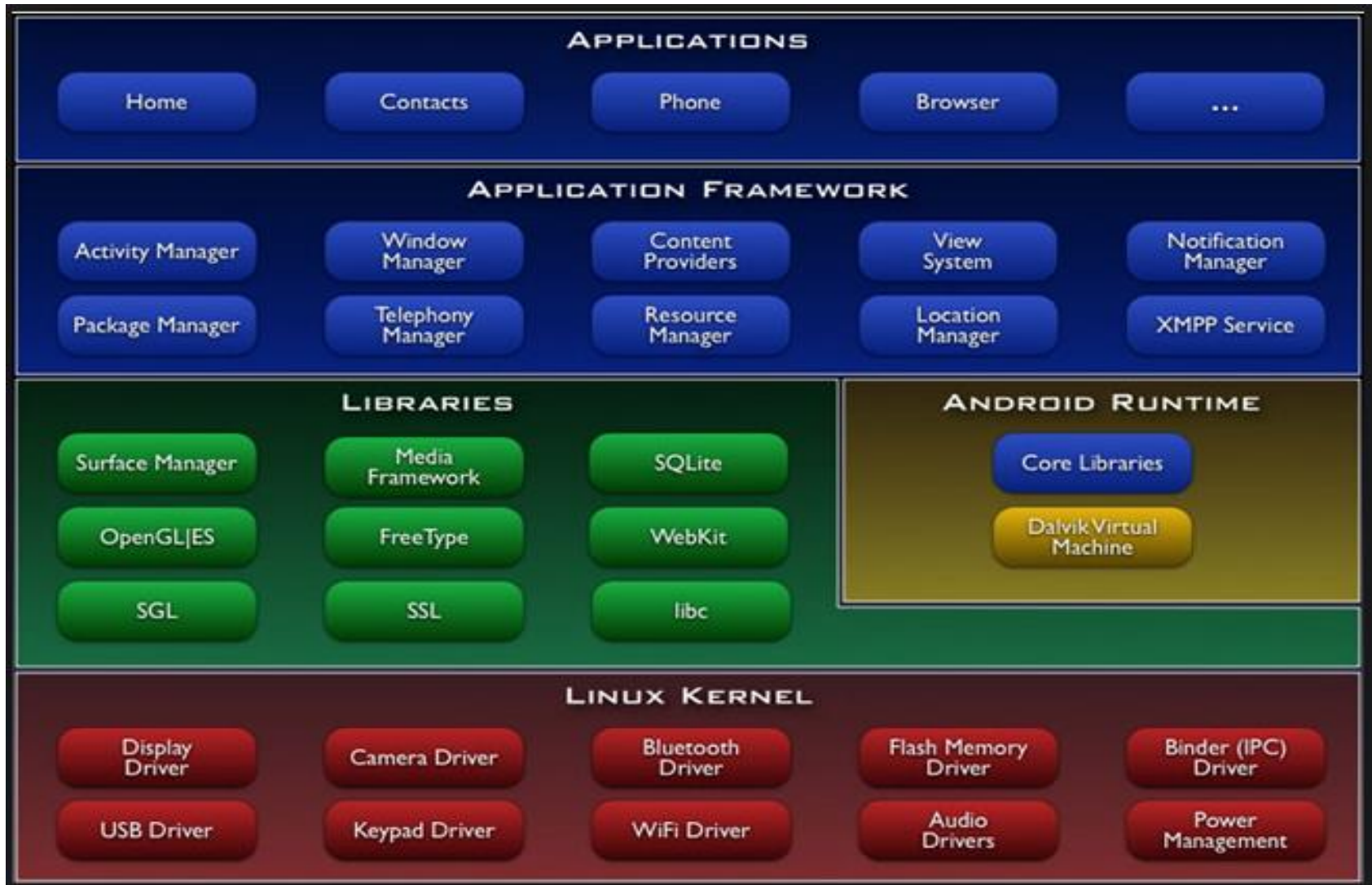
二、Android的安全机制

- ❖ Android的核心安全机制，包括三个方面：
 - 程序沙箱
 - 应用签名
 - 权限机制

2.1 程序沙箱



Android系统结构



Delvik虚拟机

- ❖ Android应用程序采用Java开发，但其并不是运行在Java虚拟机上。原因：
 - 解决移动设备上软件运行效率问题；
 - 规避与Oracle公司的版权问题。
- ❖ Dalvik虚拟机
 - 采用DEX格式的可执行文件，体积更小，执行速度更快；
 - 基于寄存器架构，拥有一套完整的指令系统；
 - 每个Android进程对应一个Dalvik虚拟机实例。

