移动互联网安全

----问题与对策

杨泽明 副研究员
中科院高能所网络安全实验室
yangzm@ihep.ac.cn
13021179127

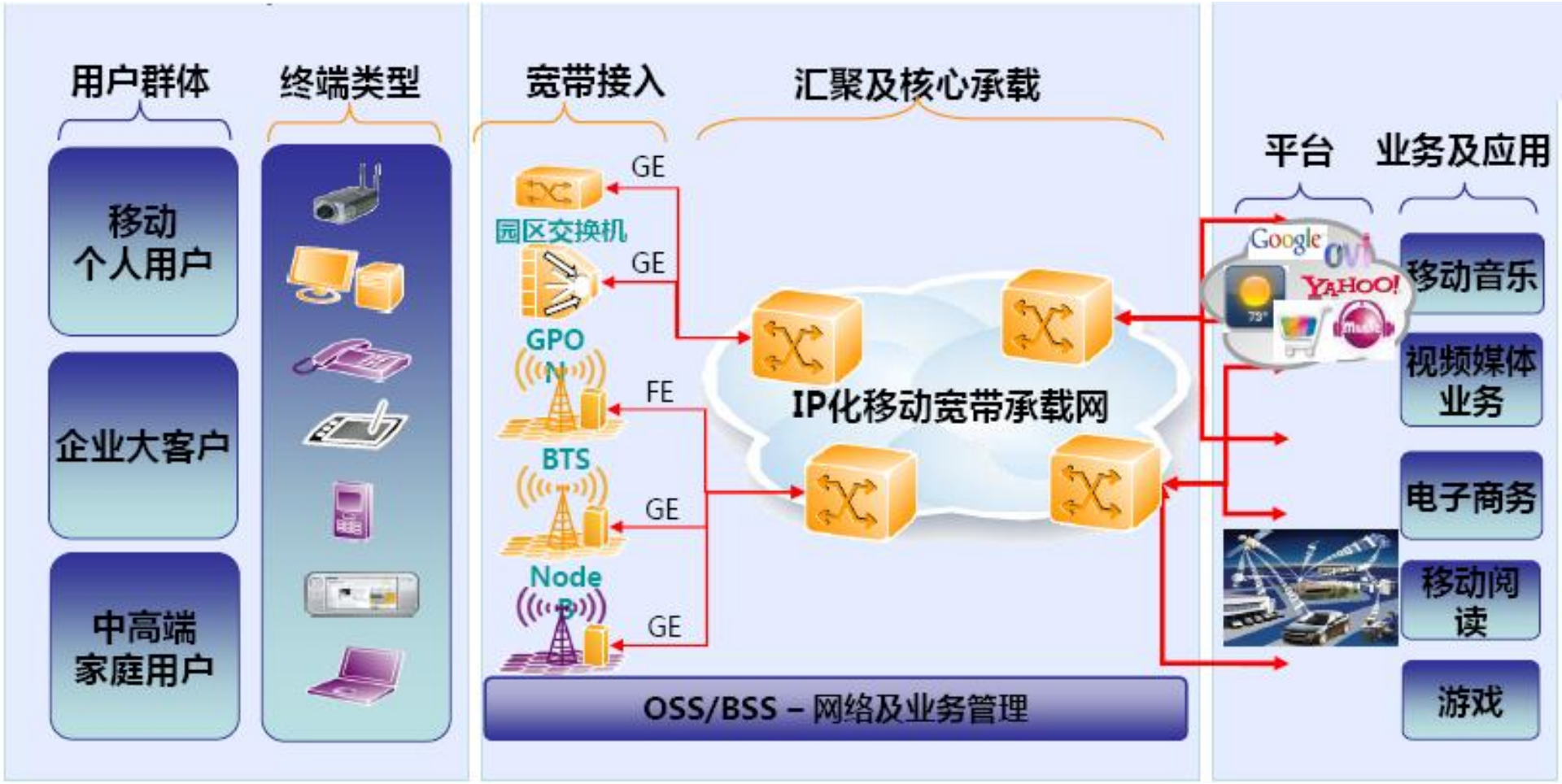
2012年4月6日

目 录

- 移动互联网安全形势
- 移动互联网安全分析
- 移动智能终端安全技术
- 移动智能终端安全工具

移动 互联网概念

❖基于移动通信技术，广域网、局域网及各种移动信息终端按照一定的通讯协议组成的互联网络



移动 互联网特点

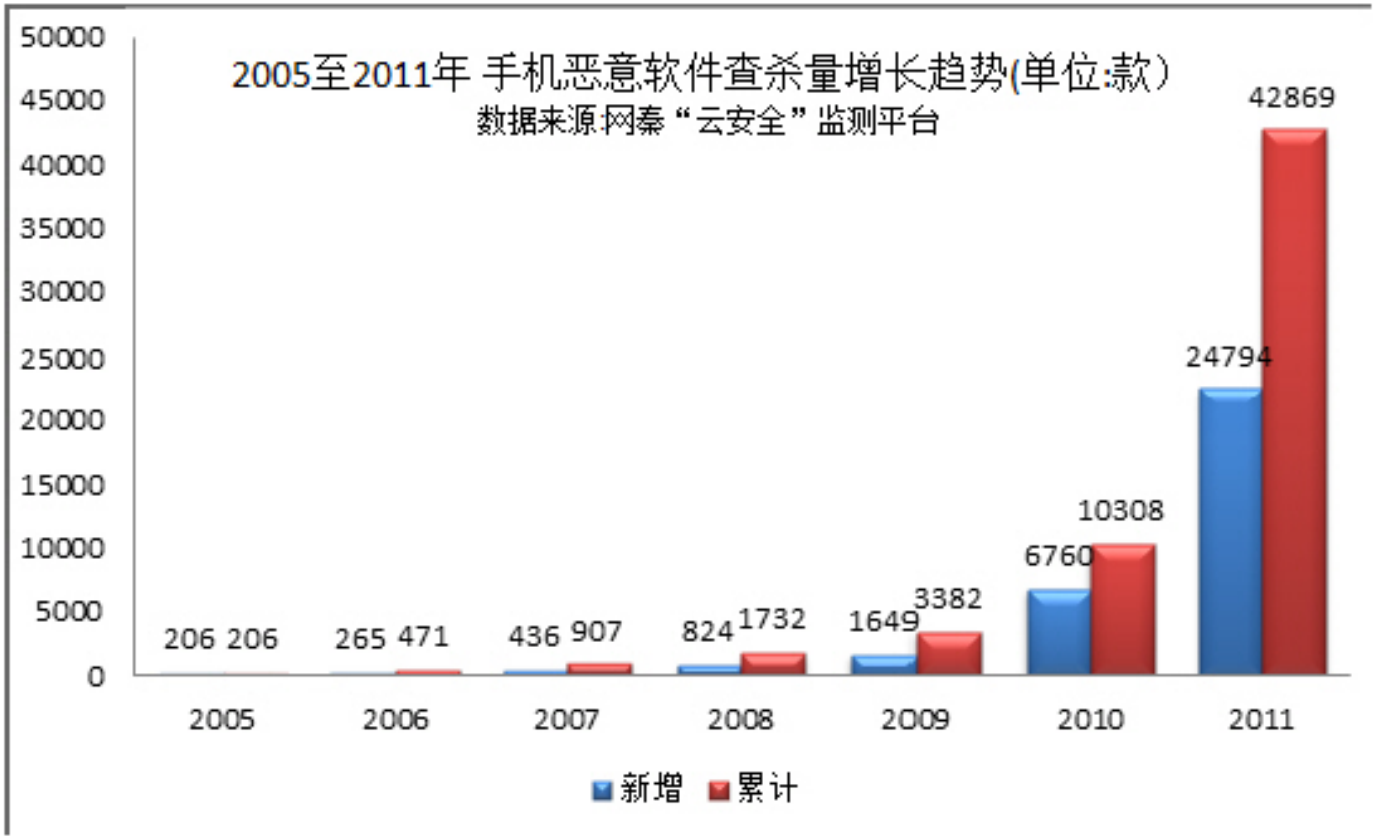
- 具有终端智能化、网络IP化、业务多元化的特点
- 移动智能终端（智能手机和平板电脑）的出现，改变了行业生态
  - 智能手机把通信行业、媒体和互联网行业自然整合在一起
  - 平板电脑把PC、媒体和互联网整合在一起
- 最明显的特点在于终端的移动性和业务的个性化
- 用户安全防范水平降低

黑色产业链伸向移动互联网

黑客的攻击目标进一步扩大，延伸到移动互联网领域

移动互联网的特性决定了在其之上的威胁更要远甚于传统的互联网

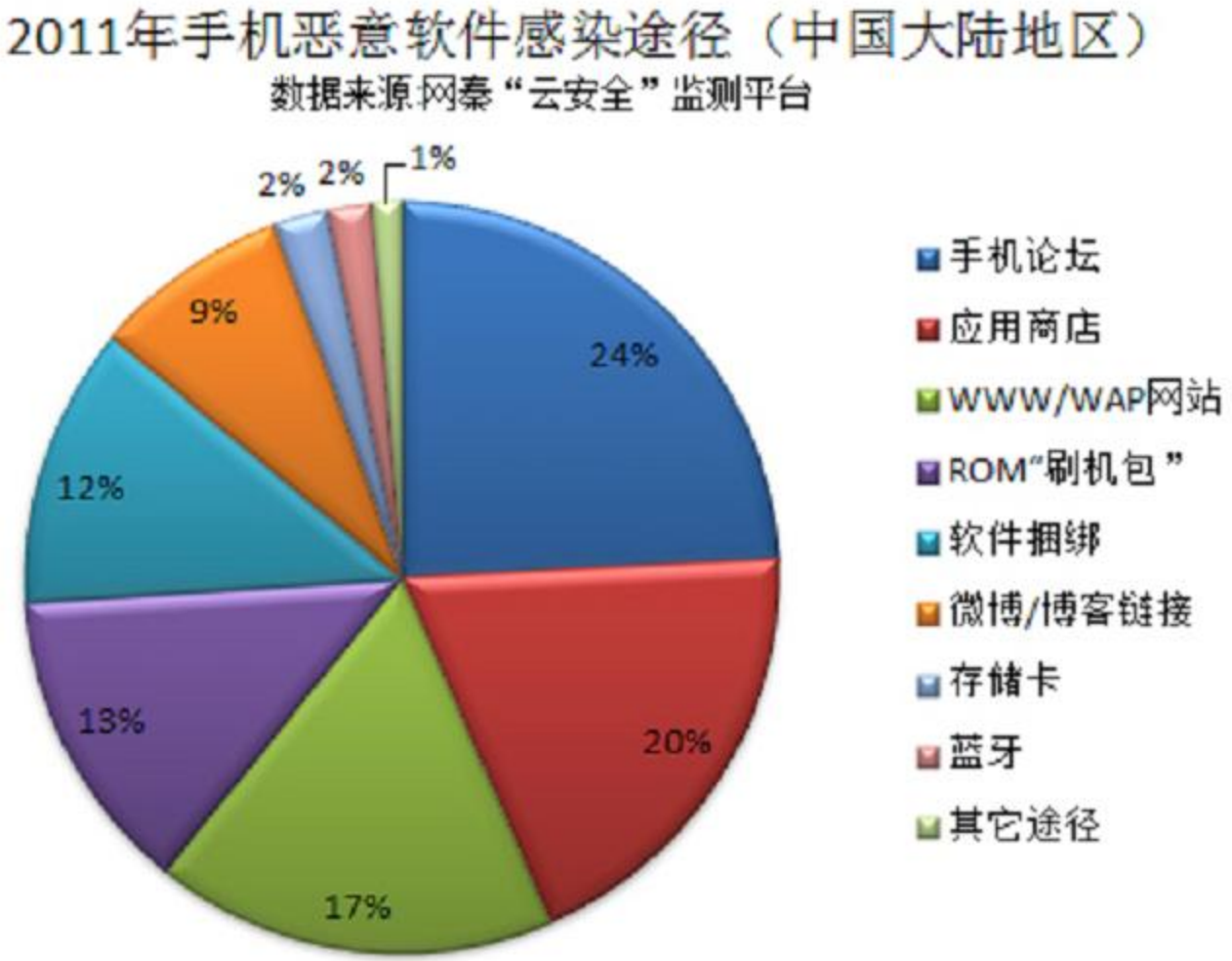
手机恶意软件呈现爆炸式增长



2005 至 2011 手机恶意软件增长趋势（数据:网秦“云安全”监测平台）

截至2011 年12 月，网秦“云安全”监测平台新增手机病毒2943 个，同比增长14.4%
全年查杀到手机恶意软件24794 款，同比增长266%，2005 年至今累计查杀42869 款
中国大陆地区2011全年累计感染智能手机1152 万部，全球范围内，累计感染智能手机3711 万部（以感染次数统计，未去重）。

