ICS 33.050.01
M 30

YD

中华人民共和国通信行业标准

YD/T 2674-2013

移动智能终端信息安全设计导则

Design guidance of information security for smart mobile terminals

2013-10-17 发布　　2014-01-01 实施

中华人民共和国工业和信息化部 发布

目　次

前　言……II
引言……III
1　范围……1
2　规范性引用文件……1
3　术语、定义和缩略语……1
3.1　术语和定义……1
3.2　缩略语……2
4　设计原则……3
5　设计思路……3
6　安全威胁和攻击……4
6.1　硬件安全……4
6.2　操作系统安全……4
6.3　接口安全威胁……4
6.4　应用层安全威胁……4
6.5　用户信息安全威胁……4
6.6　终端刷机安全威胁……5
6.7　恶意代码安全威胁……5
6.8　垃圾信息安全风险……5
7　安全框架……5
7.1　移动智能终端安全框架……5
7.2　移动智能终端安全目标……6
8　安全要求……6
9　解决方案……6
9.1　终端硬件安全方案……6
9.2　操作系统安全方案……6
9.3　应用软件安全方案……7
9.4　通信接口安全方案……8
9.5　用户数据安全方案……9
附录A（资料性附录）　应用软件商店安全分析和安全措施……11
参考文献……14

前　言

本标准为移动智能终端安全系列标准之一。该系列标准的名称和结构预计如下：

——YD/T 2674-2013《移动智能终端安全能力设计导则》；

——YD/T 2407-2013《移动智能终端安全能力技术要求》；

——YD/T 2408-2013《移动智能终端安全能力测试方法》。

本标准按照GB1.1给出的规则起草。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、北京电信规划设计院有限公司、中国电信集团公司、诺基亚通信有限公司、北京展讯高科通信技术有限公司。

本标准起草人：落红卫、汪　坤、潘　娟、张大江、陈　萍、仝建刚。

引　言

移动通信技术与互联网技术日益结合，不仅催生移动互联网业务应用，同时也促进了移动智能终端发展。一方面，移动智能终端使用方便，功能强大，给人们的工作和生活带来了极大的方便。另外一方面，伴随其开放性和便携性，移动智能终端也给用户带来了巨大的安全威胁。

人们已普遍认识到移动智能终端信息安全应该在设计阶段就植入，而不是在其进入产品阶段再来考虑。同时，为了充分发挥信息安全效用，应将其作为一个重要的问题来考虑，贯穿移动智能终端从系统构想到设备淘汰的整个生命周期。特别是，在移动智能终端设计阶段和系统开发阶段对安全问题考虑不周，很容易导致其产生易受攻击的风险。标准化在移动智能终端设计阶段的信息安全起至关重要的作用，确保移动智能终端的信息安全成为技术标准制定过程应考虑的重要问题和指导原则，以帮助移动智能终端的信息安全能力足够可靠有力来抵抗外部攻击。

本标准的制定必将规范移动智能终端信息安全要求和设计，简化设计人员工作，改善移动智能终端安全形势，使开发人员把更多精力投向移动智能终端业务和功能创新，最终推动整个移动互联网的健康发展。相反，如果没有相关标准规范，不仅会使设计工作无章可循，使信息安全问题纷乱繁杂，同时导致后期信息安全问题的解决难度大幅度增加。所以，非常有必要制定移动智能终端信息安全设计导则规范。通过技术标准的制定，可以：