Dalvik虚拟机与JVM比较

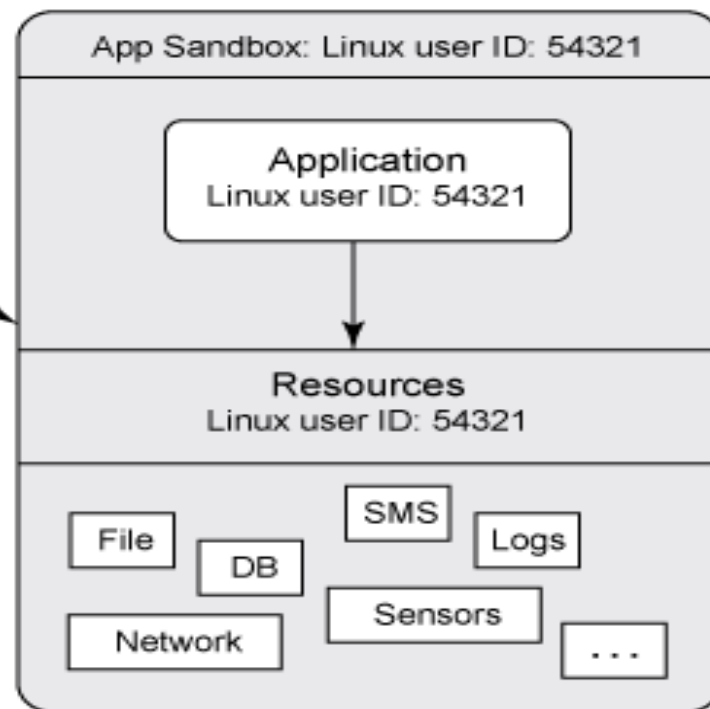
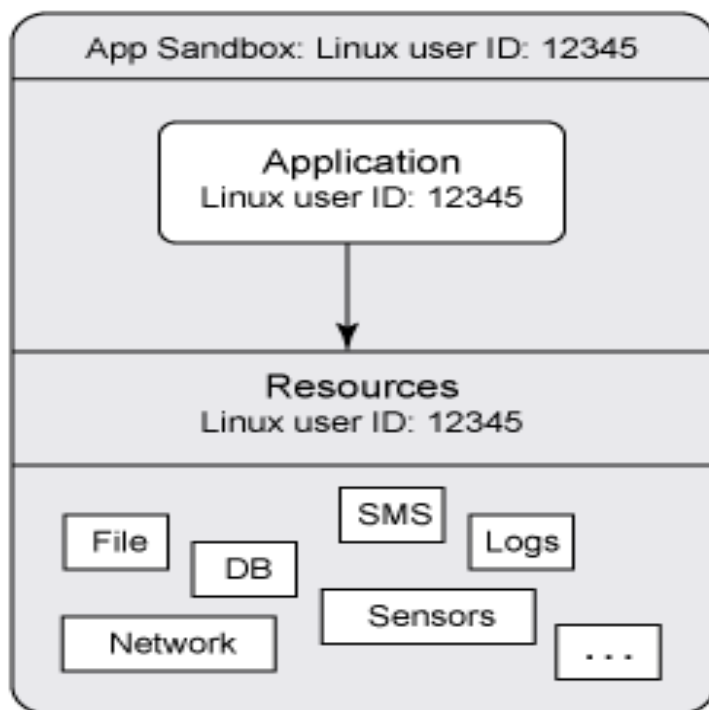
- ❖ (1) 运行的字节码不同
 - JVM运行保存在class文件中的JAVA字节码;
 - Dalvik运行保存在DEX文件中的Dalvik字节码, 该字节码由Java字节码转换而来 (DX工具)。
- ❖ (2) Dalvik可执行文件体积更小
 - 类间引用, 导致类中方法签名信息在不同类间冗余存放;
 - 类间引用, 使得Java字节码中大量的常量字符串在不同类中冗余存放。

Dalvik虚拟机与JVM比较

- ❖ (3) JVM与Dalvik虚拟机架构不同
 - JVM基于**栈架构**，虚拟机需要频繁从栈上读取和写入数据，耗费CPU开销较大；
 - Dalvik虚拟机基于**寄存器架构**，数据访问通过寄存器间直接传递，效率更高。
 - Dalvik的指令类似“op vAAAA,vBBBB”，寄存器的取值范围是v0 ~ v65535。

Android沙箱模型

Android application/process space



Two applications on different processes (with different user-ids)

<http://CEnriqueOrtiz.com>

2.2 应用签名

- ❖ `java -jar signapk.jar testkey.x509.pem testkey.pk8 update.apk update_signed.apk`
- ❖ 通过signapk.jar这个可执行jar包，以“testkey.x509.pem”这个公钥文件和“testkey.pk8”这个私钥文件对“update.apk”进行签名，签名后的文件为“update_signed.apk”。
- ❖ 签名好的APK包中增加1个META-INF的文件夹，内有3个文件，MANIFEST.MF、CERT.SF和CERT.RSA。

SignAPK原理

- ❖ 1、生成MANIFEST.MF文件
 - 程序遍历APK包中的所有文件，对非文件夹非签名文件的文件，逐个生成SHA1的数字签名信息，再用Base64进行编码。
- ❖ 2、生成CERT.SF文件
 - 对前一步生成的Manifest，使用SHA1-RSA算法，用私钥进行签名。
- ❖ 3、生成CERT.RSA文件
 - CERT.RSA文件中保存了公钥、所采用的加密算法等信息。

签名检查机制

- ❖ 签名是防止软件破解、防软件重编译重要方法。
- ❖ Android的签名检查机制
 - 软件在发布时需要开发人员对其进行签名，签名使用的密钥文件是开发人员独有的；
 - 软件运行时，若发现运行时的签名和发布时的不同，说明软件被篡改过，软件终止执行。
 - 应用的签名可以放在本地作为本地的字符串资源或是放在网络上，运行时动态校验。