手机恶意软件感染途径多种多样



2011年度十大手机病毒

- 安卓吸费王（MSO.PJApps）
- 短信窃贼（SW.Spyware）
- 短信大盗（SW.SecurePhone）
- X 卧底（Spy.Flexispy）
- 安卓窃听猫（SW.Msgspy）
- 电话吸费军团（BD.LightDD）
- 电话杀手（SW.PhoneAssis）
- 联网杀手（s.rogue.uFun）
- 跟踪隐形人（BD.TRACK）
- 阿基德锁（a.privacy.AckidBlocker）

安卓吸费王（MSO.PJApps）

一款名为“欢乐斗地主”的手机游戏
手机被强行定制了一项每月自动扣费的**SP**业务

“安卓吸费王”再度来袭 伪装**500**款热门手机应用

ZDNet 病毒防范 来源： ZDNET安全频道 2011年10月12日 评论(11)

关键词： 手机安全 手机吸费 Android吸费

APP的捞钱术 “安卓吸费王”单月吸费超百万元

时间：2012-02-08 09:27 来源：中国消费网 • 中国消费者报 作者：岳纲举

就APP应用软件本身存在的风险和缺陷，以及各方蜂拥而入APP市场后，带来的一些不规范现象进行深入调查，抽丝剥茧，分析该市场在发展过程中遇到的问题，以及其未来的发展可能。

X 卧底


1
•手机安装Xwodi
•隐藏在系统中
5
自动通过GPRS将短信/
通话录音发回
XWODI
呼叫详单及短信详单
Xwodi服务器
7
监视者通过
WEB访问
6
通过短信网关
转发给监视者手机
2
•启动窃听器功能
•普通用户无法看到
其已经运行
3 监视者拨打被监视者电话
4 通过话音信道传回，远程监听

跟踪隐形人（BD.TRACK）

■侵入用户手机安装后无图标。

■收到指定内容短信后，后台自动开启**GPS**，窃取用户地理位置

■后台发送短信，消耗用户资费

■给用户造成经济和隐私安全的双重损失。

病毒危害

1.隐藏在后台，提供远程操控手机接口，给用户手机带来威胁。

2.后台发送短信，消耗用户资费，造成经济损失。

3.后台联网，窃取用户地理位置，泄露用户隐私。

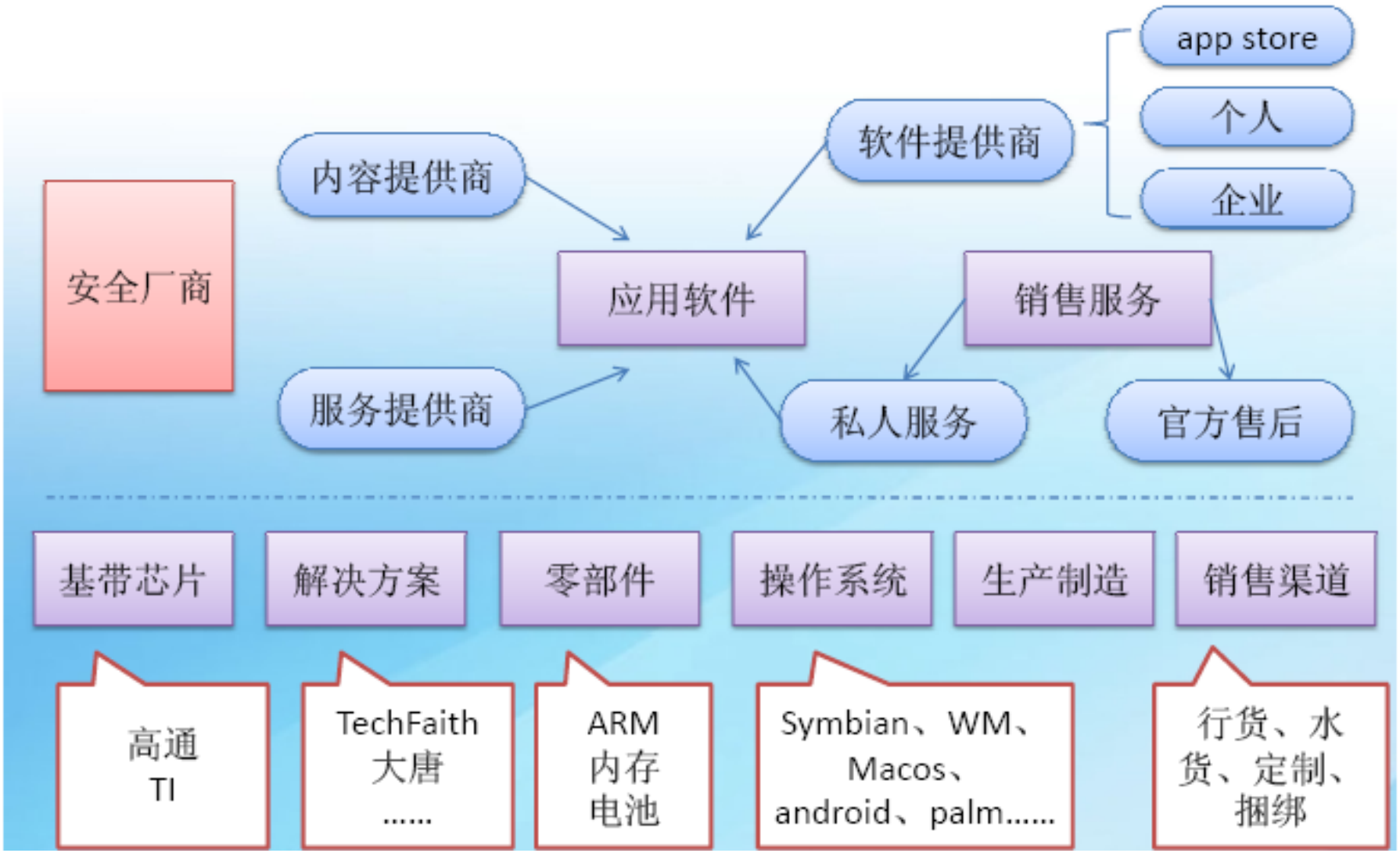
移动隐患展示

- ■木马的植入
- ■木马的隐藏
- ■位置追踪
- ■手机短信监听
- ■获取手机通讯录
- ■窃听木马手机周围环境
- ■木马手机录音
- ■遥控拨打电话
- ■遥控手机关机

目 录

- 移动互联网安全形势
- 移动互联网安全分析
- 移动智能终端安全技术
- 移动智能终端安全工具

移动互联网产业链条复杂



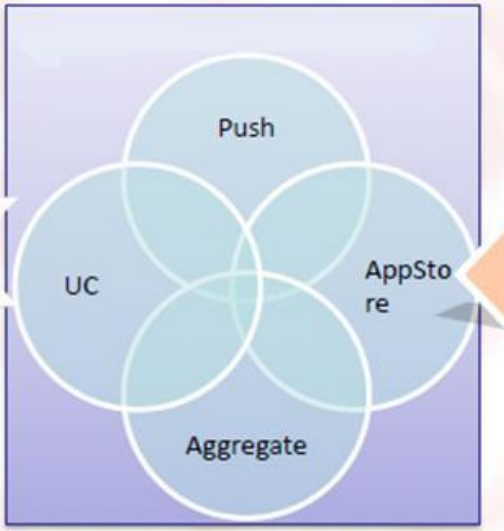
移动互联网的安全特点

	传统互联网安全	移动互联网安全
安全漏洞	传统计算机操作系统、应用程序都存在漏洞、网络设备也如此。	移动互联网的网络设备和智能手机面临同样困境，如IKEE.B是利用IPhone越狱后的sshd弱口令传播的蠕虫
恶意代码	大量的蠕虫、病毒、木门、僵尸网络程序泛滥	针对各种智能手机的病毒已经突破2000多种，并呈现激增趋势。
DDOS攻击	传统互联网僵尸网络发动的DDOS攻击防不胜防	移动互联网也出现相应的手机僵尸肉鸡，如BotSMS.A利用控制手机肉鸡发送大量的垃圾短信
钓鱼欺诈	钓鱼网站+网络木马轮番上阵，窃取网银、网游账号牟利	通过短信/彩信欺骗用户安装软件来实现恶意订购，如21CNread.A诱导用户下载欺诈软件从而订购21世纪手机报
垃圾信息	垃圾邮件常年泛滥，已经成为互联网的生态现象	垃圾短信方兴未艾，感染病毒的手机成为批量发送垃圾短信、彩信的新平台
信息窃取	大量木马在从事窃取个人隐私、敏感数据甚至国家秘密的工作	手机病毒不仅可以让手机成为窃听器，可将通话记录、短信内容、记事本内容全部偷走，效果更显著
恶意扣费	尚难以直接从终端电脑上扣费	手机天然带计费，传播会被扣费，上网也被扣费、恶意订购也被扣费，因此备受地下经济关注

移动互联网终端的安全威胁

移动智能终端

后台服务



内容提供者

- 个人隐私泄露
- 个人身份盗用
- 应用程序安全
- 位置定位
- 手机病毒

- 拒绝服务攻击
- 信息窃取

- 不良信息源
- 存在安全漏洞的业务应用

移动互联网终端的安全威胁

- 经济类危害：盗打电话（如悄悄拨打声讯电话），恶意订购SP业务，群发彩信等。
- 信用类危害：通过发送恶意信息、不良信息、诈骗信息给他人等。
- 信息类危害：个人隐私信息丢失、泄露。如通讯录、本地文件、短信、通话记录、上网记录、位置信息、日程安排、各种网络账号、银行账号和密码等。
- 设备类危害：移动终端死机、运行慢、功能失效、通讯录被破坏、删除重要文件、格式化系统、频繁自动重启等。
- 窃听：通过安装恶意软件，可以拨打静默电话，使得移动终端变成一个窃听器。
- 骚扰电话，垃圾短信。

移动互联网终端安全威胁的传播方式

- 网络下载传播：是目前最主要的传播方式。
- 蓝牙（Bluetooth）传播：蓝牙也是恶意软件的主要传播手段，如恶意软件Carbir。
- USB传播：部分智能移动终端支持USB接口，用于PC与移动终端间的数据共享。可以通过这种途径入侵移动终端。
- 闪存卡传播：闪存卡可以被用来传播恶意软件；闪存卡还可以释放PC恶意软件，进而感染用户的个人计算机，如CardTrap。
- 彩信（MMS）传播：恶意软件可以通过彩信附件形式进行传播，如Commwarrior。

移动互联网网络的安全威胁

- 移动互联网的接入方式多种多样，引入了IP互联网的所有安全威胁
- 通过破解空中接口接入协议非法访问网络，对空中接口传递信息进行监听和盗取
- 尤其是大量恶意软件程序发起拒绝服务攻击会占用移动网络资源
- 如果恶意软件感染移动终端后，强制移动终端不断地向所在通信网络发送垃圾信息，这样势必导致通信网络信息堵塞
- 接入带宽的提升加剧了有效资源的恶意利用威胁
- 信令干扰