1）指导移动智能终端信息安全设计；

2）引导企业自主研究移动智能终端信息安全技术，从而加强其安全功能和性能；

3）带动企业实行产品创新，创造新的价值链；

4）为移动互联网发展构建更加安全和谐的发展环境。

移动智能终端信息安全设计导则

1 范围

本标准规定了移动智能终端信息安全的设计原则、设计思路、安全威胁、安全框架、安全目标、安全要求和解决方案。

本标准适用于蜂窝移动通信网的移动智能终端。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

YD/T 2035　　移动终端垃圾短消息过滤技术要求

YD/T 2407-2013　移动智能终端安全能力技术要求

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

电信智能卡

移动智能终端所使用的智能卡，包括SIM、UIM、USIM等。

3.1.2

访问控制

一种防止资源被未授权用户使用的安全策略。

3.1.3

授权

在用户身份经过认证后，根据预先设置的安全策略，授予用户相应权限的过程。

3.1.4

数字签名

附在数据单元后面的数据，或对数据单元进行密码变换得到的数据。允许数据的接收者证明数据的来源和完整性，保护数据不被伪造，并保证数据的不可否认性。

3.1.5

移动智能终端操作系统

移动智能终端最基本的系统软件，它控制和管理移动智能终端各种硬件和软件资源，并提供应用程序开发的接口。

3.1.6

用户

与移动智能终端交互的任何实体。

3.1.7

用户数据

由用户在本地生成或为用户在本地生成的数据及在用户许可后由外部进入用户数据区的数据。

3.1.8

移动智能终端

采用开放式操作系统的移动终端，用户可以在该终端上安装或者卸载应用软件，同时，第三方开发人员可以基于该操作系统提供的API接口进行软件开发。

3.2 缩略语

下列缩略语适用于本文件。

API	Application Programming Interface	应用程序接口
CDMA	Code Division Multiple Access	码分多址
CF	Compact Flash	紧凑式闪存
CPU	Central Processing Unit	中央处理单元
DDoS	Distributed Denial of Service	分布式拒绝服务
DoS	Denial of Services	拒绝服务
EMS	Enhanced Messaging Service	增强型消息业务
GPS	Global Positioning System	全球定位系统
GSM	Global System for Mobile Communications	全球移动通信系统
HTML	HyperText Markup Language	超文本标记语言
ID	Identifier	标识
IM	Instant Messaging	即时消息
IMEI	International Mobile Equipment Identity	国际移动设备识别
IMSI	International Mobile Subscriber Identity	国际移动用户识别码
IP	Internet Protocol	互联网协议
ME	Mobile Equipment	移动设备
MMS	Multimedia Messaging Service	多媒体消息业务
NFC	Near Field Communication	近场通信
OS	Operating System	操作系统
OTP	One-Time Password	一次性口令
PC	Personal Computer	个人电脑
PDA	Personal Digital Assistant	个人数字助理
PIN	Personal Identification Number	个人识别号码
PUK	Personal Unlock Key	个人解锁密钥
R-UIM	Removable User Identity Module	可更换用户识别模块
SIM	Subscriber Identity Module	用户识别模块
SMS	Short Messaging Service	短消息业务
TCP	Transmission Control Protocol	传输控制协议

TD-SCDMA	Time Division-Synchronous Code Division Multiple Access	时分同步码分多址
UIM	User Identity Module	用户识别模块
USB	Universal Serial Bus	通用串行总线
USIM	Universal Subscriber Identity Module	普通用户识别模块
WCDMA	Wideband Code Division Multiple Access	宽带码分多址
WLAN	Wireless Local Area Network	无线局域网

4 设计原则

为了提高移动智能终端的信息安全能力，首先要求设计者改变单一片面认识，树立起全面系统的观念。移动智能终端的信息安全不是单纯技术问题，也不是简单安全功能的堆砌，而是一项复杂的系统工程。同时，设计者应意识到信息安全问题不可能彻底消除，只能在有一定目的性和确定成本的情况下尽可能地减小，故此，在进行移动智能终端信息安全设计的同时，应考虑到以下设计原则：

- 整体性原则：任何硬件和软件的安全漏洞都可能导致移动智能终端受到安全威胁，同时，移动智能终端的硬件和软件作为有机整体相互关联，例如：外围接口非法调用，既涉及接口本身，也涉及操作系统，还涉及应用软件。故此，移动智能终端的信息安全应从整体的角度来全面考虑。
- 相对性原则：绝对安全可靠的移动智能终端并不存在，故此，移动智能终端的信息安全应适度，不能偏离实际情况而片面追求绝对安全，应采用分类分级的方法针对性地提高移动智能终端的信息安全能力。
- 目的性原则：移动智能终端的信息安全设计应有目标、有重点地实施，例如商业用户更关注移动电子商务应用安全；政府官员更关注信息泄密；普通用户更关心吸费问题。而面面俱到的信息安全的移动智能终端并不存在。故此，需要对移动智能终端信息安全进行一定程度分类，有重点地加强移动智能终端信息安全。
- 扩展性原则：移动智能终端的信息安全形势以及对应安全技术是不断发展的，在一段时期内，信息安全发挥了其应有的作用，达到一定平衡，但一旦有安全攻击技术超越安全防护，新的安全周期就要重复开始。故此，移动智能终端信息安全应具备充分的扩展性。
- 易用性原则：移动智能终端的主要特点就是人机友好，易于掌握和使用灵活，安装卸载应用软件方便，任何信息安全措施都不能严重影响移动智能终端的易用性。故此，移动智能终端的信息安全措施基于其易用性，达到安全性和易用性的平衡。

5 设计思路

图1所示为移动智能终端信息安全解决方案。首先需要了解移动智能终端所要面临的安全威胁和攻击，进而在安全目标约束下分析相应的安全需求，形成安全机制，最后研制开发需要的安全技术和功能。

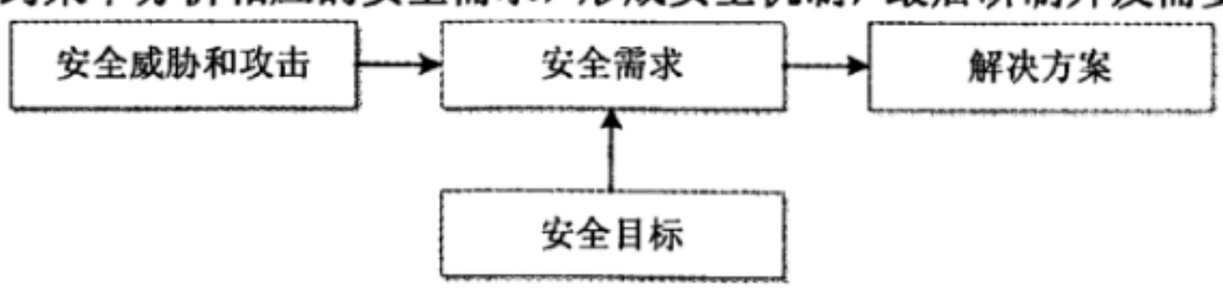


图1 移动智能终端信息安全解决方案

6 安全威胁和攻击

6.1 硬件安全

硬件是移动智能终端的基础，硬件安全问题往往会给移动智能终端造成极大的安全威胁，应引起足够的重视。如硬件芯片可能内置系统漏洞或者后门程序，从而可以被远程维护乃至控制。此外，部分移动智能终端的智能卡算法存在一定的漏洞，存在被克隆的风险，克隆后的智能卡可以用来拨打电话，以致造成机主的话费损失；同时可以接听部分电话和短消息，造成机主漏接电话和漏收短消息，乃至关键短消息被截获。