❖ 演示

2.3 权限机制

- ❖ 权限控制是Android的基础安全措施;
- ❖ 程序需要申请特定的权限才能进行特定的操作, 如打电话、发短信等。否则, 程序会抛出 SecurityException 异常。
- ❖ 申请权限, 只需要在程序的AndroidManifest.xml 文件中添加相应的权限代码即可。例如发短信:

```
<uses-permission android:name="android.permission.SEND_SMS">
```
- ❖ 总的思路是: 应用的开发者在AndroidManifest.xml 中显示的申明该应用需要哪些权限。应用在安装时明确提示用户该应用需要哪些权限, 安装完成后不可更改。

Android Platform的权限分类

- ❖ Android平台为第三方开发者提供了一个丰富的API接口，其中涉及的权限数不断增加。

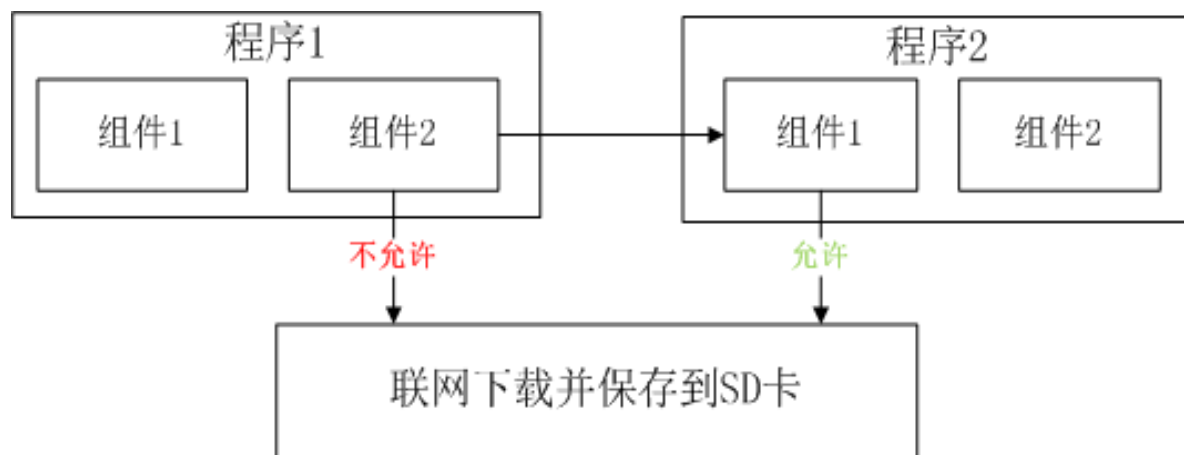
API level	Android platform	SDK codename	Total permissions	Release (mm-dd-yy)
15	4.0.3	Ice Cream Sandwich MR1	165	12-16-11
14	4.0.2 4.0.1	Ice Cream Sandwich	162	11-28-11 10-19-11
10	2.3.4 2.3.3	Gingerbread MR1	137	04-28-11 02-09-11
9	2.3.2 2.3.1 2.3	Gingerbread	137	12-06-10
8	2.2.x	Froyo	134	05-20-10
7	2.1.x	Eclair MR1	122	01-12-10
6	2.0.1	Eclair 0 1	122	12-03-09
5	2.0	Eclair	122	10-26-09
4	1.6	Donut	106	09-15-09
3	1.5	Cupcake	103	04-30-09

Android权限机制存在的问题

- ❖ 属于**粗粒度**的安全控制，存在的安全风险包括：
 - 赋予程序访问隐私数据权限的负担，转嫁到没有安全意识的用户头上，一旦授权后对隐私数据的访问将不受控制，Android也不会通知用户；
 - Android缺乏应对权限攻击的有效机制；
- ❖ 权限提升攻击包括：
 - 非授权应用可以利用其它程序的漏洞间接获得隐私数据；
 - 攻击者可以组合多个已感染的或恶意程序形成串谋攻击；

权限串谋攻击

- ❖ 程序1本身无任何权限，它的组件2想要“联网并下载文件并保存到SD卡”，正常情况不被允许。
- ❖ 程序2的组件1拥有该权限。此时程序1的组件2可以通过访问程序2的组件1来实现文件的下载，突破Android系统的权限控制机制。



串谋攻击的防范

- ❖ 串谋攻击是由不安全的编码造成的。
- ❖ 原因是上例中程序2的文件下载功能是通过接收下载请求广播，然后在下载广播接收者中完成。
- ❖ 恶意的程序1，通过发送下载请求，而程序2直接接受下载请求进行下载。而实际上，程序1没有任何下载的访问权限。
- ❖ **根本原因：**程序2的DownloadReceiver广播接收者不需要任何权限就可以调用。
- ❖ **防范措施：**可以使用Android平台的安全评估工具Mercury，进行组件权限提升漏洞检测。

权限攻击检测工具--Mercury

The screenshot shows the GitHub repository page for `mwrlabs/mercury`. The browser address bar shows the URL `https://github.com/mwrlabs/mercury`. The repository is public and has 96 stars and 36 forks. The main navigation bar includes links for Explore, Features, Enterprise, and Blog, along with Sign up and Sign in buttons. The repository page shows the `master` branch with 5 files, 5 commits, and 12 issues. The commit history is displayed, showing the latest commit by `dbradberry` 2 months ago, which fixes a small typo in the intent help topic. The commit message is "fixing a small typo in the intent help topic". The commit hash is `d2c6a7c46a`. The commit history table lists the following commits:

File	Time	Commit Message
bin	2 months ago	remove an unnecessary variable, process, that was generated [dbradberry]
src	2 months ago	fixing a small typo in the intent help topic [dbradberry]
test	3 months ago	adding a couple of unit tests for the argparse_completer [dbradberry]