移动互联网应用的安全威胁

- SQL注入、DDoS攻击
- 隐私敏感信息泄露
- 移动支付安全威胁
- 恶意扣费
- 业务盗用
- 业务冒名使用
- 业务滥用
- 违法信息
- 不良信息

移动互联网安全的影响

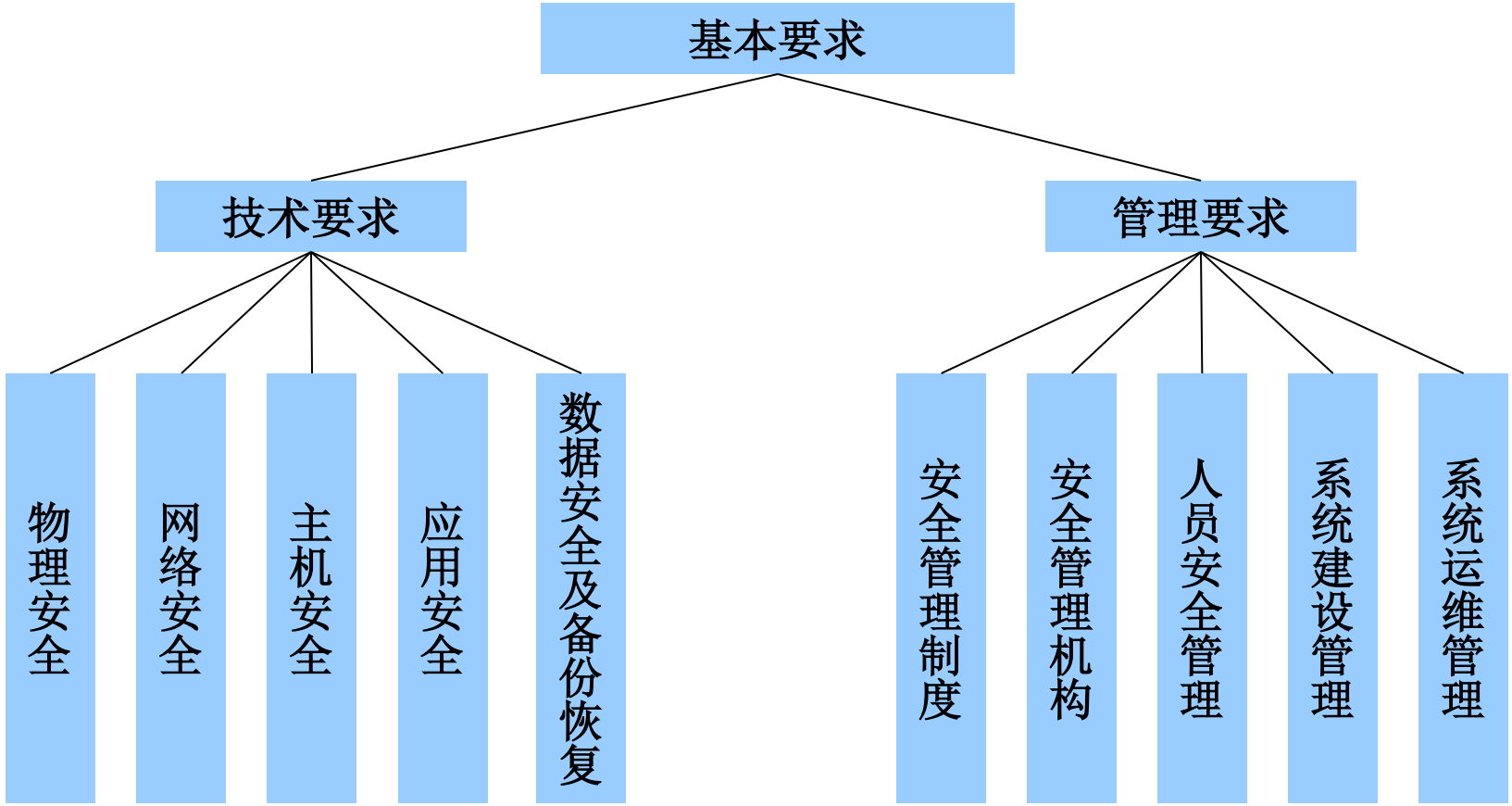
- 安全威胁将给参与移动互联网的各方造成损失
- 对于用户而言，不仅将面临着经济上的损失，还将面临着隐私泄露和通信方面的障碍
- 对于运营商而言，这些威胁不仅会让他们的业务运营成本增加，还将大大降低他们在用户心目中的好感度
- 对于终端厂商而言，售后服务成本增加，手机耗电量的上升是他们不得不面对的问题
- 内容服务商与政府主管部门同样会受得这些安全威胁的影响

移动互联网与等级保护

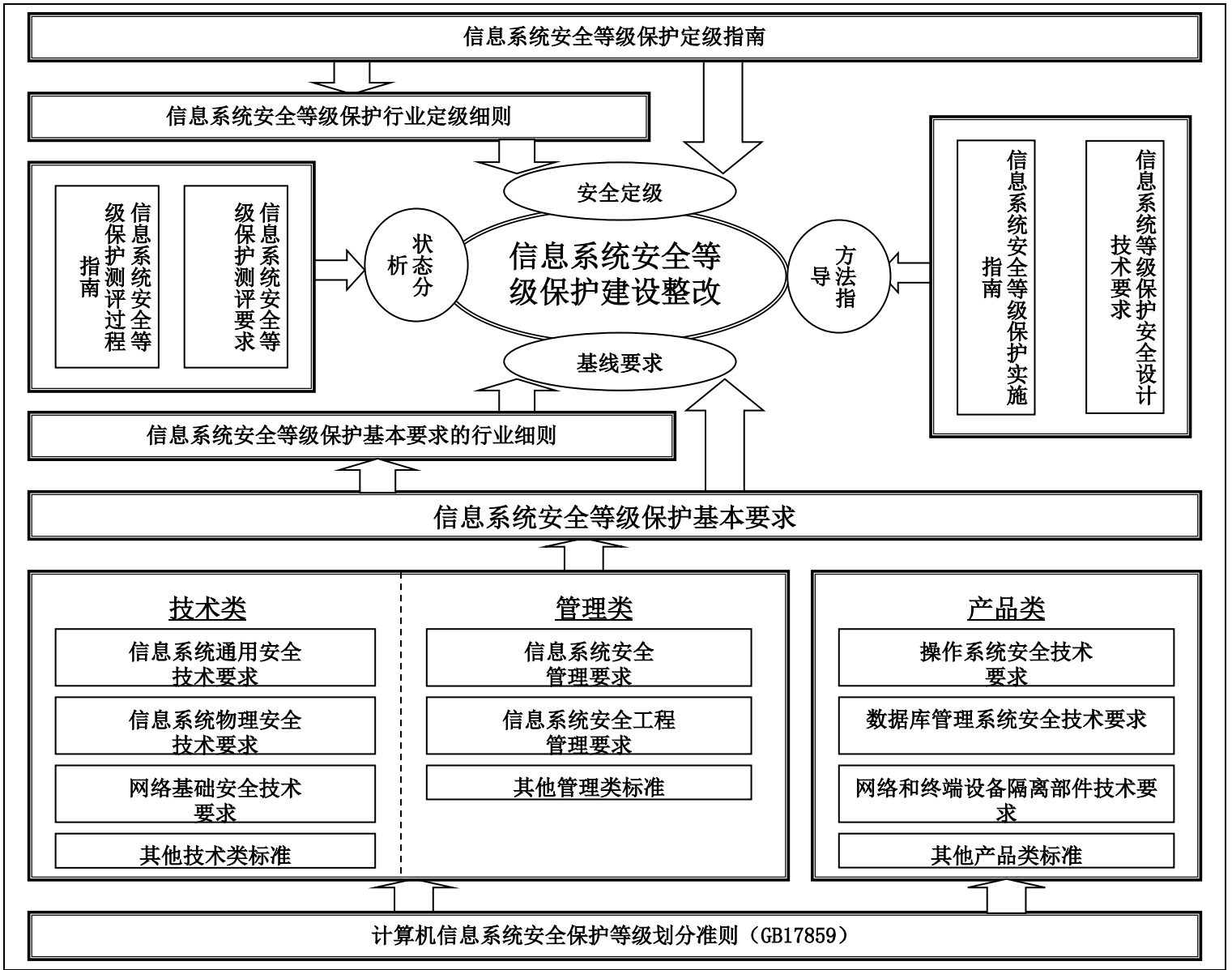
- CSDN泄密门告破：网站吃罚单 5黑客被拘
- 北京警方对CSDN网站开展全面调查，发现其未落实国家信息安全等级保护制度，安全管理制度和技术保护措施落实不到位，是造成用户信息泄漏的主要原因。市公安局于是向CSDN网运营公司提出了具体整改要求，并依据《中华人民共和国计算机信息系统安全保护条例》（中华人民共和国国务院令147号）第二十条第（一）项规定，对CSDN网站做出行政警告处罚。
- 信息安全等级保护首例“罚单”
- 自2012年1月起，北京警方对全市106家互联网网站开展信息安全检查工作，发现并现场纠正206处安全隐患，有效提高了首都互联网网站安全管理水平。

移动互联网与等级保护

根据信息系统在国家安全、经济建设、社会生活中的重要程度；遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度；将信息系统划分为不同的安全保护等级并对其实施不同的保护和监管。



移动互联网与等级保护


信息系统安全等级保护定级指南
信息系统安全等级保护行业定级细则
信息系统安全等级保护测评过程指南
信息系统安全等级保护测评要求
安全定级
状态分析
信息系统安全等级保护建设整改
方法指导
基线要求
信息系统安全等级保护实施指南
信息系统等级保护安全设计技术要求
信息系统安全等级保护基本要求的行业细则
信息系统安全等级保护基本要求
技术类
信息系统通用安全技术要求
信息系统物理安全技术要求
网络基础安全技术要求
其他技术类标准
管理类
信息系统安全管理要求
信息系统安全工程管理要求
其他管理类标准
产品类
操作系统安全技术要求
数据库管理系统安全技术要求
网络和终端设备隔离部件技术要求
其他产品类标准
计算机信息系统安全保护等级划分准则（GB17859）

信息安全管理的持续改进-ISO 27000系列

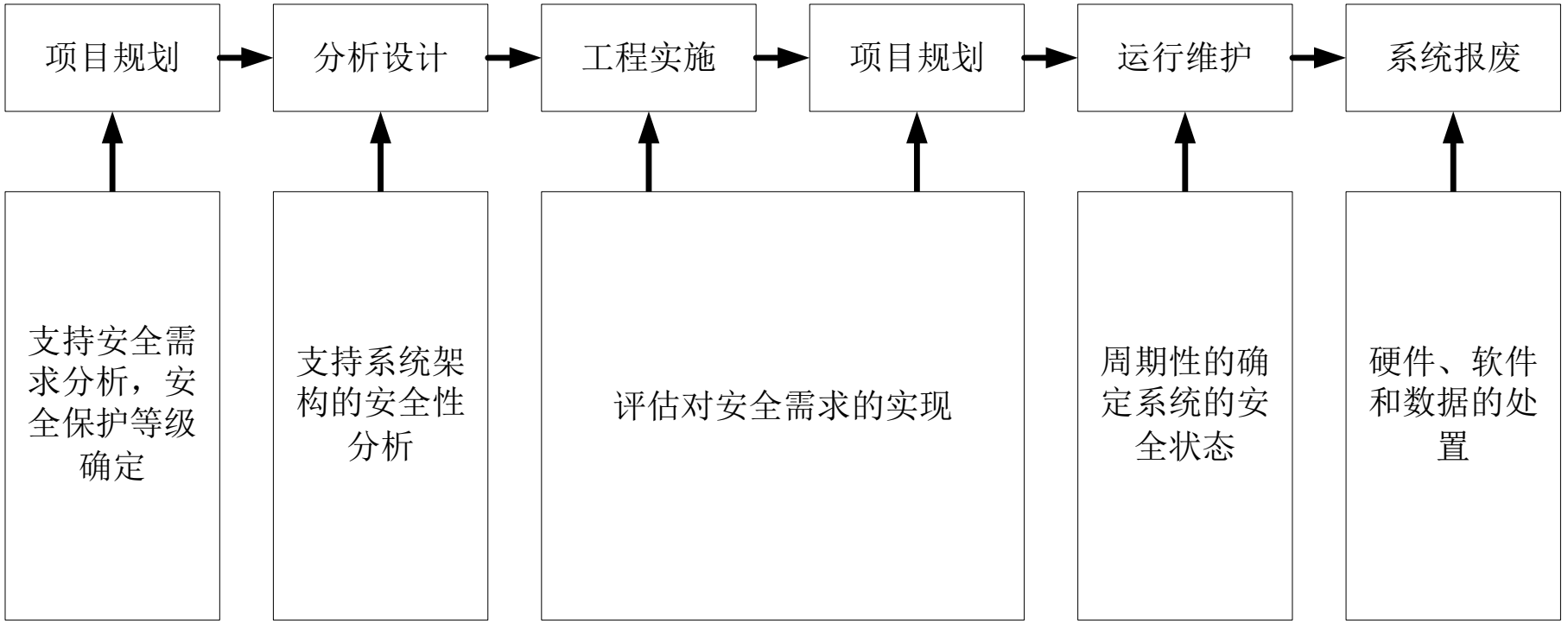
■ISMS是组织在整体或特定范围内建立信息安全方针和目标，以及完成这些目标所用方法的体系。

■它是直接管理活动的结果，表示成方针、原则、目标、方法、过程、核查表（Checklists）等要素的集合。

信息安全管理要素模型

应用于ISMS的PDCA

风险评估在移动互联网生命周期过程中的应用



移动互联网的安全监管问题

- 微博和博客大量使用
- “新的技术与社交媒体正在转变整个世界，它正在使全球转型”
- “人人都是信息源”，管理的难度和复杂性前所未有
- 部分移动智能终端采用了应用层加密技术，如RIM公司的黑莓手机
- 部分移动智能终端甚至可内嵌VPN和SSH隧道实施加密传输
- 现有传统互联网的监管技术手段难以覆盖移动互联网，缺乏针对移动互联网的有效管控平台