6.2 操作系统安全

操作系统是系统软件中最核心的部分，其安全问题是整个移动智能终端安全问题的关键。与通用操作系统相比，移动智能终端的操作系统在存储管理、设备管理、文件管理、API 调用和系统服务等方面都有较大区别，其中最为典型的就是其开放性，用户在开发应用程序时可调用某些敏感 API，给移动智能终端安全带来威胁。此外，操作系统的系统漏洞和后门程序是移动智能终端的典型安全威胁。

6.3 接口安全威胁

移动智能终端接口安全威胁主要来源于空中接口和外围接口。

对于移动智能终端，用户数据/信令均通过无线信号在空间进行传播与基站进行通信，因此用户数据存在在空间被截获的风险。用户的通话、短消息等个人私密内容均有被攻击者在空口被窃听的威胁。

此外，移动智能终端上具有 WiFi（基于 IEEE 802.11 系列协议的无线局域网）、USB、蓝牙、红外线、NFC 等多种外围接口。通过这些接口，移动智能终端能够与其他设备进行数据交互、同步，但也带来通信数据被截取、恶意代码传播攻击、支付安全等安全隐患。

6.4 应用层安全威胁

随着移动互联网和移动智能终端的融合，移动智能终端的应用协议也越来越丰富，带来了与应用内容及应用协议相关的安全问题。首先，由于移动智能终端操作系统的开放性，可根据自己的需求对其进行定制开发，因而其内嵌的文字、图片、音视频和互联网链接等数字内容可能会出现预置违法违规数字内容以及包含恶意扣费、隐私窃取等行为的链接等问题。其次，移动智能终端预置应用软件可能存在恶意扣费、隐私窃取等恶意行为，给用户信息安全造成威胁。再次，由于移动智能终端应用越来越丰富，其协议是否完善、协议是否具有足够的健壮性，也有待进一步验证。这里的协议健壮性是指针对移动智能终端上的应用层协议（包括基于应用内容的数据、图片、音频、视频等传统应用层协议以及由于移动互联网、云计算等新技术发展产生的新型应用协议，如 HTML5、Web2.0、浏览器相关协议等），根据不同场景发送异常的协议报文，移动智能终端仍能正常工作的能力。

6.5 用户信息安全威胁

移动智能终端更新换代比较快，当用户需要更换移动智能终端时，旧的移动智能终端中存储的个人私密信息存在泄露的安全风险。目前很多手机在删除用户电话簿、短消息等信息时仅仅是删除了文件的索引，并没有实际覆盖掉原来的信息，当移动智能终端流落到别处时，就存在被攻击者恶意恢复移动智能终端上所有私密信息的风险，导致用户私密信息被泄露。

其次，移动智能终端与计算机相连，通过电脑上的客户端可以备份电话薄、短消息等，也存在用户信息泄露的风险，而且现在越来越多的互联网公司提供云存储功能，也存在用户信息泄露的风险。

再次，用户随身携带移动智能终端，有时移动智能终端放置在某些地方，如开会放在会场、上班放在办公桌上，在用户暂时离开的时候，用户移动智能终端上的信息（电话簿、短信、日程安排等）就存在被泄露的风险，这可能导致一些商务机密被泄露，给用户造成巨大的损失。因此需要研究如何安全存储用户机密信息，如何控制移动智能终端内信息不被非法访问。

此外，移动智能终端很大的一个安全问题是容易丢失、被盗。移动智能终端中存储的个人私密信息很多，因此移动智能终端丢失、被盗容易造成用户私密信息的泄露。除非移动智能终端已经由其拥有者设置了保护以禁止未经授权的使用，否则任何得到移动智能终端的人都能够与手机原来的所有者一样任意地查看手机信息。如果移动智能终端里面的机密信息（电话簿、短信、个人身份信息等）被他人获得并利用，则会给用户造成很大的损失。因此需要研究相应的安全机制来保护移动智能终端在丢失、被盗的情况下个人信息的安全处理。

6.6 终端刷机安全威胁

很多移动智能终端在出厂后还能够进行刷机操作，通过对移动智能终端刷机，有可能修改移动智能终端的协议栈，有可能给移动智能终端植入恶意代码，因此移动智能终端如果不限制出厂后的刷机操作会给移动智能终端带来巨大的安全威胁。

6.7 恶意代码安全威胁

移动智能终端应用软件上病毒、木马等恶意程序的泛滥，是移动智能终端安全威胁的重要来源。对于移动智能终端来说，由于采用了开放的操作系统平台，并且移动智能终端的处理能力大大增强，因此针对移动智能终端存在的各种漏洞，攻击者开发出的病毒越来越多，危害也越来越大。借助各种外部接口以及无线网络连接病毒传播的速度也越来越快。