■ 权限攻击演示

三、Android主要安全威胁

- ❖ 3.1 Root权限
- ❖ 3.2 数据安全
- ❖ 3.3 ROM安全
- ❖ 3.4 病毒防治
- ❖ 3.5 二维码隐患

3.1 ROOT权限

❖ 为什么用户要ROOT手机？

- 刚出厂的手机不具备ROOT权限，使用带来限制。例如，捆绑了一些“垃圾软件”，无法删除；
- 要想获得更高的性能，个性化系统，需要自己动手修改系统，此时需要ROOT权限。

❖ 较流行的工具：刷机精灵

[首页](#)[功能介绍](#)[支持机型²](#)[常见问题](#)[商务合作](#)

支持机型



其他品牌

51

手机ROOT原理

破解/提权教程 - 三星 I9000手机论坛_提供三星 I9000 Galaxy S 评测,教程,刷机rom,软件游戏下载_安卓论坛 - Powered by Discuz! - Mozilla Firefox

文件(F) 编辑(E) 查看(V) 历史(S) 书签(B) 工具(T) 帮助(H)

Root 权限提权 视频 - Google 搜索 x 破解/提权教程 - 三星 I9000手机论... x +

bbs.hiapk.com/forum.php?mod=forumdisplay&fid=218&filter=typeid&typeid=1074 百度 <Ctrl+K>

火狐官方网站 访问最多 新手上路 常用网址

安卓首页 资讯 挖客 教程 刷机 手机 手机大全 乐翻 动漫 | 安卓市场 游戏 软件 壁纸 铃声 主题 | 安卓论坛 切换到窄版

推荐主题

[三星 Samsung Galaxy S GT-I9000 Odin刷机教程 \(图+视频\)](#) i9000—键root 最快捷

发帖 返回

全部 刷机教程 ROM 制作/修改 教程 **破解/提权教程** APP TO SD 教程

筛选: 全部主题 全部时间 排序: 最后发表 | 精华 | 最新发帖

	新窗	作者	回复/查看	最后发表
[破解/提权教程] 三星I9000获取root权限及完美刷机教程,全程视频操作,新手不可错过,申请加精 ... 2 3 4 5 6 .. 59		sdher 2013-2-14	586 5860	13532712335@qq.com 昨天 01:07
[破解/提权教程] 港行原生2.2 ROOT问题解决了!!! ... 2 3 4 5 6 .. 51		leslie73522@163.com 2010-12-4	501 24843	wenchan 4 天前
[破解/提权教程] i9000一键ROOT本人亲测 ... 2 3 4 5 6 .. 155		www.403974391@qq.com 2011-5-8	1548 61885	alanlee8 4 天前
[破解/提权教程] 精编三星i9000锁三键版去除锁3e的方法		游戏江湖行 2013-4-12	9 759	54% 0K/S 0K/S
[破解/提权教程] i9000获取root权限 (傻瓜式) ... 2 3 4 5 6 .. 430		nikker 2010-6-29	4298 334783	chgho12 2013-5-25 14:52
[破解/提权教程] 求高手啊,		solotp 2013-4-20	0 84	solotp 2013-4-20 02:17:54
[破解/提权教程] I9000 一键root成功 ... 2 3 4		13822010999@139.com 2011-10-26	34 11460	爱我中华110 2013-4-15 08:21:04
[破解/提权教程] i9000一键root 最快捷 ... 2 3 4 5 6 .. 68		zhengqun 2010-12-16	670 39401	simery 2013-2-25 21:21:16

8:21 2013-06-07

手机ROOT原理（续）

- ❖ 采用 “一键ROOT” 工具，选择永久ROOT后：
 - 1、向手机系统的/system/app目录下写入ROOT权限管理软件（如superuser.apk）；
 - 2、向/system/bin或/system/xbin目录写入su程序；
 - 3、su程序与superuser.apk合作，对系统进行Root权限管理。

提权漏洞检测工具

❖ X-ray For Android



ROOT后的安全隐患

❖ 1、系统不稳定

- 系统删减过程中，可能误删重要文件；
- 手机ROOT后，将不再保修！！

❖ 2、病毒侵入

- 手机ROOT后，所有软件都能获得ROOT权限；
- 虽然可以使用权限控制软件，但用户一般无从判断软件获取ROOT权限的用途，一般选择放行。

❖ 3、隐私数据暴露

- 非ROOT手机，应用安装后，有属于自己的程序目录，其他用户与软件没有访问权限；
- ROOT后，所有数据都暴露，聊天记录、网银账号等。

三、Android主要安全威胁

- ❖ 3.1 Root权限
- ❖ **3.2 数据安全**
- ❖ 3.3 ROM安全
- ❖ 3.4 病毒防治
- ❖ 3.5 二维码隐患

3.2 Android数据安全

❖ Android中用户的隐私数据

- 手机号码、通信录、短信息、聊天记录、电子邮件、网络软件的帐号密码等等。

❖ Android数据安全包括：

- **数据存储安全**和**数据通信安全**

❖ Android数据存储

- 若数据存储不好，会将手机中的隐私数据暴露给系统中的所有软件。

❖ Android数据存储方式

- 外部存储和内部存储

外部存储

- ❖ Android SDK提供的一种最为简单的存储方式，是所有存储方式中安全隐患最大的，任何软件只要在AndroidManifest.xml中申请了权限就可以读写外部存储设备。