移动互联网的安全监管问题

Opera Mini

中国移动通信 CHINA MOBILE

中国电信 CHINA TELECOM

Mobile Market 移动应用商场

China unicom 中国联通

监督政策

尚需完善

用户服务

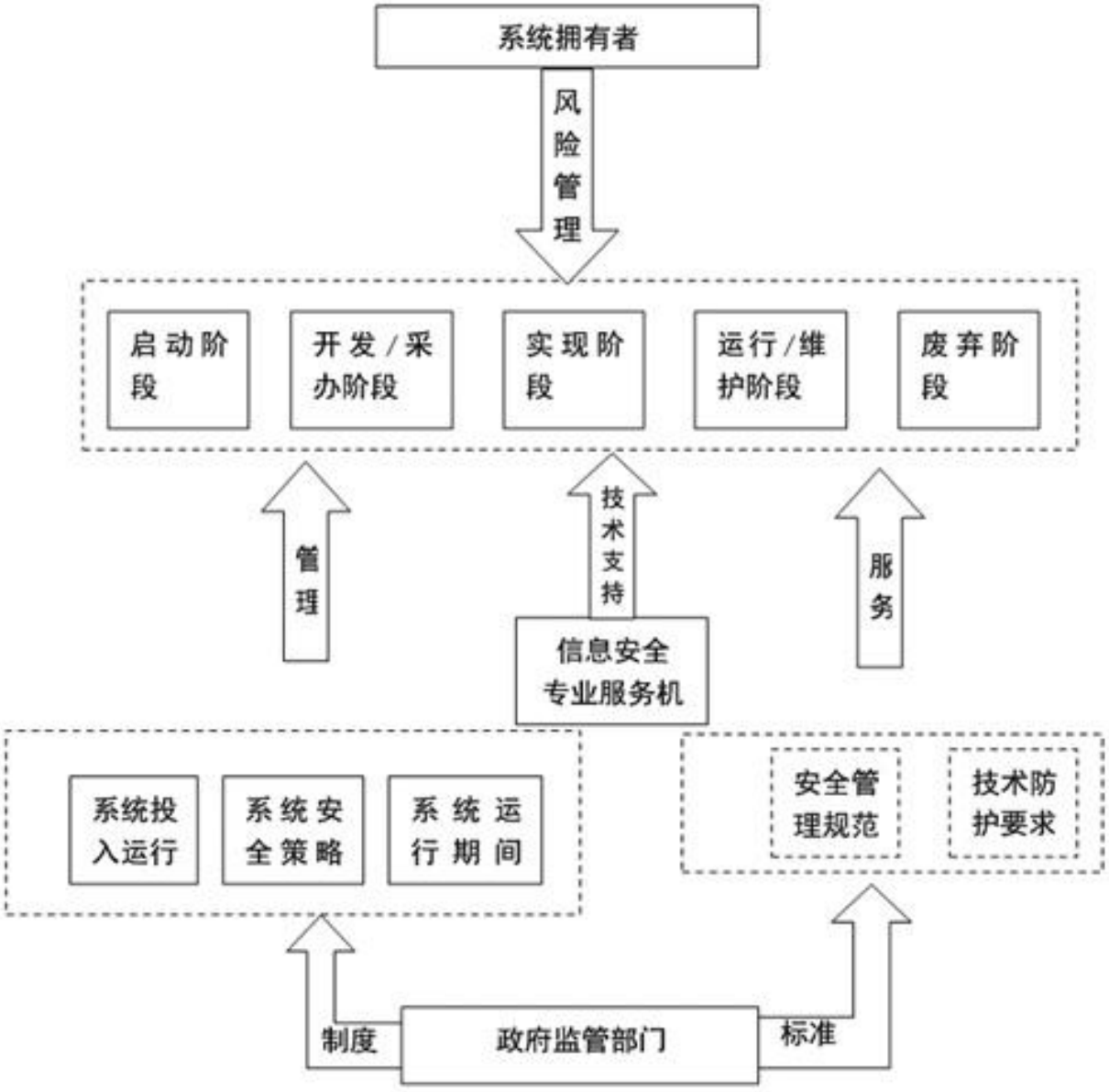
缺乏权威机构协调监管

行业技术

缺乏移动互联网监测与恶意软件认定技术

Android
Symbian
WM OS
BlackBerry
iOS
MTK

移动互联网的安全监管框架



政策法规标准

- 2009年年底，工信部公布了《通信网络安全防护监督管理办法 征求意见稿 》
- 2011年6月9日，中国互联网协会反网络病毒联盟近日发布了我国首个关于手机病毒命名及描述的技术规范——《移动互联网恶意代码描述规范》
- 2011年12月09日 ，工信部印发了《移动互联网恶意程序监测与处置机制》（以下简称《机制》），这是工业和信息化部首次出台移动互联网网络
- 2012年4月，工信部联合30多家单位起草的《信息安全技术、公共及商用服务信息系统个人信息保护指南》已正式通过评审，正报批国家标准。安全管理方面的规范性文件，引起了业界的广泛关注。
- 工信部正会同有关部门制订《移动智能终端管理办法》
- 筹备针对智能终端安全测评专项研究

目 录

- 移动互联网安全形势
- 移动互联网安全分析
- 移动智能终端安全技术
- 移动智能终端安全工具

移动智能终端的CVE安全漏洞-Android

There are **178** CVE entries or candidates that match your search. **CVE version: 20061101**

Name	Description
CVE-2012-1485	Unspecified vulnerability in the NetFront Life Browser (com.access_company.android.nflifebrowser.lite) application 2.2.0 and 2.3.0 for Android has unknown impact and attack vectors.
CVE-2012-1484	Unspecified vulnerability in the WaliSMS CN (cn.com.wali.walisms) application 2.9.2 and 3.7.0 for Android has unknown impact and attack vectors.
CVE-2012-1483	Unspecified vulnerability in the Message Forwarder (com.gmail.zbnetium) application 1.12.20110409.1 for Android has unknown impact and attack vectors.
CVE-2012-1482	Unspecified vulnerability in the TouchPal Contacts (com.cootek.smartdialer) application 3.3.1 and 4.0.1 for Android has unknown impact and attack vectors.
CVE-2012-1481	Unspecified vulnerability in the Textdroid (com.app.android.textdroid) application 2.5.2 for Android has unknown impact and attack vectors.
CVE-2012-1480	Unspecified vulnerability in the Pansi SMS (com.pansi.msg) application 1.97, 2.01, and 2.07 for Android has unknown impact and attack vectors.
CVE-2012-1479	Unspecified vulnerability in the AContact (com.movester.quickcontact) application 1.8.2 for Android has unknown impact and attack vectors.
CVE-2012-1478	Unspecified vulnerability in the UCMobile BloveStorm (com.blovestorm) application 2.2.0 and 3.2.1 for Android has unknown impact and attack vectors.
CVE-2012-1477	Unspecified vulnerability in the Cnectd (mci.cnectd) application 3.1.0 for Android has unknown impact and attack vectors.
CVE-2012-1476	Unspecified vulnerability in the KKtalk (com.kkliaotian.android) application 4.0.0 and 4.1.5 for Android has unknown impact and attack vectors.
CVE-2012-1475	Unspecified vulnerability in the YagattaTalk Messen has unknown impact and attack vectors.
CVE-2012-1474	Unspecified vulnerability in the Youni SMS (com.snd and attack vectors.
CVE-2012-1409	Unspecified vulnerability in the Tiny Password (com. unknown impact and attack vectors.
CVE-2012-1408	Unspecified vulnerability in the App Lock (com.cc.ap attack vectors.
CVE-2012-1407	Unspecified vulnerability in the GO Message Widget 2.3 for Android has unknown impact and attack vec
CVE-2012-1406	Unspecified vulnerability in the GO Bookmark Widge Android has unknown impact and attack vectors.
CVE-2012-1405	Unspecified vulnerability in the GO Note Widget (cor Android has unknown impact and attack vectors.

2006：1
2007：5
2008：3
2009：9
2010：22
2011：82
2012：56(Q1)

谷歌Android曝严重漏洞 可致系统崩溃

http://www.enet.com.cn/enews/ 2012年03月28日08：39 来源：搜狐IT

【文章摘要】国外研究人员日前发现了Android系统存在一个严重漏洞，该漏洞可以被黑客利用发起DoS攻击导致移动设备完全瘫痪。在发现漏洞之后，发现该漏洞的研究团队已为Android系统打上了补丁。

北京时间3月27日消息，据国外媒体报道，国外研究人员日前发现了Android系统存在一个严重漏洞，该漏洞可以被黑客利用发起DoS攻击导致移动设备完全瘫痪。在发现漏洞之后，发现该漏洞的研究团队已为Android系统打上了补丁。

移动智能终端的CVE安全漏洞-iOS

There are **131** CVE entries or candidates that match your search. **CVE version: 20061101**

Name	Description
CVE-2012-0646	Format string vulnerability in VPN in Apple iOS before 5.1 allows remote attackers to execute arbitrary code via a crafted racoon configuration file.
CVE-2012-0645	Siri in Apple iOS before 5.1 does not properly restrict the ability of Mail.app to handle voice commands, which allows physically proximate attackers to bypass the locked state via a command that forwards an active e-mail message to an arbitrary recipient.
CVE-2012-0644	Race condition in the Passcode Lock feature in Apple iOS before 5.1 allows physically proximate attackers to bypass intended passcode requirements via a slide-to-dial gesture.
CVE-2012-0643	The kernel in Apple iOS before 5.1 does not properly handle debug system calls, which allows remote attackers to bypass sandbox restrictions and execute arbitrary code via a crafted program.
CVE-2012-0642	Integer underflow in Apple iOS before 5.1 allows remote attackers to execute arbitrary code or cause a denial of service (device crash) via a crafted catalog file in an HFS disk image.
CVE-2012-0641	CFNetwork in Apple iOS before 5.1 does not properly construct request headers during parsing of URLs, which allows remote attackers to obtain sensitive information via a malformed URL, a different vulnerability than CVE-2011-3447.
CVE-2012-0635	WebKit, as used in Apple iOS before 5.1 and iTunes before 10.6, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2012-03-07-1 and APPLE-SA-2012-03-07-2.
CVE-2012-0633	WebKit, as used in Apple iOS before 5.1 and iTunes before 10.6, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site, a different vulnerability than other WebKit CVEs listed in APPLE-SA-2012-03-07-1 and APPLE-SA-2012-03-07-2.
CVE-2012-0632	WebKit, as used in Apple iOS before 5.1 and iTunes before 10.6, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and a other WebKit CVEs listed in APPLE-SA-2012-03-07-
CVE-2012-0631	WebKit, as used in Apple iOS before 5.1 and iTunes cause a denial of service (memory corruption and a other WebKit CVEs listed in APPLE-SA-2012-03-07-
CVE-2012-0630	WebKit, as used in Apple iOS before 5.1 and iTunes cause a denial of service (memory corruption and a other WebKit CVEs listed in APPLE-SA-2012-03-07-
CVE-2012-0629	WebKit, as used in Apple iOS before 5.1 and iTunes cause a denial of service (memory corruption and a other WebKit CVEs listed in APPLE-SA-2012-03-07-
CVE-2012-0628	WebKit, as used in Apple iOS before 5.1 and iTunes cause a denial of service (memory corruption and a other WebKit CVEs listed in APPLE-SA-2012-03-07-

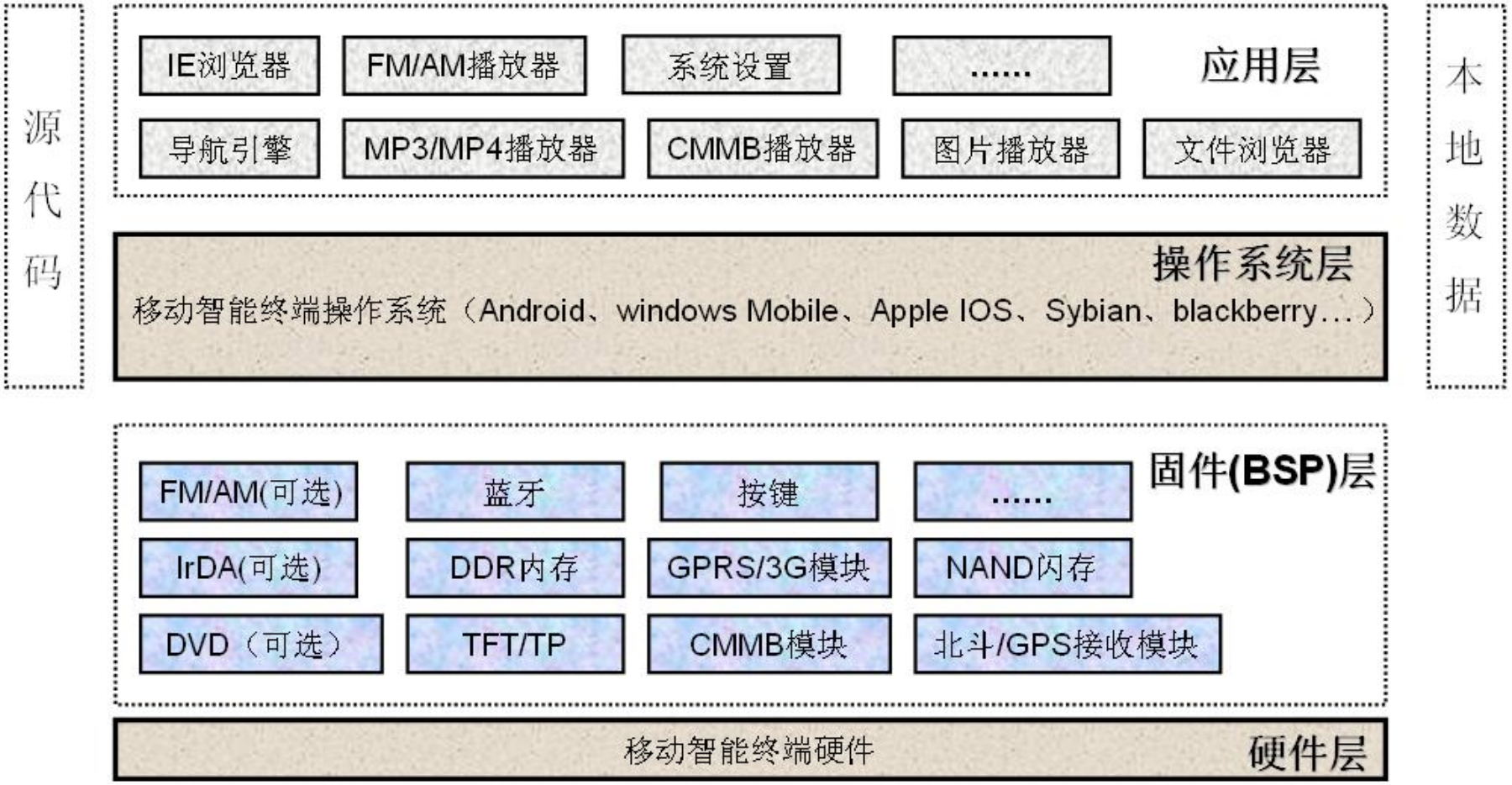
德国安全机构：苹果iOS操作系统存重大漏洞

2011-07-07 16:50:15 新浪科技 【大】【中】【小】 评论：[0]条

德国联邦信息安全局称：“这些缺陷使得潜在攻击者可以获得管理员权限，从而控制整个系统。”这个问题可能会发生于所有安装了iOS 4.3.3系统的设备上，如iPhone 3GS、iPhone 4、iPad、iPad 2和iPod Touch，同时还不能排除其他iOS版本具有相同缺陷的可能性。