病毒对移动智能终端本身可能带来的危害有：侵占终端内存导致移动智能终端死机关机、修改手机系统设置或者删除用户资料，致使软硬件功能失灵，手机无法正常工作。盗取手机上保存的个人通讯录、日程安排、个人身份信息、甚至个人机密信息，窃听机主的通话、截获机主的短信，对机主的信息安全构成重大威胁。自动外发大量短信、彩信、拨打声讯台、订购增值业务，导致机主通信费用及信息费用剧增。

病毒还可能导致终端对网络产生危害：向网络发起DoS/DDoS攻击，致使网络资源被耗尽，造成网络无法正常为用户提供服务。

6.8 垃圾信息安全风险

越来越多的垃圾短信、骚扰电话及不良信息的传播给用户带来巨大的困扰。非法的广告营销以及色情、反动等不良信息传播，对社会传统和青少年身心健康造成伤害，对社会造成巨大的安全威胁。

7 安全框架

7.1 移动智能终端安全框架

移动智能终端安全框架主要包括5个部分：最底层是终端硬件安全；之上为操作系统安全；顶层为应用软件安全；另外还有通信接口安全和用户数据安全，同时涉及操作系统和应用软件。具体如图2所示。

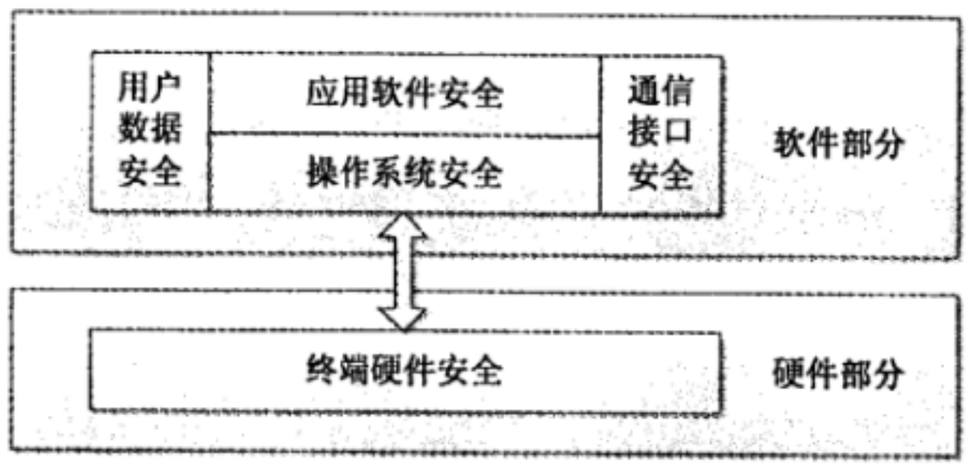


图2 移动智能终端安全能力框架

7.2 移动智能终端安全目标

应符合YD/T 2407-2013第4.2条。

8 安全要求

应符合YD/T 2407-2013第5章。

9 解决方案

9.1 终端硬件安全方案

移动智能终端存储芯片应具备完整性和机密性保护机制。完整性是指数据免遭非法更改或破坏的特性。机密性是指信息对于非授权个人、实体、或进程是不可知、不可用的特性。移动智能终端的数据存储区域一般分为系统引导部分、操作系统、通信协议栈、系统校验参数、密钥证书、用户存储空间以及系统保留空间等。为了实现对不同区域数据不同层次的保护，移动智能终端芯片应对存储区域进行划分，通过数据配置、地址配置、控制配置等手段实现对不同存储区域不同层次的保护。为了实现数据的完整性和机密性，移动智能终端存储芯片应将数据进行加密存储。本安全解决方案，对于系统引导部分、操作系统、通信协议栈、系统校验参数、密钥证书均单独划分存储区域，并采用硬件加密算法对数据进行加密存储。另外还应为用户存储区单独划分一个高安全级别的存储区域，同样使用硬件加密存储的方式进行数据的加密存储，用户可以通过人机界面对用户数据存储区域进行选择，将私人敏感数据存储在该特殊区域。

移动智能终端硬件应具备唯一可识别性，硬件标识不可被更改。这里的“不可被更改”有两种含义：一是硬件标识所写区域是不可被改写的；二是硬件标识区域可被改写，但改写是受控的，移动智能终端能够识别改写发生，并采取措施进行控制。

采取的措施包括提示用户硬件标识被非法修改，移动智能终端自动关机。

移动智能终端硬件标识包括IMEI号码（TD-SCDMA/GSM/WCDMA终端）、ESN号码（CDMA1X/cdma2000终端），或其它唯一标识移动智能终端芯片的号码。

移动智能终端SIM卡应提高防克隆能力，如有些运营商目前基于索引随机数方案增加对SIM卡进行安全鉴权的模块，以提高SIM卡防克隆能力。

9.2 操作系统安全方案

由于非法操作系统可能会影响用户使用并干扰正常网络运行，因此操作系统应当阻止一切非法的修改和刷新。

另外由于大多数的入侵都需要修改操作系统的内容，因此对操作系统进行完整性和一致性验证可有效地防止外部入侵。

实现操作系统完整性和一致性验证的一个有效方法是采用安全启动（secure boot）方式。附录A 介绍了使用RSA算法和MD5算法配合实现对软件系统文件验签的安全启动（secure boot）。