权限申明：

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

File类进行文件读写：

```
File configFile = new File("/sdcard/config.txt");
FileOutputStream os;
try {
    os = new FileOutputStream(configFile);
    os.write("I am a CIQ Virus".getBytes());
    os.close();
}catch (Exception e ){
    e.printStackTrace();
}
```

内部存储安全

- ❖ **内部存储**：是将文件保存在设备内部存储器中。默认情况下，这些文件是相应程序私有的，对其他程序不透明，对用户也是不透明的。当程序卸载后，这些文件就会被删除。
- ❖ **内部存储安全的实现**：Android系统为每个程序分配独立的用户与用户组，然后为每个用户和用户组独立的分配访问权限（Linux的文件访问权限机制）。
- ❖ Android SDK提供OpenFileInput()和OpenFileOutput()进行私有程序的读写。

内部存储安全

❖ 提供多种私有数据权限：

- MODE_PRIVATE, MODE_APPEND, MODE_WORLD_READABLE, MODE_WORLD_WRITEABLE

内部存储代码示例：

```
try {  
    FileOutputStream fos = new openFileOutput("config.txt", MODE_PRIVATE);  
    fos.write("I am a CIQ Virus".getBytes());  
    fos.close();  
} catch (Exception e) {  
    e.printStackTrace();  
}
```


❖ 使用权限错误，会导致安全隐患；

❖ 通过其他途径获得访问权限、系统漏洞提升权限、手机ROOT后恶意软件能够访问隐私数据。

Android数据通信安全

- ❖ 数据通信安全对于Android而言，包括2个方面：
 - 组件间通信安全：系统内软件间的通信；
 - 网络通信安全：软件与网络服务器间的通信安全。
- ❖ 网络通信安全
 - Android软件使用Wifi与服务器进行通信；
 - 不加密地明文传输敏感数据；
 - SSL通信不检查证书有效性；
 - 使用短信注册帐号或接收密码。

网络通信安全



[Add search to your site](#) | [Check links](#) | [Submit URL](#)

Search File!

Size: -

☐ Rapidshare ☒ Hotfile ☒ Mediafire
☒ Depositfiles ☒ Mega ☒ 4shared

Listing files for: **faceniff.apk**



Previous



Next



Display

30 files



▲ Filename	▼ Size	▲ Source
Faceniff.apk motomodtr.zip	519 KB	http://motomo...
FaceNiff-2.1b.apk	515 KB	http://adwite...
FaceNiff-2.0-beta2.apk	289 KB	http://whytov...
faceniff v2.0.apk	287 KB	http://www.ap...
FaceNiff-1.9.4-crd.apk	944 KB	http://forum....
FaceNiff-2.1b[1].apk	515 KB	http://www.yo...
FaceNiff-2.1b.apk	515 KB	http://www.yo...
FaceNiffGen[UNLOCKER].apk	17 KB	http://www.yo...
FaceNiff-2-1.1b.apk	515 KB	http://hvgaqv...
faceniff-1.9.4-unlocked.apk	944 KB	http://www.ce...
FaceNiff-2.1b.apk	515 KB	http://aplica...

使用短信注册帐号或接收密码

- ❖ 短信并不是一种安全的通信方式。
- ❖ 恶意软件只要声明了SEND_SMS、RECEIVE_SMS和READ_SMS这些权限，就可以通过系统提供的API向任意号码发送任意短信、接收指定号码发来的短信并读取其内容，甚至拦截短信。
- ❖ 这些方法已在Android恶意代码中普遍使用，甚至出现拦截并回传短信中的网银登录验证码的盗号木马Zitmo。
- ❖ Zitmo DEMO:

<http://www.youtube.com/watch?v=DCh6OJhMChw>

三、Android主要安全威胁

- ❖ 3.1 Root权限
- ❖ 3.2 数据安全
- ❖ **3.3 ROM安全**
- ❖ 3.4 病毒防治
- ❖ 3.5 二维码隐患

3.3 ROM安全

- ❖ ROM：只读存储器；
- ❖ 手机ROM：存放手机**固件**代码的存储器，俗称手机“系统”；
- ❖ 固件：firmware，固化的软件，是指将某个系统程序写入到特定硬件系统中的FlashROM（快速擦写只读编程器，闪存）的过程。
- ❖ ROM种类
 - 官方ROM
 - 第三方ROM
 - 民间个人版ROM



孰优孰劣

❖ 官方ROM

- 手机出厂时被刷入的ROM;
- 通常被认为：“官方的，总是最好的”？
 - 手机硬件质量如何，暂且不论；
 - 官方ROM里有太多软件开发商和手机厂商合作植入的大量“垃圾”软件，这些软件属于系统程序，普通用户无法卸载，只能ROOT手机来删除它们，手机ROOT后，风险增加；

第三方ROM

- ❖ 第三方ROM制作团队或厂商制作的ROM;
- ❖ 影响力较大的要数CyanogenMod团队;



民间个人版ROM

- ❖ 个人在官方或第三方ROM基础上修改而成的；
- ❖ 国内的现象是：民间的个人版ROM比第三方ROM更受追捧，存在巨大的安全风险，往往给用户带来巨大的经济损失。
- ❖ 很多人不买“国行”，购买“日行”、“港行”，然后自己选择“中意”的ROM来刷机，存在诸多问题。