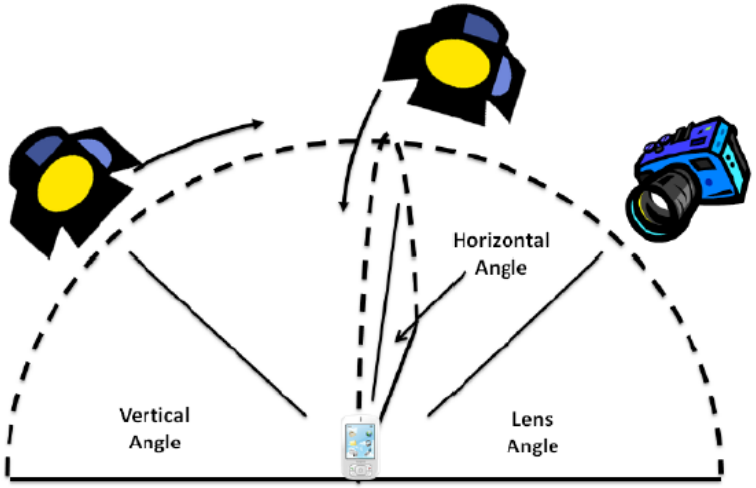
德国信息安全机构联邦信息安全局(Federal Office for Information Security)周三警告称，iPhone、iPad和iPod Touch等苹果设备采用的iOS操作系统具有“严重缺陷”，犯罪分子可以利用这一缺陷窃取这些设备上的机密数据。

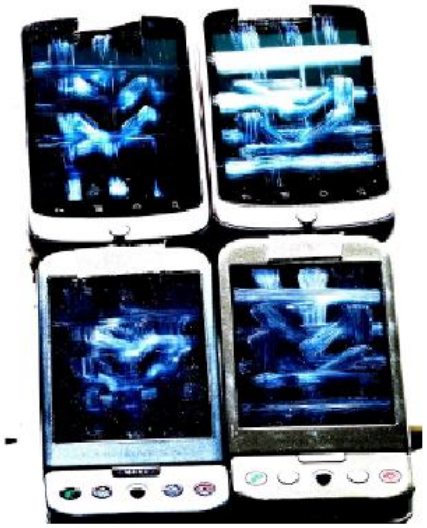
移动智能终端安全层次体系



Smudge攻击

加拿大卡尔顿大学carleton university



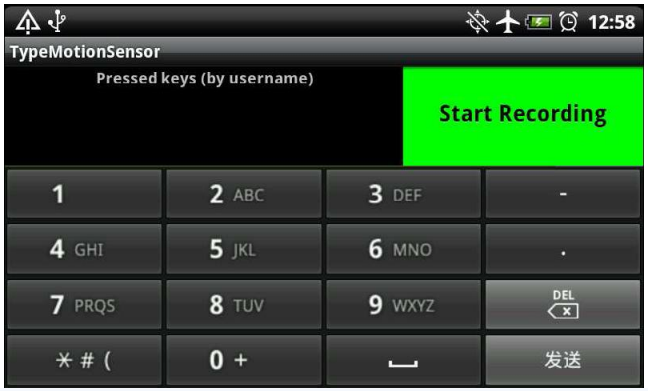


■图形密码是一种认证系统，通过让用户在图形用户界面上显示的图像中按照特定的顺序进行选择来工作

■图形密码方法有时也称为图形用户认证（GUA）

■对于大多数人来说，图形密码比文本方式的密码更容易记忆

■图形密码比文本密码提供的的安全性更强



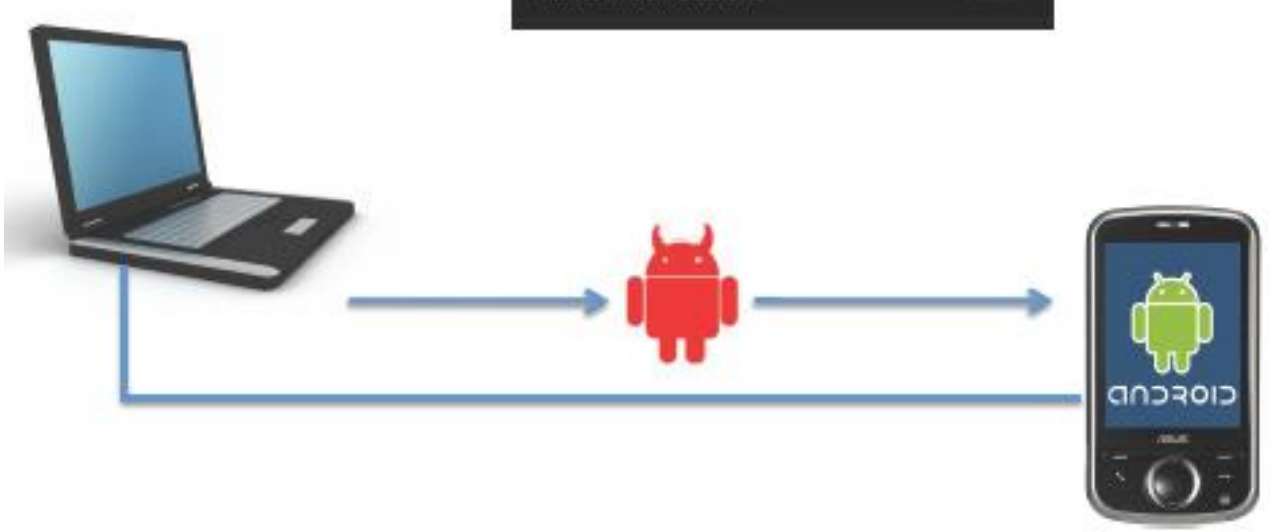
听按键音破译银行卡密码 男子3分钟盗取近20万

http://www.sina.com.cn 2012年03月24日 15:03 金羊网－新快报 微博

新快报讯 通过电话按键音破译银行卡密码，案犯在3分钟内盗取卡内近20万元存款。近日上海浦东新区法院审理的一案揭示了新的犯罪手段。

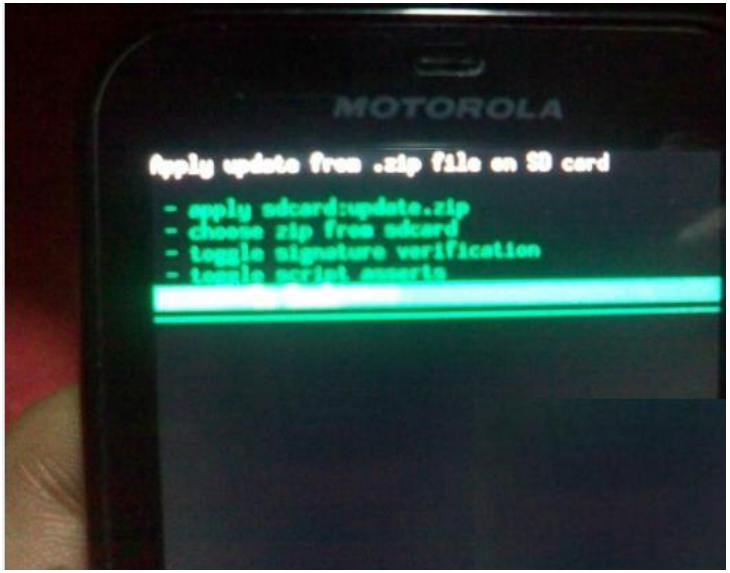
通过ADB进行物理访问

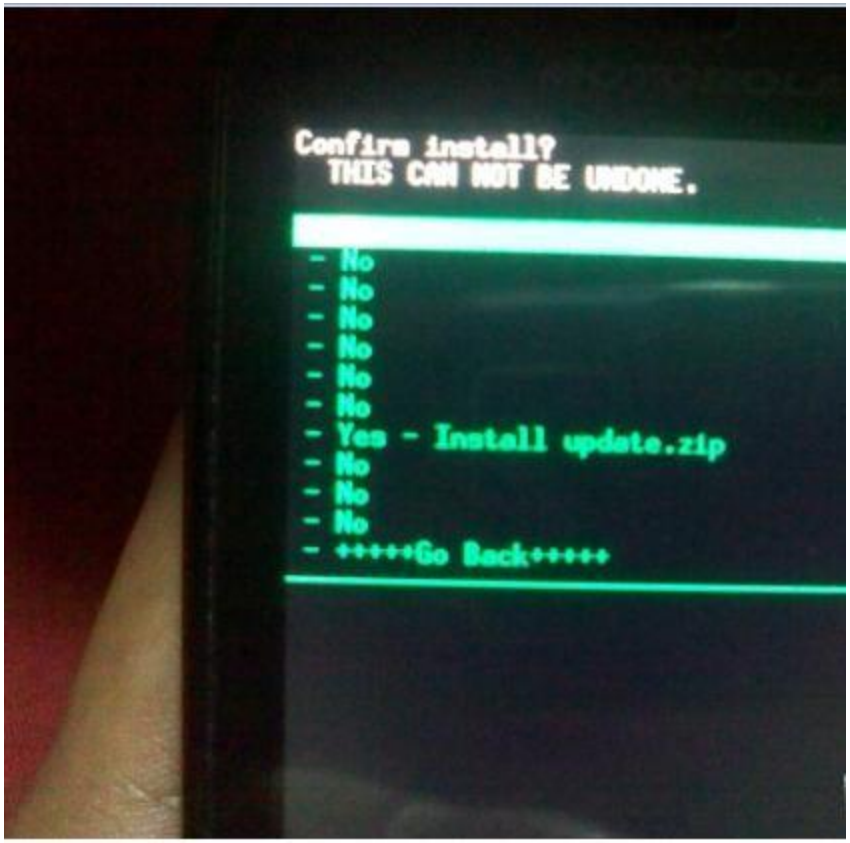
•如果坏人能不受限制的对您的手机进行物理访问，那他就不再是您的手机了
•If a bad guy has unrestricted physical access to your phone, it's not your phone anymore