移动智能终端的中间层有很多的API开放给用户进行二次开发，如果完全开放所有的API则会给移动智能终端带来很大的安全风险，因此移动智能终端操作系统应具备API调用权限的分级控制功能，这样可有效防止应用越级调用API或非法调用API。

例如：

API的分类：通信控制类、多媒体类、显示类。

由于通信会涉及费用问题，因此为了避免吸费软件等恶意软件的流行，应将通信控制类API定为最高级别的API，只有高级授权用户才能够进行该类API的调用。

多媒体类及显示类主要涉及用户体验，可以将该类API定为二级API。

移动智能终端操作系统应具备监控开机自动启动程序的修改及变更的能力。有些应用软件在一开机时就需要自动启动，但也有病毒软件在用户不知情的情况下开机后自动启动并在后台运行。为了避免恶意软件的自启动，移动智能终端操作系统应具备开机自动启动程序的监控能力。移动智能终端应当在出厂时就维护一张开机自启动程序列表，当发现不在列表内的软件在开机时自动启动，则操作系统应能够给用户提示，在得到授权用户确认后才能够继续正常启动过程，并修改开机自起动程序列表。

9.3 应用软件安全方案

9.3.1 终端访问控制

由于移动智能终端、电信智能卡（SIM、USIM、R-UIM等）内存储了很多的关键参数及用户数据，因此移动智能终端有必要提供用户分级访问控制，对于不同级别的用户只能开放不同级别的内容。对于电信智能卡可以使用PIN码进行保护。通过将电信智能卡与移动智能终端进行绑定，也可以实现使用PIN码对移动智能终端的保护。对于移动智能终端本身应提供移动智能终端自身的密码/指纹识别保护。当移动智能终端处于待机状态时，可以使用相应的密码/指纹识别对移动智能终端进行锁定。

9.3.2 防病毒

移动智能终端杀毒功能是安装在移动智能终端中用于发现和处置手机病毒的能力，该功能仅适用于具有开放式操作系统的移动智能终端。事实上，无论如何提高移动智能终端的安全系数，移动智能终端都没有绝对的安全，特别是对于移动智能终端，由于用户能随意安装应用软件，故此感染病毒的可能性远大于普通移动智能终端，而防病毒软件则成为了保证移动智能终端安全的重要条件。由于开放式操作系统的多样性，针对不同的操作系统开发出的杀毒软件大相径庭，但至少应具备如下功能：

- 全盘扫描功能；
- 实时监控功能；
- 文件系统监控功能；
- 文件修复功能；
- 日志功能；
- 病毒库更新。

对于使用开放式操作系统的移动智能终端，在出厂时应预装杀毒软件，并且用户可以根据自己的需要来安装、卸载和更换相应杀毒软件。

9.3.3 防骚扰

骚扰电话、垃圾短信对用户带来很大的困扰，甚至影响用户的正常工作和生活，移动智能终端应提供软件或功能使用户能够按照自己的要求或设定的规则对来电进行过滤。移动智能终端应至少提供按照基于手机号码进行来电过滤的功能，包括黑名单和白名单两种形式。黑名单是指来自相应电话号码的通话都要被拦截；白名单是指只有来自相应电话号码的通话才允许通过。对于手机通信薄电话，默认为白名单。

移动智能终端应该支持单条或者成组添加黑白名单、单条或者成组删除黑白名单，并且支持黑白名单查询统计。同时，移动智能终端应支持对已拦截通话的统计、查询和删除。

移动智能终端应提供垃圾短消息过滤功能来屏蔽垃圾信息。移动智能终端至少应支持基于地址（包括手机通信簿）的垃圾短信过滤功能，具体应符合YD/T 2035的要求。

9.3.4 移动智能终端应用软件安装

移动智能终端应具备认证签名机制，能够阻止未签名的应用软件的自动安装，能够提示用户软件的签名状态。

9.3.5 其他业务

由于定位信息对于用户来说是涉及用户个人隐私和安全的信息，因此如果移动智能终端集成了定位功能，移动智能终端应能够限制定位信息的发送，只有授权用户才能够进行定位信息的处理和发送。对于发送定位信息，该软件应该可以对用户进行提示。

9.4 通信接口安全方案

9.4.1 话音通信安全

由于目前国内公众通信网络空中接口没有启用加密，因此为了保证电路域通话、短信的安全，移动移动智能终端可采用的安全解决方案是提供端到端的加密功能。语音通信是移动智能终端最基本也是最重要的基础业务之一，移动智能终端用户使用语音通信进行各种各样的活动，因此语音通信内容是用户的重要私密信息之一。通过端到端的语音加密功能，可有效提升用户语音通信的安全性。

加密方法可以采用硬件加密，也可以采用软件加密。

硬件加密需要在通话双方均增加语音加密模块来实现语音的加解密。

软件加密可以在通话双方选择同样的加密方法来实现语音的加解密。

语音加密安全功能仅仅为用户提供了一种加密的选项，仅当用户选择进行语音加密时，语音才经过加密模块或加密软件进行加解密过程。这种加密只能在通话双方均具备同样的加解密能力时才能够实现。

该安全解决方案适用于有加密需求的群体，比如使用公务手机的公司员工。

当移动智能终端接收到的短消息、多媒体消息包含特殊的处理功能，比如短消息包含特殊字符，多媒体消息包含可运行附件，移动智能终端不应自动执行相应的过程，而应给用户相应的提示，仅当得到授权用户确认之后才可执行相应的处理功能，这样可以在一定程度上防范病毒短息、彩信的发作。