ROM的制作过程

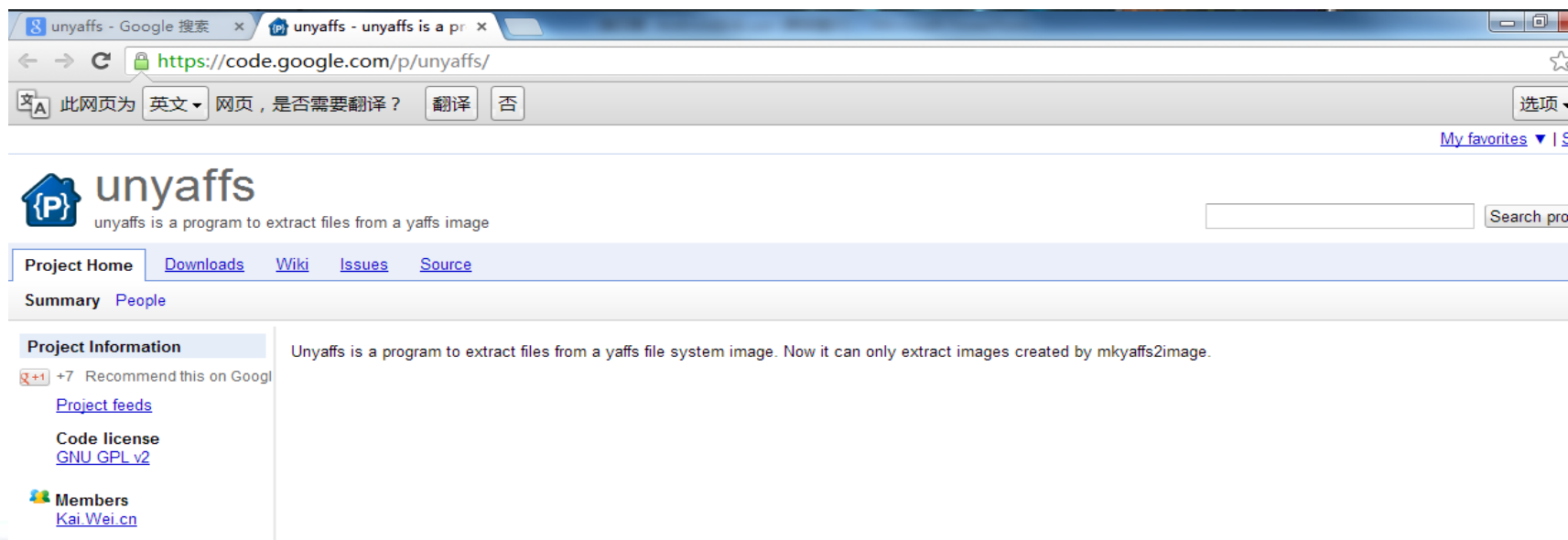
- ❖ 两种途径：基于Android源码和基于官方的ROM改造。
- ❖ 基于源码：
 - 缺少与手机硬件相关的驱动；
 - 驱动是手机厂商的秘密，不开源；
- ❖ **CM团队的做法：**基于源码与官方ROM提供的驱动结合起来加以改造。
- ❖ **国内的通行做法：**在CM提供的开源的ROM基础上进行二次开发。
- ❖ **个人版ROM：**在现有的ROM基础上进行微调。

个人版ROM的加工过程

❖ ROM**解包**、ROM**修改**、ROM**打包**三步。

❖ ROM解包依据刷机方式不同：

- 线刷：通过USB线连接电脑，通过电脑的刷机软件进行刷机。一般是官方采用的刷机方式，需要单独的刷机工具，包格式为sdf格式文件。



ROM修改

❖ 线刷包的修改：

- 多数手机厂商的线刷包都是自定义的文件格式，需要经过相应的解包工具提取其中的内容进行修改。
- 优化版的ROM修改：
 - 手机基带、Wi-Fi驱动、摄像头驱动、DSP音效增强、系统主题增强、隐私保护增强等，对技术要求较高。
- 美化版的ROM修改：
 - 主要是修改framework-res.apk里面的资源文件，UI图标、桌面背景、界面文字等。

ROM修改

❖ 卡刷包的修改

- 卡刷包中的任何一个单独文件都可以提取出来进行修改，针对CM卡刷包的加工，可以直接进行源码级的修改。
- 相比线刷包增加一道工序，编写刷机脚本。该脚本功能是：格式化系统、拷贝文件、设置权限等。

```
01. META-INF\com\google\android\updater-script
复制代码
```

刷机过程其实很简单，只要你理解了流程，和相关的语句。
一般来说，刷机就是如下的步骤：

```
01. 开始。
02. 清理userdata, system, cache, dalvik-cache等（这是一个可选的步骤，由ROM作者依据ROM的特性去决定是否要采用）
03. 挂载userdata, system, sdext（其中sdext为可选挂载，依据ROM特性决定）
04. 释放对应的文件/文件夹到对应的区域，例如刷机包内的目录data对应的释放到手机的userdata区域
05. Symlink，这个是必须的动作，这个有问题，会导致ROM出现一些问题，特别是错误的链接或者不存在的链接，很容易引发问题。
06. 设置权限，这一个步骤也很重要，关系到ROM能否正常使用，Android是base在linux基础上的，对于文件的权限非常重要，没有权限，一个应用程序是无法被执行或者读写
07. 刷入内核引导文件boot.img
08. 取消挂载的各个分区，刷机结束。
复制代码
```