利用恢复模式获取权限

- 恢复模式没有认证机制
- 黑客可以加载恶意的镜像
- 在不影响用户数据的情况下，访问用户数据

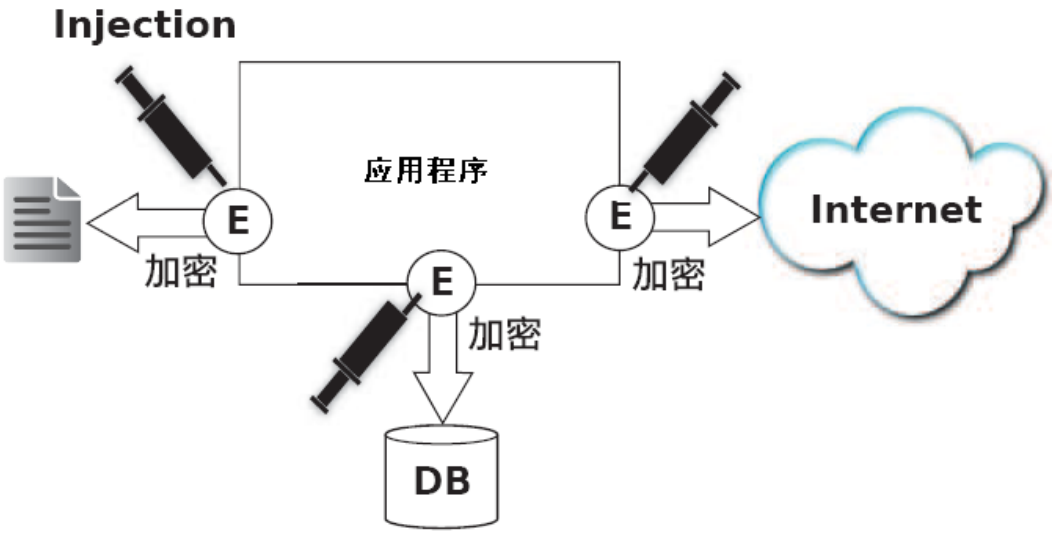




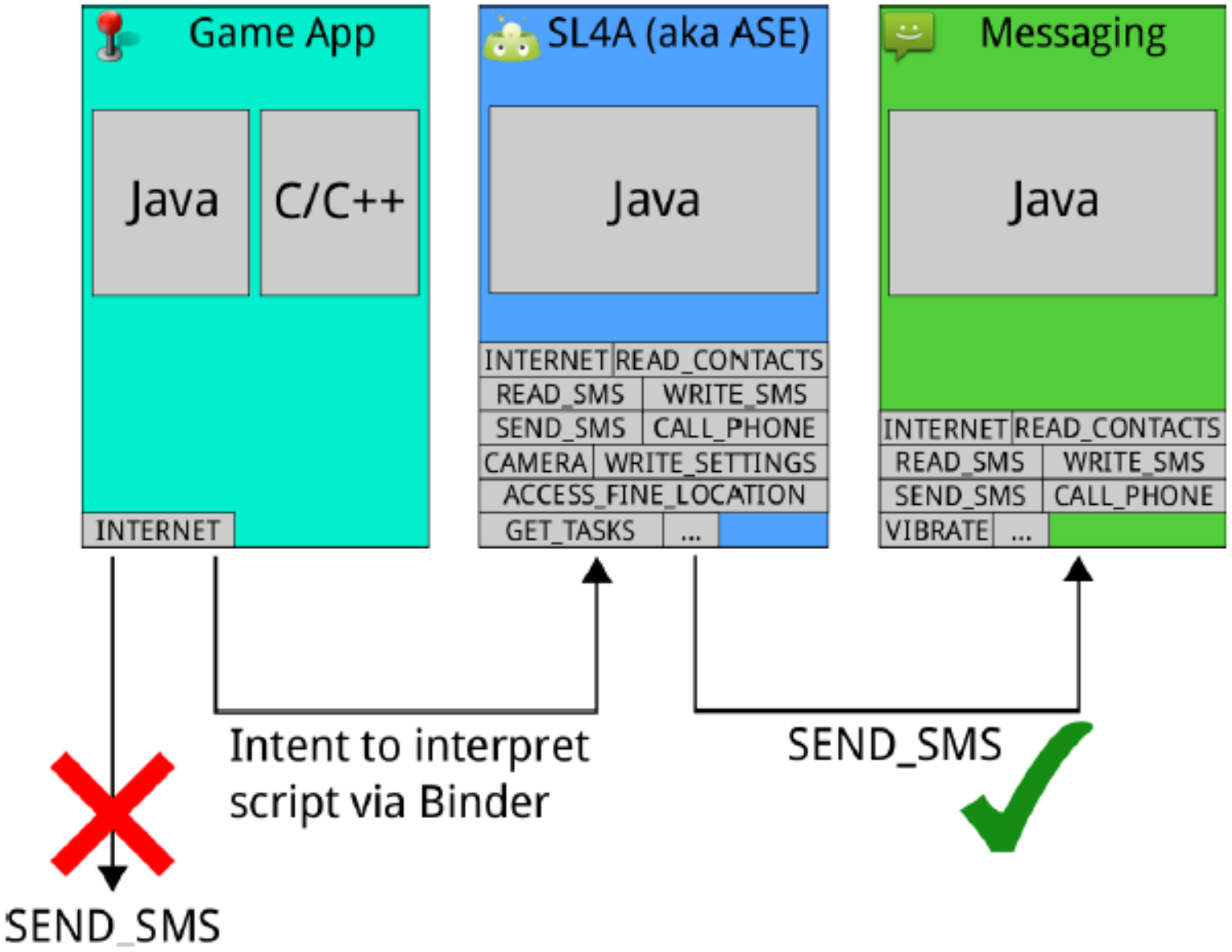
注入攻击

android系统sqlite数据库注入攻击

- 编程过程中，经常会把用户输入的数据拼成一个SQL语句，然后直接发送给服务器执行，比如：**string SqlStr = select * from customers where CompanyName Like % + textBox1.Text + %;**
- 这样的字符串连接可能会带来灾难性的结果，比如用户在文本框中输入：**a or 1=1**
- 那么**SqlStr**的内容就是：**select * from customers where CompanyName like %a or 1=1**
- 整个**customers**数据表的所有数据就会被全部检索出来，因为**1=1**永远**true**

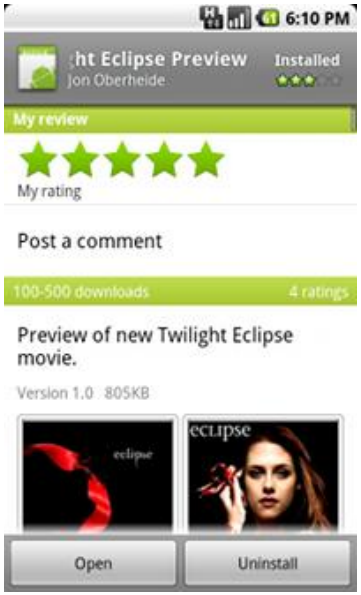


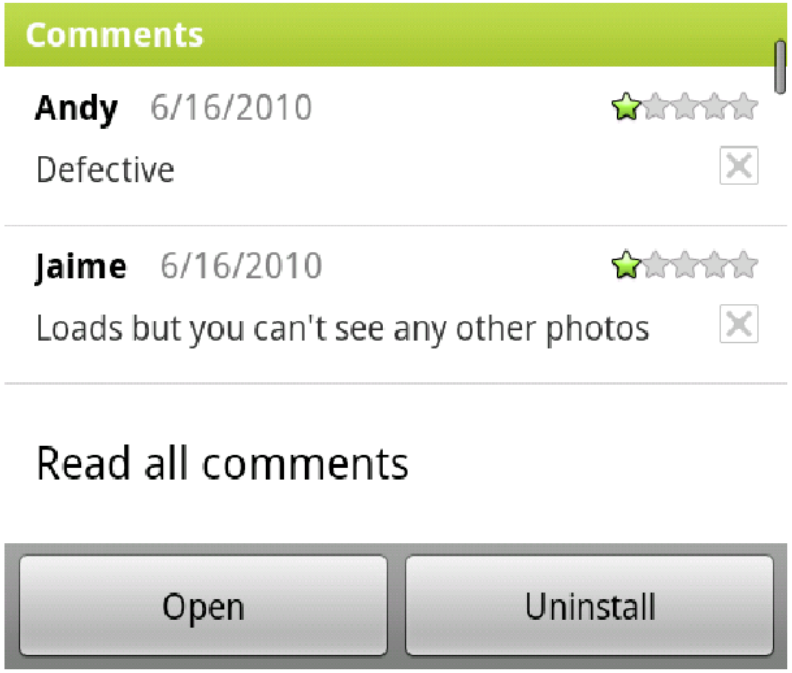
权限提升攻击


Game App
Java
C/C++
INTERNET
SL4A (aka ASE)
Java
INTERNET
READ_CONTACTS
READ_SMS
WRITE_SMS
SEND_SMS
CALL_PHONE
CAMERA
WRITE_SETTINGS
ACCESS_FINE_LOCATION
GET_TASKS
...
Messaging
Java
INTERNET
READ_CONTACTS
READ_SMS
WRITE_SMS
SEND_SMS
CALL_PHONE
VIBRATE
...
Intent to interpret script via Binder
SEND_SMS
SEND_SMS

社会工程学

•如果坏人能说服你安装并运行应用程序，那它就不再是您的手机了
•If a bad guy can convince you to install and run an app, it's not your phone anymore





2011 年十大最易被手机病毒植入的应用

1.伪装对象:**QQ 斗地主** 平台:Android
这是一款知名的手机游戏，部分传播渠道的安装包被植入了“安卓吸费王”病毒代码，感染用户后将在后台自动联网下载用于恶意推广的软件，大量消耗用户的手机资费。
2.伪装对象:**手机加速器** 平台:Android
手机加速器是一款 Android 平台上火热的工具软件，其被植入了远程控制代码，植入手机后自动联网接收服务器派发的一系列恶意指令。
3.伪装对象:**打地鼠** 平台:Android
打地鼠游戏是 Android 平台上的一款热门游戏，后经发现在部分渠道中传播的应用被植入了远程控制代码，植入手机后会自动连接服务器接收恶意指令
4.伪装对象:**五子棋** 平台:Android
五子棋是一款 Android 休闲游戏，经分析发现部分渠道中传播的这款应用中存在吸费代码
5.伪装对象:**指纹锁屏** 平台:Android
作为一款 Android 热门应用，经分析发现在部分渠道中提供的下载包内存在在窃取隐私的代码，通过远程控制木马植入后会派发恶意指令来盗取用户隐私。
6.伪装对象: **新蜀山剑侠** 平台:Symbian
根据“云安全”数据监测新蜀山剑侠这款热门的 Symbian 游戏的部分程序中被植入了吸费代码，一旦下载将落入黑客设置的陷阱之中。
7.伪装对象: **语音短信** 平台:Symbian
语音短信是一款新兴的移动互联网应用，但其也很快成为了黑客的伪装对象，数据显示部分渠道中存在的这一应用被植入了吸费代码。
8.伪装对象:**欢乐斗地主** 平台:Android
联机游戏“欢乐斗地主”成为了 Android 手机中的热门应用，但在一些中小软件论坛中却有一些病毒作者以提供这款游戏下载为名传播手机病毒。一旦下载将在后台运行恶意程序，以外发短信、强制开通 SP 服务的方式实施恶意扣费。
9.伪装对象: **冷血狙击** 平台:Android
冷血狙击是一款 Android 热门游戏，网秦“云安全”数据分析中心发现，有部分渠道提供的魔音软件中存在窃取隐私行为。
10. 伪装对象:**来电反转** 平台:Android
来电反转是一款热门的手机工具软件，据网友反应在部分中小手机论坛下载这款软件后，发现手机出现了遭恶意扣费的现象，后据网秦“云安全”数据分析中心发现，部分渠道的这款软件实际被植入了存在扣费行为的“安卓吸费王”手机病毒。

- ■特点1:恶意软件被大批植入到热门应用中
- ■特点2:手机ROOT 权限一再被滥用
- ■特点3:APP 应用发布前缺乏安全审核

主要的安全技术手段

功能	描述
Personal Firewall、Incoming Call Filter、SMS Antispam	可以过滤垃圾短信、过滤来电以及 IP 数据包
VPN	支持 L2TP/PPTP VPN、SSLVPN、IPSEC VPN
抗病毒	杀毒
防盗	通讯录取回功能、隐私信息远程删除功能、远程控制功能
WAP Push 过滤	WAP URL 过滤，对通过 WAP Push 下发的 URL 进行过滤，防止用户下载恶意 URL 链接。
文件加密	本地文件加密
系统清理，漏洞修复	清理垃圾信息，修复系统和应用软件漏洞
响一声电话提醒	防止用户回拨，恶意扣费
进程拦截、流量监控	进程启动联网时提示，防止进程悄悄联网等行为。对上网流量进行统计、告警
家长控制	控制移动终端行为如上网网址，用于家长控制小孩安全使用移动终端，防止访问不健康的信息
端口控制（Port Control）	严格统一管理这些外设，设置其启用或禁用。通过外设安全防护机制，可以实现对 FireWire、Wireless LAN、Bluetooth、SD 卡等外设的控制
增强认证机制	指纹认证等手段，防止移动终端丢失导致信息泄露