9.4.2 数据通信安全

对于支持分组域的移动智能终端，在分组域的数据访问会给移动智能终端带来巨大的安全隐患。目前移动智能终端接入互联网的带宽越来越大，能够下载的应用服务也越来越多，随之而来给移动智能终端带来了巨大的安全隐患。为了加强分组域的安全性，提供以下分组域的安全解决方案：

移动智能终端提供对分组域应用程序的访问控制机制，只有授权应用程序才能够在程序运行过程中启动分组域连接。

移动智能终端应能够监测所有应用程序的分组域连接尝试,当出现分组域连接尝试时，移动智能终端能够发现该连接尝试并给用户相应的提示。

在分组域连接建立后，移动智能终端能够对分组域传输的数据进行监控，监控的内容包括数据传输的上下行流量，数据连接的对端地址。当移动智能终端支持IMS接入时，移动智能终端应支持通过分组域接入IMS时的安全要求，包括支持IMS-AKA认证机制，支持与P-CSCF间使用CK和IK建立IPsec安全通道。

9.4.3 无线外围接口

对于支持无线方式的外围接口（红外、蓝牙、其他短距离通信技术）的移动智能终端，为了保障外围接口数据通信的安全性，移动智能终端应具备物理开关，可开启、关闭蓝牙、红外等终端支持的所有除蜂窝移动通信制式外的其他无线接入方式。当无线外围接口建立数据连接时，移动智能终端能够发现该连接并给用户相应的提示，仅当用户确认建立本次连接时，连接才可建立。

对于支持WLAN接入的移动智能终端，为了保证WLAN接入的可控，移动智能终端应具备物理开关可以开启、关闭WLAN功能。当通过WLAN建立数据连接时，移动智能终端能够发现该连接并给用户相应的提示，仅当用户确认建立本次连接时，连接才可建立。移动智能终端应支持EAP-SIM/AKA等高安全强度的认证算法，在WLAN与3GPP网络融合场景下，应支持与PDG协商建立IPSec安全隧道。

9.4.4 有线外围接口

对于支持有线外围接口的移动智能终端，当有线外围接口建立数据连接时，移动智能终端应给用户相应的提示，仅当授权用户确认本次连接时，连接才可以建立。

9.4.5 外置存储设备

对于支持外置存储设备的移动智能终端，应严格限制重要和敏感数据不能存储在外置存储设备中。移动智能终端内置应用程序和授权第三方应用程序访问重要和敏感数据应进行严格的控制，确保非授权应用程序不能访问用户重要和敏感数据，同时保证所有授权应用程序不能将这些重要和敏感数据移动、复制、转存到外置存储设备中。

9.5 用户数据安全方案

移动智能终端应能够保护用户私密数据安全可靠的存储，不被非法获取，在各种情况下（更换手机、丢失、被盗）都能保证用户私密数据不被泄露。

为了保证用户数据安全可靠的存储，不被非法泄露，安全解决方案有：终端的一般数据与用户私密数据放置在存储芯片互相隔离的区域内，在终端放置用户私密数据的存储区域内，未获得授权或非法的程序不可访问该区域内的内容。终端使用加密功能，对真实的用户私密数据加密后再放置于存储区域内，即使出现存储芯片被拆卸，或其他防御机制被非法程序绕过，出现该存储区域内的数据内容被访问到的情况，也无法仅从访问到的数据中还原出用户私密数据的真实内容。

