第六章

1移动智能终端

1.1移动智能终端的定义

移动智能终端是指具有独立操作系统、可安装应用程序、使用无线局域网或移动通信网访问因特网的设备,其典型代表如智能手机和平板电脑。

1.2移动智能终端的逻辑结构



1.3移动智能终端的分类

智能手机

平板电脑

1.4移动智能终端的功能

能够访问不同模式的移动通信网络

能够通过不同的网络接口访问因特网

具有开放的API接口

支持多任务

具有多媒体功能

具有GPS导航功能

1.5移动智能终端具有哪些特点

具备一个具有开放性的操作系统平台,可以安装更多的应用程序从而使智能终端的功能得到无限扩充

具备PAD功能包括PIM(个人信息管理)、日程记事、任务安排、多媒体应用、浏览网页等功能

具备无线接入互联网的能力即需要支持GSM网络下的GPRS或者CDMA网络下的CDMA1X或3G网络

功能强大扩展性强支持多个第三方软件.

2移动智能终端安全威胁

2.1移动智能终端安全形势

智能终端操作系统敏感权限滥用

应用软件难溯源

智能终端操作系统漏洞

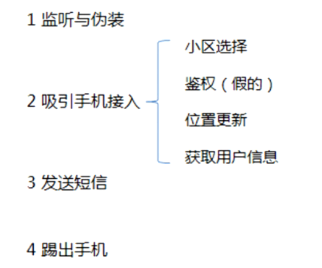
智能终端操作系统后门

2.2移动智能终端面临的主要安全威胁

伪基站攻击

“伪基站”即假基站,设备一般由主机和笔记本电脑或手机组成,通过短信群发器、短信发信机等相关设备能够搜取以其为中心、一定半径范围内的手机卡信息,利用2G移动通信的缺陷,通过伪装成运营商的基站冒用他人手机号码强行向用户手机发送诈骗、广告推销等短信息。

伪基站的工作流程



二维码扫描

二维码(TWo- Dimenslonalcode,TDC)是指在一维条码的基础上扩展出来的另一种具有可读性的条码。二维码使用黑白色矩形图案表示二进制数据。

二维码的基本特点

信息容量大，编码范围广

容错能力强，译码可靠性高

编译简便，成本低

二维码带来的安全问题

成为病毒木马、钓鱼网站传播新渠道。

二维码信息更容易泄露

对二维码的监管力度不够

二维码成为违法信息传播新方式

二维码与移动支付结合,成为金融诈骗新手段

移动终端遗失

手机丢失后先做6件事

致电运营商挂失手机号

致电银行冻结手机网银

微信用户登录110.qq.Com冻结账号

修改微博、微信、QQ等密码

到手机运营商处补手机卡

手机病毒

手机病毒是一种具有传染性、破坏性的手机程序。手机病毒可通过短信、彩信、电子邮件和蓝牙等方式进行传播,常常伪装成手机软件和系统程序诱骗用户下载。

手机病毒的危害

窃取用户信息

用户信息丢失

破坏手机硬件

发送垃圾信息

恶意扣费软件

恶意扣费软件是指没有对用户进行任何提示,通过发送短信或联网等方式强制扣除用户手机话费的软件。

3移动智能终端的安全使用

3.1移动终端安全使用建议

意隐私权限访问请求

慎重扫描二维码

不要“见码就扫”

不要随意“晒码”和丢弃含有二维码的票据

从正规渠道下载应用

安装安全防护软件

定期备份

不要登录到不安全的无线网络

尽量避免访问财务或银行信息

在上网浏览器不要选择“记住我”

清空历史记录和缓存内容

启动用户认证

谨慎对待陌生信息

注意安全管理终端