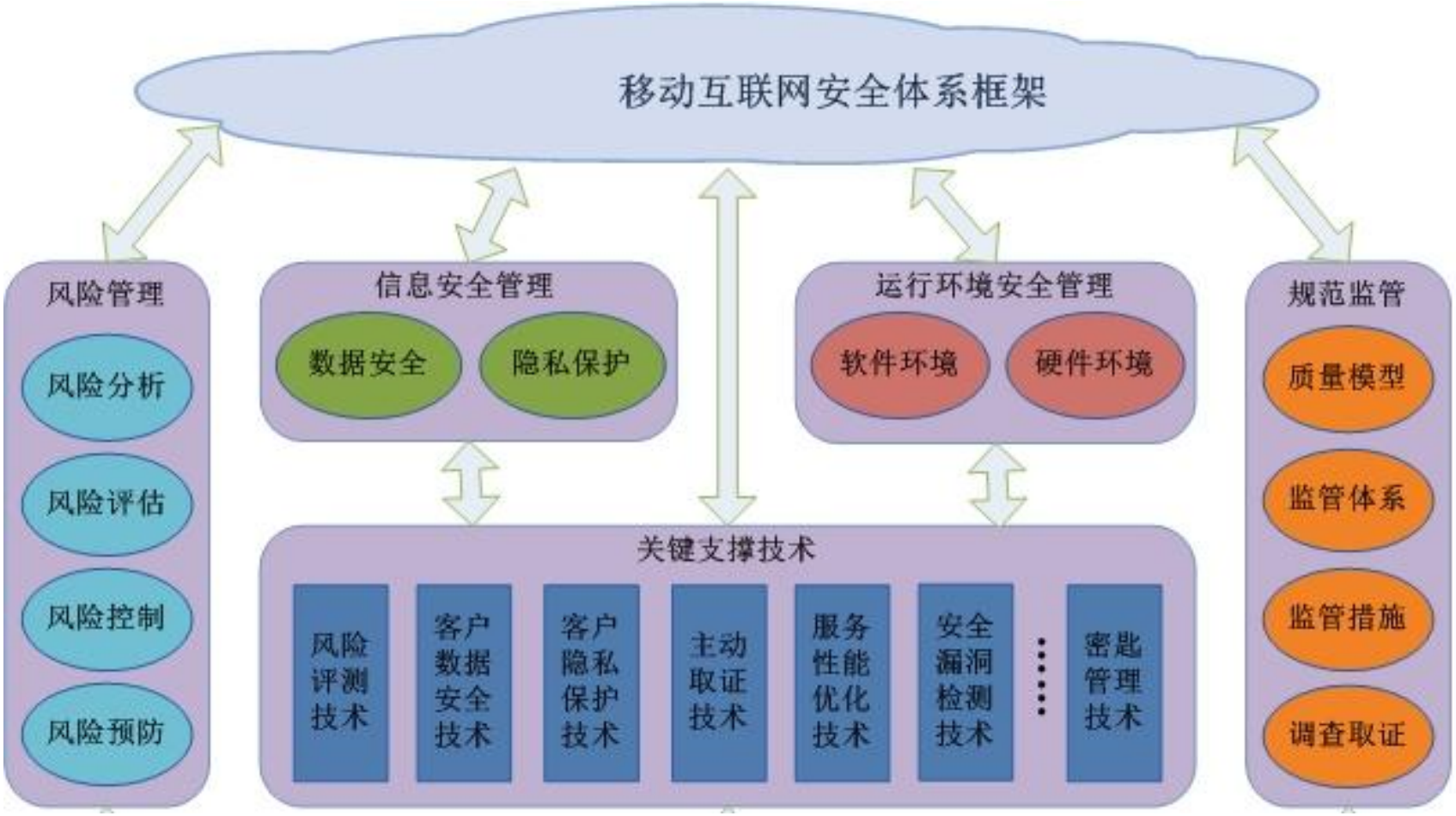
谷歌Bouncer

- 谷歌并未对应用程序上架Android Market要求太多审核的过程，这对开发者而言十分便利，却也为恶意软件提供了可乘之机。
- 2012年2月3日，谷歌发布了用来维护Android Market安全性的机制“Bouncer”。
- 与苹果以人工审核AppStore的形式不同，Bouncer是自动扫描Android Market上的应用程序，分别对新上传的、已上传的应用程序做分析，比对是否符合已知恶意软件特征，或是应用程序有不正常行为。
- 谷歌会在云端实际执行每个应用程序，模拟手机上的运作状况，以便找出潜藏其中的病毒或木马。
- Android操作系统本身也提供了沙盒、权限、移除三种安全机制。有必要时，谷歌Android Market甚至可以远端移除移动设备上的恶意程序。

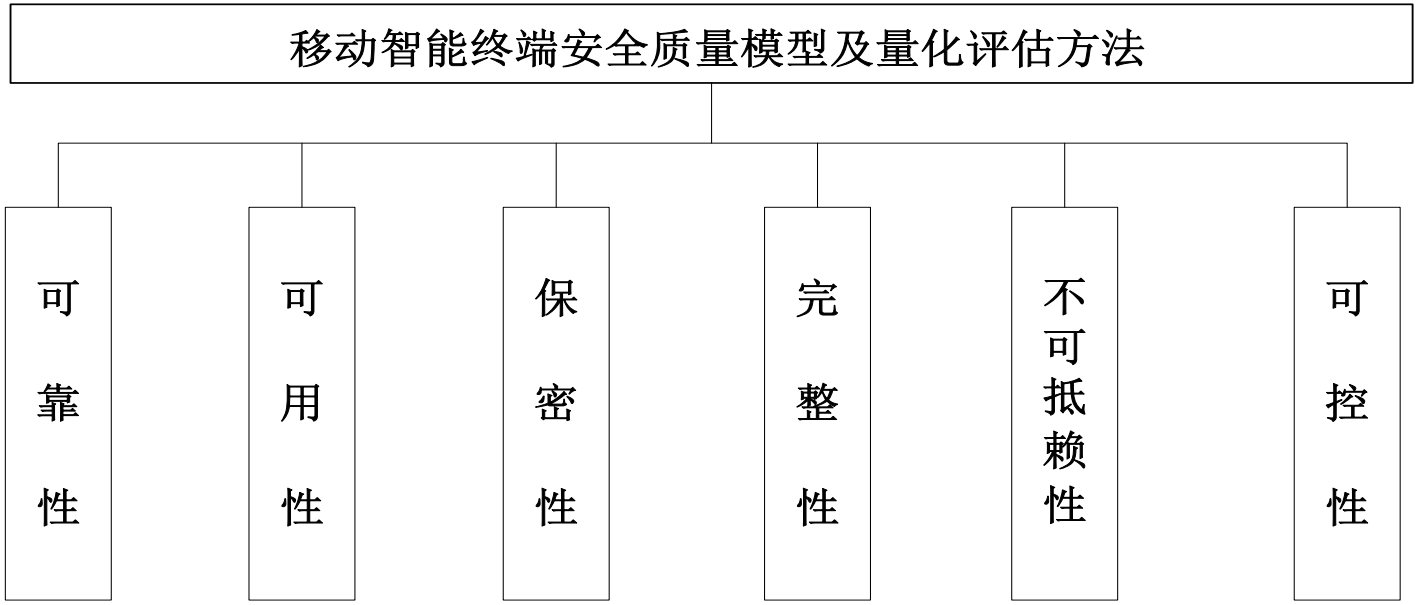
Android手机防盗-DroidRing

- DroidRing 是一款Android手机防盗程序
- 通过发送短信给丢失的手机，可以得到当前手机地理信息（地图链接，街道名称）
- 此外提供更换SIM卡提示，响铃提醒等功能，帮助您找回手机。
- 主要功能
  - ✓ 通过发送短信得到当前丢失手机地理位置。(地图链接，街道地址)
  - ✓ 过发送短信使得手机以最大声音响铃，不论之前是否是静音。可帮助进一步寻声找到手机
  - ✓ 发送的指令短信到丢失手机不会产生任何提醒，避免持有者警觉。这些短信会被转移到保护文件夹，以备以后查询
  - ✓ 当SIM卡被更换，新的卡号和现在地理位置自动发送到预先设定的安全手机中。

移动互联网安全体系框架



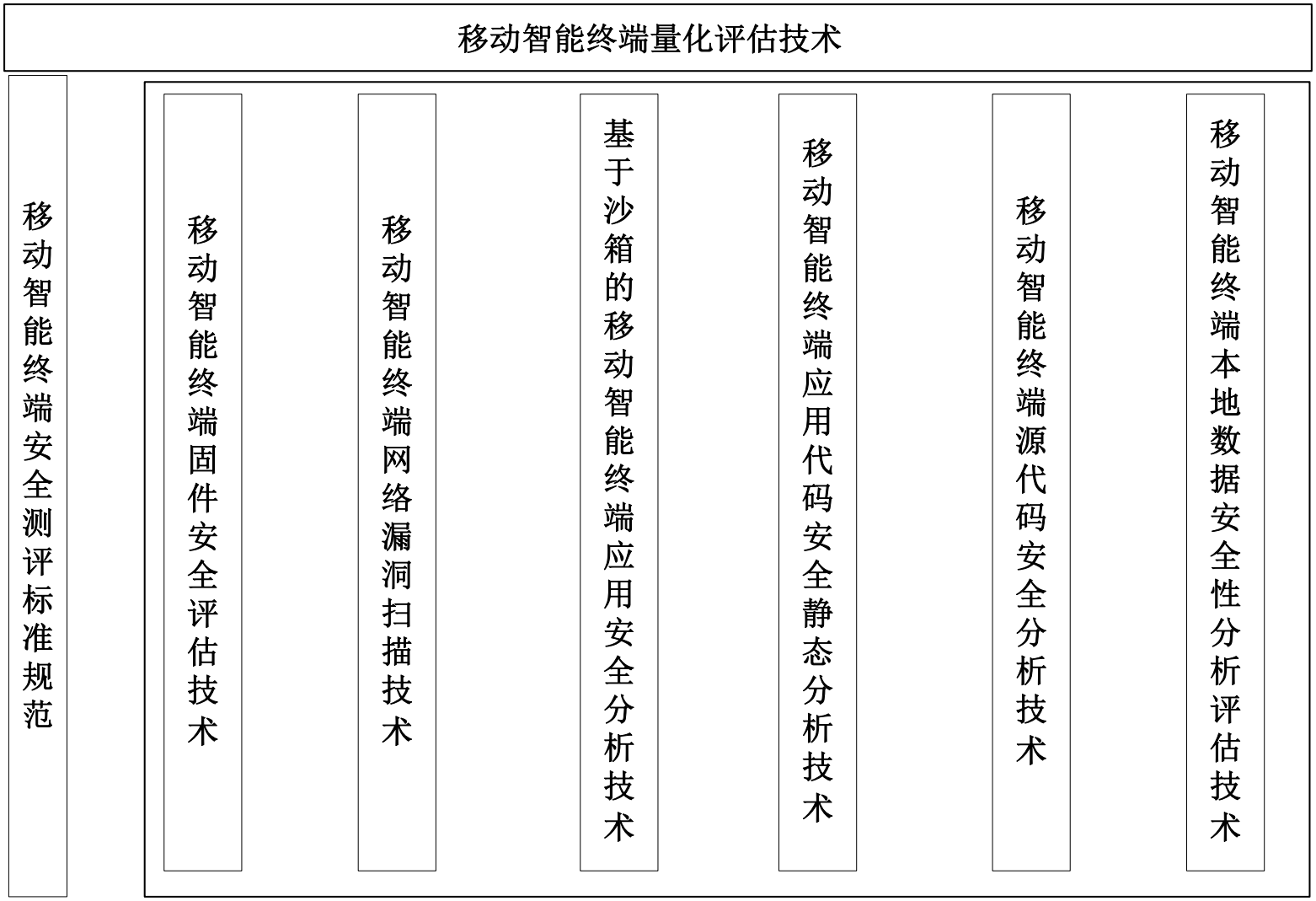
移动智能终端安全评估模型和方法



■一套能够全面反映移动智能终端安全特征的量化评估模型，包括层次化评估指标体系的建立、评估指标的标准化、评估方法的确定等重要环节，具有科学性、全面性、可比性、可操作性等特点。

■将应用层析分析法首先将移动智能终端安全问题层次化，分解为不同的组成因素，并按照因素之间的相互关联影响以及隶属关系将因素按不同的层次聚集组合，形成一个多层次的分析结构模型，从而能够适合比较复杂的终端安全问题状况

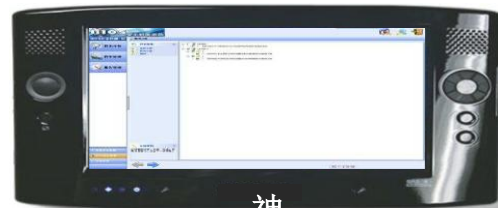
移动智能终端量化评估技术



固件（BSP）安全评估技术

- 针对市场上主流移动智能终端的固件（BSP）代码，采用固件代码完整性检查分析技术和基于固件漏洞的库固件漏洞信息的检查分析技术，判定移动智能终端固件的安全隐患并提供修复建议。