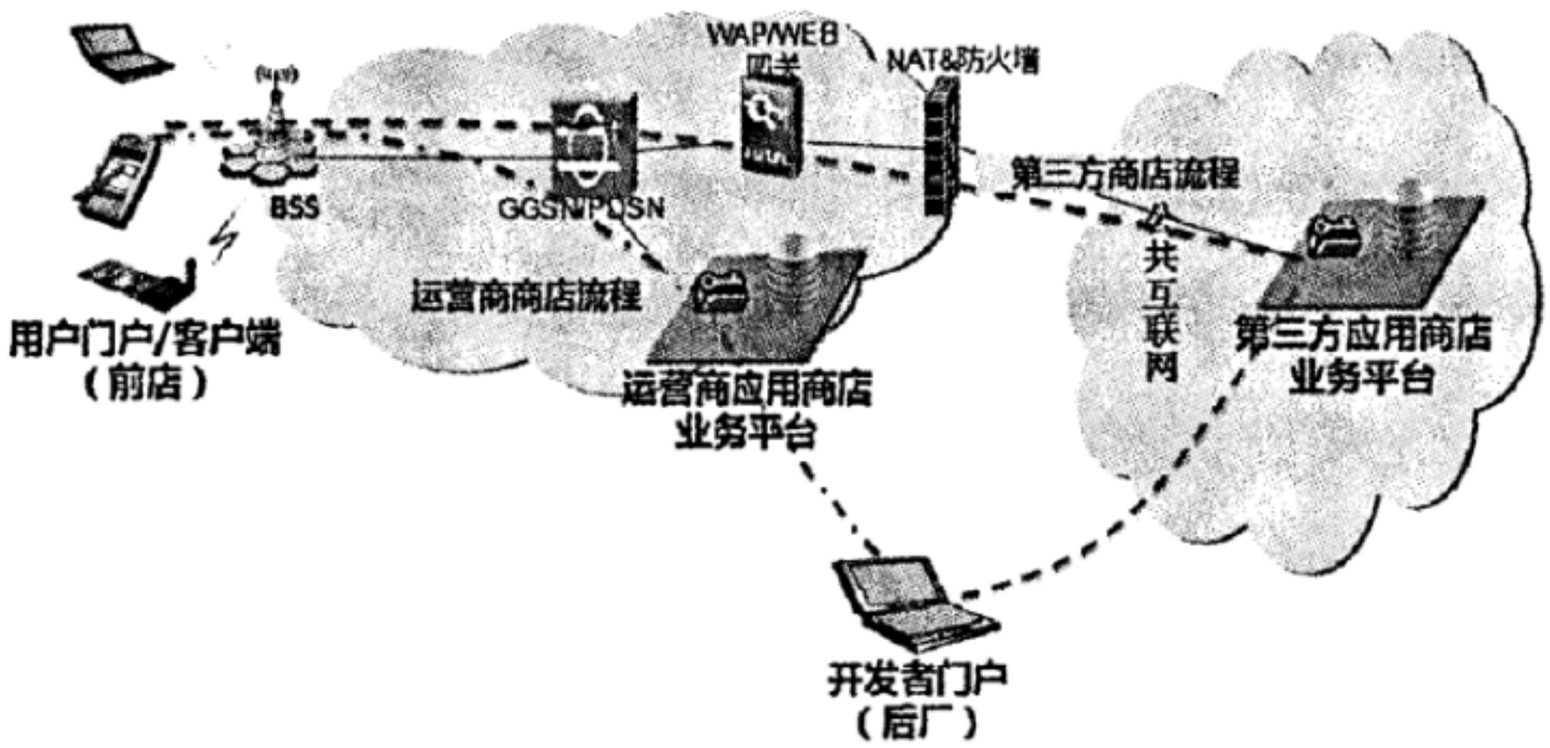
移动智能终端提供数据彻底删除功能，以保证被删除的用户数据不可再恢复出来。一般的删除功能仅会删除数据在存储器件中放置位置的索引，而该区域内实际存储的数据没有完全清空，在数据被删除之后，非法程序通过读取该区域的内容，仍有可能从读取到的数据中恢复被删除的私密数据。彻底删除功能应把该区域内实际存储的数据彻底消除。可在对应的存储区域使用全“0”或全“1”进行填充。

移动智能终端丢失、被盗后的用户数据安全保护，移动智能终端提供用户数据的远程保护功能，以便用户在手机遗失或其他情况下，终端中的用户数据不被泄露。包括远程锁定移动智能终端、远程取回用户数据、远程销毁用户数据。移动智能终端提供的远程保护功能也应具备安全设置，确保远程保护功能仅在达到了用户预设条件的情况下才会启动。

附 录 A
（资料性附录）
应用软件商店安全分析和安全措施

A.1 应用软件商店安全分析

应用软件商店是指以互联网、移动通信网等信息网络为通道，为移动智能终端提供应用软件、数字内容等产品的交易服务平台。应用软件商店一般由移动智能终端制造商、网络运营商或者第三方运营商运营。其网络架构和系统结构如图A.1所示。



注：

BSS	基站子系统	Base Station Subsystem
GGSN	网关 GPRS 支持节点	Gateway GPRS support node
NAT	网络地址转换	Network Address Translation
PDSN	分组数据服务节点	Packet Data Serving Node
WAP	无线应用协议	Wireless Application Protocol

图A.1应用软件商店的网络架构

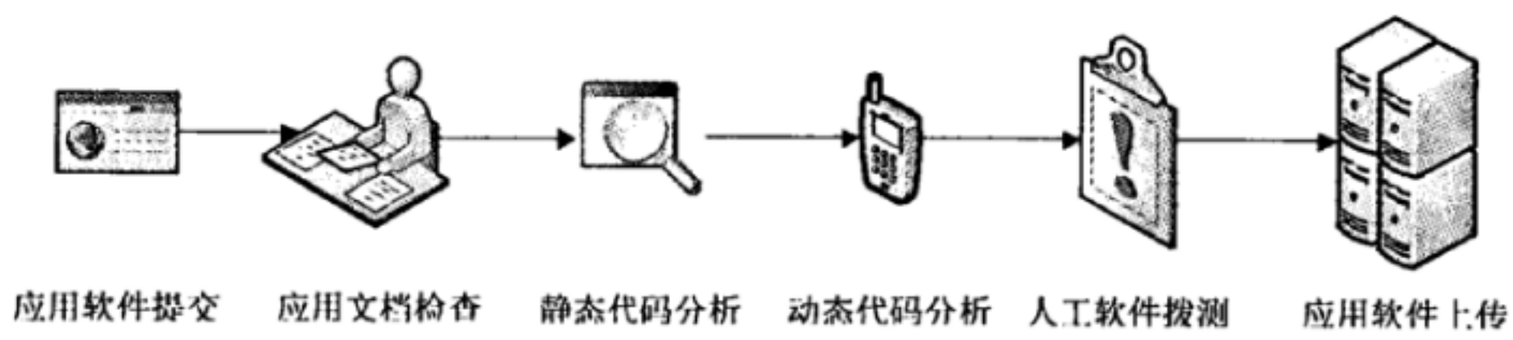
应用软件商店作为一种移动应用内容的发布渠道，在促进移动互联网业务蓬勃发展的同时，也带来了一些潜在的安全隐患，最常见的是不法分子利用这个渠道传播包含吸费陷阱、僵尸病毒、手机木马等恶意代码，损害用户信息安全和利益。其根源在于移动智能终端的开放软件平台架构。虽然开放软件平台架构为第三方应用软件的开发和使用带来了极大方便，但操作系统本身安全漏洞、后门的存在容易被恶意的应用开发者所利用，从而对用户的信息安全、网络安全带来隐患。恶意程序可以借助终端软件系统的安全漏洞破坏、散播用户数据，甚至借助木马程序调动感染的终端发起对移动网络、网络中特定目标的攻击。恶意程序还可以通过终端操作系统的“后门”对终端进行远程控制、窃取信息。由于除移动智能终端预置应用软件之外，基本上都来自于应用软件商店，故此，非常有必要加强应用软件商店的安全措施，避免恶意代码散播到用户移动智能终端。