ROM打包

- ❖ 打包修改后的文件为刷机包。
- ❖ 卡刷包的做法是：
 - 将修改后的系统文件做成yaffs镜像；
 - 例如： `./mkyaffs2image system system.img`
 - 然后，使用特定厂商ROM的工具进行打包；
- ❖ 线刷包的做法更为简单：通过解压缩工具导入线刷包里面的文件。
- ❖ 签名：
 - 线刷包：使用特定厂商ROM的工具进行签名；
 - 卡刷包：与apk签名一样，使用signapk.jar即可。

ROM的安全隐患

❖ ROM病毒：CIQ病毒（收集用户隐私）

- CIQ软件是美国硅谷企业CarrierIQ公司旗下的一款手机软件产品，它被应用在苹果、三星、诺基亚、黑莓、等众多手机厂商、电信运营商的手机中，是能够识别手机掉线，电池问题等问题的软件，并且预测移动网络可能出现的问题。
- CIQ曾在全球掀起了一股“涉密丑闻”的风暴。包括苹果、HTC、三星、
、Sprint、T-Mobile等



com.android.providers.user

4.00KB



com.carrieriq.iqagent

0.00B



Contacts Storage

492KB

ROM的安全隐患

❖ 民间版ROM的黑色产业链

- 成为广告软件和非法服务提供商SP生存的一个寄宿点；
- 初级做法：在ROM中植入广告软件后，使用论坛活动或其他方式诱骗用户使用；
- 高级做法：在ROM中更改系统源码、修改系统组件、添加恶意软件，如修改电话与短信模块，直接在系统底层进行非法暗扣短信。

ROM安全防衛

❖ 尽量使用官方的ROM

- 使用对Android源码支持较好的手机，如Google自己的手机；

❖ 使用权威机构的ROM

- 质量和安全上有保证；

❖ 使用自己的ROM

- 自己动手，丰衣足食。

三、Android主要安全威胁

- ❖ 3.1 Root权限
- ❖ 3.2 数据安全
- ❖ 3.3 ROM安全
- ❖ **3.4 病毒防治**
- ❖ 3.5 二维码隐患

3.4 Android病毒防治

- ❖ 1、不要轻易ROOT自己的手机
 - 手机ROOT权限后，用户拥有系统绝对的控制权；
 - 手机中的所有数据都是暴露的，任何程序都可以访问系统中的所有数据；
- ❖ 2、到正规的应用商店下载软件
 - 国内的软件市场有上百家，质量参差不齐，恶意程序充斥其中。
 - 建议先到Google Play商店，再搜软件的官方网站，再到国内知名度较高的Android市场下载。

Android病毒防治（续）

❖ 3、安装软件留心眼

- 安装时会显示将要安装软件使用到的权限，部分权限和手机扣费相关；
- 例如，下载一个阅读软件，却需要一个短信发送权限，有些不合理，需要谨慎。要么放弃安装，要不上传到在线的沙盒中测试一下。或者反编译，看是否有恶意发送扣费短信的行为。