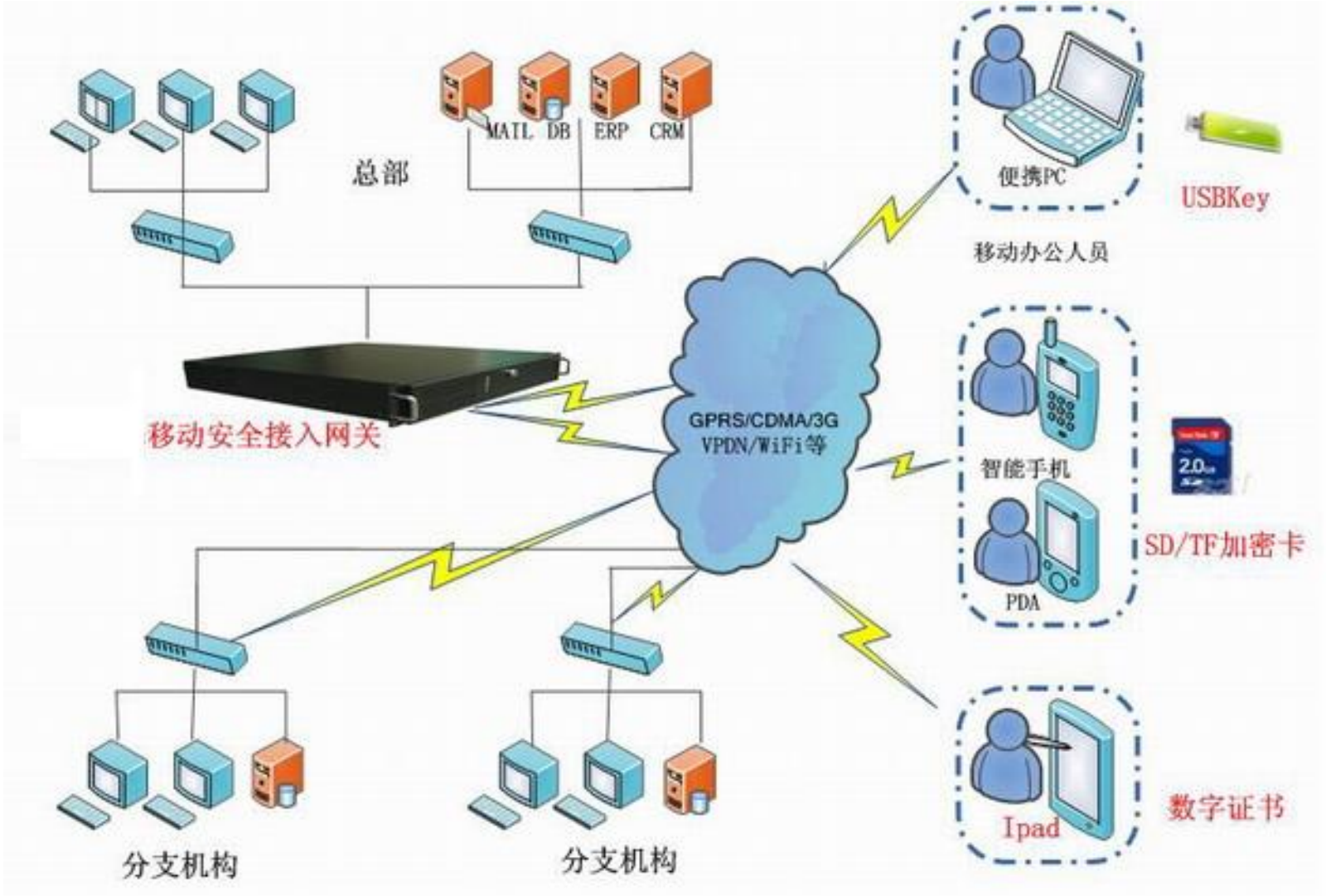
隐患名称	隐患来源
远程开机隐患	固有安全隐患
定时开机隐患	固有安全隐患
ChipAwayVirus隐患	外来安全隐患
磁盘恢复精灵隐患	外来安全隐患
Phoenix.Net隐患	外来安全隐患
BIOS木马隐患	外来安全隐患
其他未知隐患	固有/外来



终端源代码安全分析技术

- 漏洞从根本上来源于软件的源代码
- 针对移动智能终端重点应用行为相关的源代码
  - ✓ 费用相关：通信安全付费、网络支付、广告。。。
  - ✓ 恶意访问：通讯录、记事本。。。
  - ✓ 安全后门：远程控制、缓冲区溢出。。。
- 技术特点
  - ✓ 动态安全分析：通过编译程序或检测用例，检测源代码中**语法、词法、功能或结构的问题**；完成后可能仍会存在与安全相关的在编译阶段发现不了、运行阶段又很难定位的安全问题。
  - ✓ 静态安全分析：执行所分析的源代码，而是扫描源程序正文，对程序中的**数据流和控制流**等进行分析，来发现**编译阶段没有发现、运行阶段难于定位**的源代码安全问题。

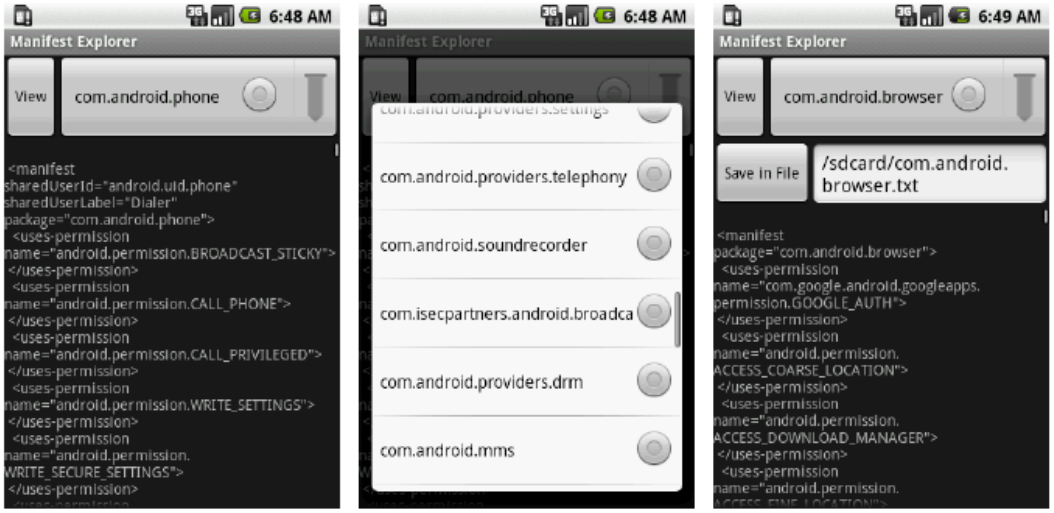
移动智能终端接入认证


总部
MAIL
DB
ERP
CRM
移动安全接入网关
GPRS/CDMA/3G
VPDN/WiFi等
便携PC
USBKey
移动办公人员
智能手机
PDA
SD/TF加密卡
Ipad
数字证书
分支机构
分支机构

目 录

- 移动互联网安全形势
- 移动互联网安全分析
- 移动智能终端安全技术
- 移动智能终端安全工具

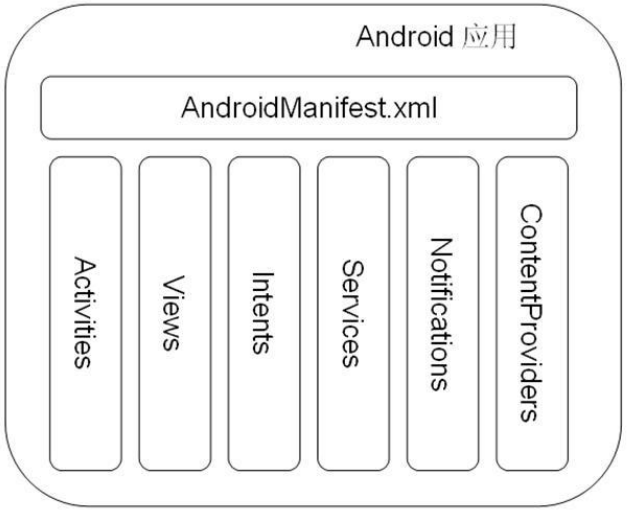
Manifest Explorer



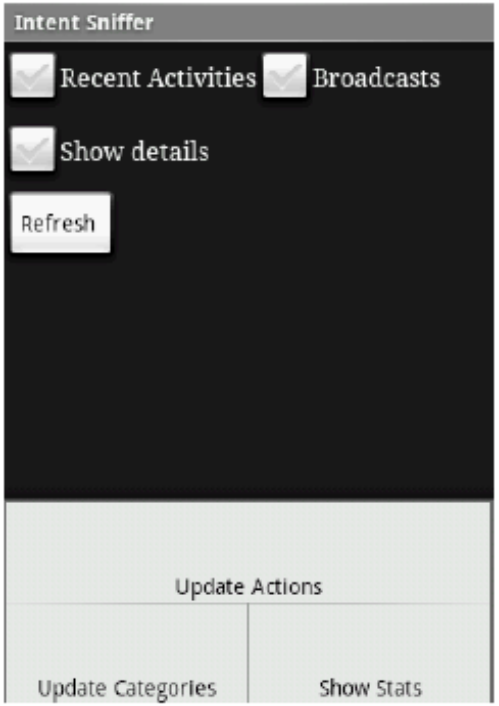
■**Android**程序的全局配置文件，是每个 **android**程序中必须的文件

■位于开发的应用程序的根目录下，描述了**package**中的全局数据，包括**package**中暴露的组件 （**activities, services,** 等等），以及他们各自的实现类，各种能被处理的数据和启动位置等重要信息

■提供了**Android**系统所需要的关于该应用程序的必要信息，即在该应用程序的任何代码运行之前系统所必须拥有的信息



Intent Sniffer

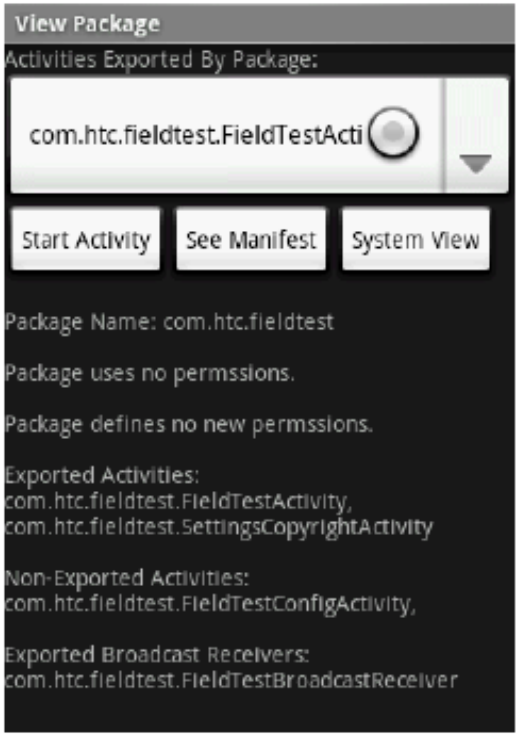


■**Android**中提供**Intent**机制来协助应用间的交互与通讯

■**Intent**负责对应用中一次操作的动作、动作涉及数据、附加数据进行描述，根据此**Intent**的描述，负责找到对应的组件，将 **Intent**传递给调用的组件，并完成组件的调用

■**Intent**不仅可用于应用程序之间，也可用于应用程序内部的**Activity/Service**之间的交互

Package Play



■显示**Android**系统中安装的所有**Package**

智能手机取证

电子证据---手机

1、iOS---iPad, iPhone,iPod Touch

2、Windows Mobile

3、BlackBarry　4、塞班　5、安卓

手机取证的理论、原则与模型

❖手机取证的原则

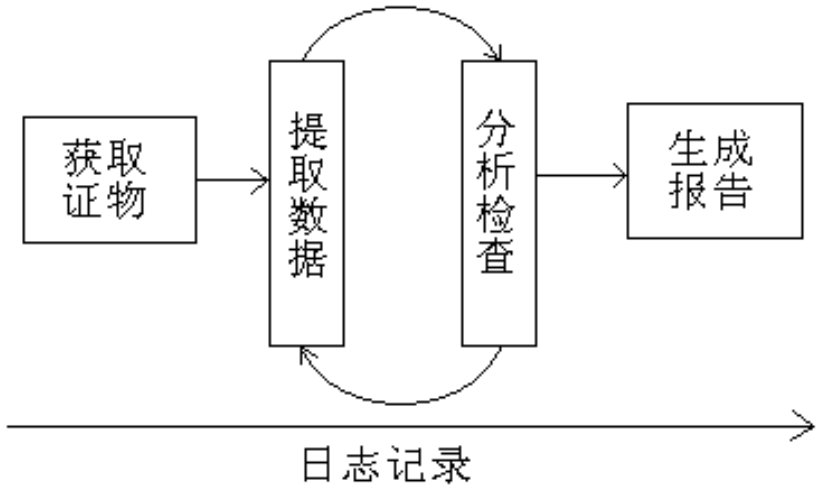
(1)作为证据的手机及其相关设备中的数据是未经改动的，对其的任何操作都要保证原始数据的完整性；

(2)由专门的人员访问手机及其相关设备中的数据,这些人员必须是有资格的,并且能够解释其行为；

(3)所有对手机及其相关设备的操作（包括对证据的获得、访问、提取、存储和转换）都必须由第三方建立日志审计，完全归档保存，以备质询；

(4)负责操作和调查的人员和组织必须遵守以上原则并对操作行为负责。

❖手机取证的基本模型



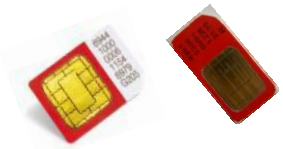
手机取证中数字证据提取方式

❖目标

- 尽可能多地获取数据
- 最大程度地保持设备数据的原始性
- 以方便理解的格式获取数据

❖对象

- 手机机身
- 手机卡
- 手机移动存储卡
- 网络运营商



智能手机取证工具

CellDEK

谢谢！