A.2 应用软件商店安全措施

应用软件商店信息安全措施主要由技术手段和管理手段共同构成。技术手段主要目标是审核和验证提交到应用软件商店软件的合法性；而管理手段主要目标是验证开发者的资质以及对非法行为的惩罚措施。具体如下：

A.2.1.1 应用软件审核和验证过程

对第三方应用软件审核主要是由一系列应用软件审核和验证环节构成，具体如图A.2所示。



图A.2第三方应用软件审核和验证过程

相应环节的说明如下。

a）应用软件提交：第三方开发者可以通过应用软件商店开放的提交接口来提交应用软件。首先，第三方开发者往往需要在应用软件商店注册；之后，第三方开发者就可以按照应用软件商店的格式要求提交应用软件，提交应用软件同时需要提交说明文档（包括应用软件的功能说明、API调用、开放区域等）。

b）应用文档检查：该项检查主要针对软件功能、API调用以及第三方开发者的资质等进行审核。一旦没有通过审核，则应用程序不被接受。

c）静态代码分析：静态代码分析在不运行代码的方式下，通过词法分析、语法分析、控制流分析等技术对程序代码进行扫描，验证代码是否满足规范性、安全性、可靠性、可维护性等指标的一种代码分析技术。静态代码分析可以帮助应用软件商店管理者查找代码中存在的结构性错误、安全漏洞等问题，从而保证软件的整体质量。静态代码分析主要具有以下特点：

- 静态分析不运行代码只是通过对代码的静态扫描对程序进行分析。
- 检测速度快、效率高，目前成熟的代码静态分析工具每秒可扫描上万行代码的特点。
- 代码静态分析是通过对程序扫描找到匹配某种规则模式的代码从而发现代码中存在的问题，这样可能存在漏洞的函数，有时会造成将一些正确代码定位为缺陷的问题，因此静态分析有时存在误报率较高的缺陷，可结合动态分析法进行修正。

d）动态代码分析：动态分析是通过在模拟测试环境中执行程序进行程序分析的方法。为了使该测试全面有效，被测程序应有足够的输入来产生有意义的行为。动态代码分析主要具有以下特点：

- 动态代码分析完全依赖于模拟测试环境，并且模拟测试环境对测试结果有一定影响；
- 由于输入有限，动态代码分析存在比较高的漏报率。

e）人工软件检查：人工把软件安装在移动智能终端上进行测试，测试一般有针对性，并且对测试人员经验要求比较高，主要用于查找以上测试环节中发现不了的信息安全问题。

A.2.1.2 第三方应用软件在线监测

不定期下载安装应用软件进而监测应用软件是否有恶意行为或者非授权使用信息系统。

A.2.1.3 应用软件商店管理手段

为了保证用户的合法权益和收集应用软件使用情况，应用软件商店管理者应给用户提供反馈平台。该平台的主要目的是发现恶意软件，同时也可以对性价比高的应用软件进行评定。当发现恶意软件时，首先该应用软件要被下架，同时开发者也会被处以行政或者经济处罚，甚至于账号被删除。

参 考 文 献

[1] YD/T 1699-2007　移动终端信息安全技术要求
[2] YD/T 1700-2007　移动终端信息安全测试方法
[3] YD/T 1760-2008　数字移动终端外围接口数据交换
[4] YD/T 1886-2009　移动终端芯片安全技术要求和测试方法
[5] ITU-T X.1126　智能手机安全
[6] ITU-T E.408　电信网络安全需求
[7] ITU-T X.supl.19　ITU-T X.1120 series - Supplement on security aspects of smartphones

中华人民共和国
通信行业标准
移动智能终端信息安全设计导则
YD/T 2674-2013
*
人民邮电出版社出版发行
北京市丰台区成寿寺路11号邮电出版大厦
邮政编码：100164
宝隆元（北京）印刷技术有限公司印刷
版权所有　不得翻印
*
开本：880×1230　1/16　　2014年7月第1版
印张：1.5　　2014年7月北京第1次印刷
字数：34千字
15115·362
定价：20元
本书如有印装质量问题，请与本社联系　电话：(010)81055492