❖ 4、安装防毒软件

- 对未知病毒查杀能力有限，但大部分查杀已知病毒还不错；有些也可以对敏感数据的访问，提供预警。
- 如果手机ROOT过了，安装带主动防御功能防毒软件。

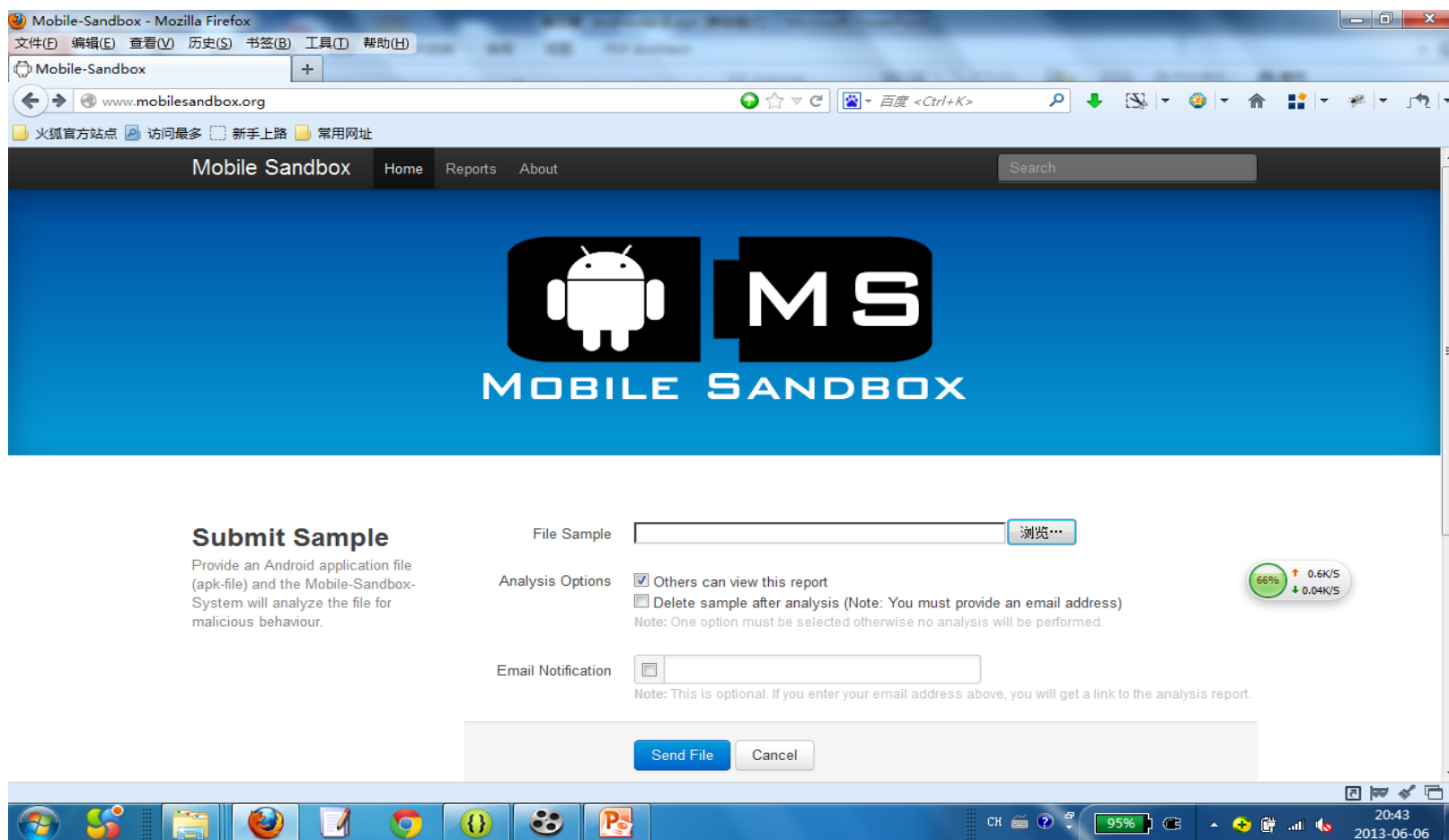
中关村在线ZOL杀毒软件测评

名次	产品外观	病毒查杀	扫描速度	内存占用	CPU、线程占用	拦截测试	总分
1、大蜘蛛	19	17.2	9	10	18.5	20	93.7
2、诺顿	16	18.8	8.5	9.5	19	20	91.8
3、瑞星	17	18.4	7.5	9	19	20	90.9
4、ESET	17	18.4	9.5	8.5	15.5	20	88.9
5、QQ	19	18	6	6	16.5	20	85.5
6、金山	19	18	7	7	14	20	85
7、趋势	19	14.4	8	7	15.5	20	83.9
8、360	19	14.4	10	5.5	12.5	20	81.4
9、网秦	20	18	5.5	7.5	15	14	80
10、AVG	17	16.8	6.5	6.5	15	14	75.8

在线沙盒

❖ <http://mobilesandbox.org>

[返回](#)



三、Android主要安全威胁

- ❖ 3.1 Root权限
- ❖ 3.2 数据安全
- ❖ 3.3 ROM安全
- ❖ 3.4 病毒防治
- ❖ **3.5 二维码隐患**

3.5 手机二维码

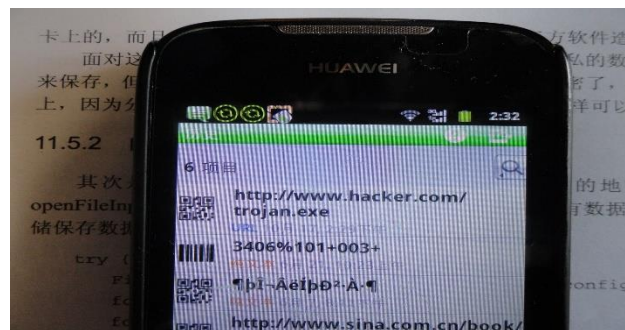
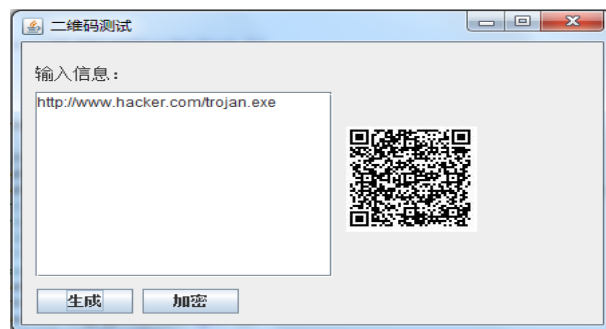
❖ 典型案例：

- “小王”上个月在网上看到一个半价销售家电的二维码信息，于是对二维码进行了扫描，扫描后跳出一个软件安装的界面，于是随手就点击了“安装”，到这个月交费时发现话费比平时超出了两倍，查询后得知手机被绑定了扣费软件。

❖ 二维码制作简单，内容缺少监管。

❖ 二维码是一个入口，本身不带毒。但是借助二维码传播钓鱼网站、发布手机病毒等。

❖ 演示



二维码威胁防范



- ❖ 1、不盲目扫描来历不明的二维码；
- ❖ 2、通过二维码链接来安装软件，装好后应先用杀毒软件杀毒后再运行；
- ❖ 3、手机二维码在线购物，支付要谨慎，要看清网站域名，不轻易点击反复弹出的小窗口页面；
- ❖ 4、若手机和银行卡绑定，卡内不要存大额现金。
- ❖ 5、使用“二维码检测工具”
 - 自动检测二维码中是否包含恶意网站、手机木马或恶意软件的下载链接等安全威胁。
 - 有些二维码扫描软件本身可以完成检测。

快拍二维码软件

- ❖ 能够通过腾讯手机管家的恶意网址库及安全网址库来检查链接的安全性。



谢谢！

