**移动终端安全问题分析与解决方案研究**

发表时间：2012/9/10 [付皓](http://www.e-works.net.cn/commsearch.aspx?author=%b8%b6%f0%a9) [戴国华](http://www.e-works.net.cn/commsearch.aspx?author=%b4%f7%b9%fa%bb%aa) [刘兆元](http://www.e-works.net.cn/commsearch.aspx?author=%c1%f5%d5%d7%d4%aa) [赵强](http://www.e-works.net.cn/commsearch.aspx?author=%d5%d4%c7%bf) 来源：万方数据

关键字：[移动终端安全](http://tag.e-works.net.cn/tagsearch.aspx?tag=%d2%c6%b6%af%d6%d5%b6%cb%b0%b2%c8%ab) [可信移动平台](http://tag.e-works.net.cn/tagsearch.aspx?tag=%bf%c9%d0%c5%d2%c6%b6%af%c6%bd%cc%a8) [用户卡](http://tag.e-works.net.cn/tagsearch.aspx?tag=%d3%c3%bb%a7%bf%a8) [端到端加密](http://tag.e-works.net.cn/tagsearch.aspx?tag=%b6%cb%b5%bd%b6%cb%bc%d3%c3%dc)

[信息化调查](http://www.e-works.net.cn/survey/survey.htm)[找茬](http://community.e-works.net.cn/userhome/MyAdvice.aspx?title=%D2%C6%B6%AF%D6%D5%B6%CB%B0%B2%C8%AB%CE%CA%CC%E2%B7%D6%CE%F6%D3%EB%BD%E2%BE%F6%B7%BD%B0%B8%D1%D0%BE%BF_%BB%F9%B4%A1%D0%C5%CF%A2%BB%AF_%CE%C4%BF%E2)[投稿](http://community.e-works.net.cn/userhome/WebPost.aspx)[收藏](http://community.e-works.net.cn/ewk_business/myeworks/my-favorites2.aspx?htmlurl=http%3A//articles.e-works.net.cn/Security/Article100485.htm&type=viewarticle)[评论](http://articles.e-works.net.cn/Security/Article100485.htm#t1)[好文推荐](mailto:%E5%A5%BD%E5%8F%8B%E4%BF%A1%E7%AE%B1?subject=%E5%A5%BD%E6%96%87%E7%AB%A0%EF%BC%9Ahttp%3A//articles.e-works.net.cn/Security/Article100485.htm)[打印](javascript:print())[社区分享](http://community.e-works.net.cn/userhome/CommunityCreateShare.aspx?t=%u79FB%u52A8%u7EC8%u7AEF%u5B89%u5168%u95EE%u9898%u5206%u6790%u4E0E%u89E3%u51B3%u65B9%u6848%u7814%u7A76_%u57FA%u7840%u4FE1%u606F%u5316_%u6587%u5E93&u=http%3A//articles.e-works.net.cn/Security/Article100485.htm)

文章首先介绍了移动终端安全问题的现状，然后对造成移动终端安全问题的原因进行了详细的研究与分析，最后针对移动终端的特点提出了移动终端安全解决方案，以给用户营造安全的移动互联网环境。

**1 引言**

    随着移动互联网与移动终端产业的发展，移动终端上的应用日渐丰富，甚至有超过电脑终端应用的趋势。但是移动互联网的流行也使得传统互联网上存在着的各种安全问题逐渐延伸到移动互联网领域，甚至演化成为新的安全威胁，可以说移动互联网的特性决定了其受到的威胁要远远多于传统互联网。对于用户而言，不仅要面临诸如垃圾短信、欺诈短信的骚扰，还要面临经济上的损失、个人隐私泄露以及通信方面的障碍；对于移动运营商而言，这些安全威胁不仅会增加运营成本，还将大大降低用户的忠诚度；对于终端厂家而言，不得不面对用户各种投诉而增加服务成本。

**2 移动终端安全问题的分类**

    总体来说，由于功能手机扩展性小，所以面临的安全威胁也少；而对于智能手机来说，由于其有开放的智能操作系统，所以带来的安全威胁也较多。移动终端面临的安全问题大体可分为三大类：

**（1）第一类：用户卡自身及存储数据安全问题**

    包括三方面内容：第一方面是用户的鉴权安全；第二方面是用户卡中用户的数据安全；第三方面是基于用户卡的应用的安全。

**（2）第二类：移动终端自身及存储数据安全问题**

    包括五方面内容：第一方面是移动终端硬件安全；第二方面是移动终端操作系统安全；第三方面是移动终端中用户数据安全；第四方面是移动终端接入安全；第五方面是移动终端用户身份认证安全。

**（3）第三类：基于终端的业务应用安全问题**

    包括两方面内容：第一方面是语音类业务安全，主要是指语音通话过程中的安全问题；第二方面是数据类业务安全，主要是指短信、彩信、上网等数据类业务。

**3 造成移动终端安全问题的原因**

**3.1外围硬件接口安全控制不足**

    移动终端硬件的发展使得外围接口越来越丰富，外围接口提供了移动终端与外界接触的渠道，丰富了手机的应用；但同时也是引入危险的途径，无线接口可能在用户不知情的情况下被非法连通，并进行非法的数据访问和数据传送，造成私密信息的泄露，还可能造成病毒的传播。

    例如：谷歌此前承认，街景地图汽车在拍摄照片时收集了未加密的WiFi网络上的数据信息，这些信息中包含完整的电子邮件地址、网址和密码。

**3.2操作系统漏洞**

    操作系统是终端中最基本与最重要的软件，是终端运行的核心；但是各种操作系统或多或少都存在设计上的漏洞，这就会给使用者带来各种各样的安全威胁。从安全角度来说，操作系统是不可能百分百无缺陷、无漏洞的；另外程序人员或者操作系统的研发厂家也可能为自己的系统留有后门，这些都会成为安全的隐患。

    例如：Android的第一个浏览器重大漏洞，由一组安全专家（包括前NSA的计算机安全顾问CharlesA.Miller）发现。这个漏洞是由Android平台的网页浏览器引起的，它将允许一个恶意网站在浏览器内部安装一个软件，用来监视用户的键盘输入，从而窃取用户名和密码。

**3.3操作系统后门**

    大多数移动终端操作系统厂家都留有自己的后门，厂家可以利用操作系统后门远程删除终端上的程序。其本质就是系统中未公开的通道，系统设计者或者其它人可以通过这些通道出入系统而不被用户发觉。

    例如：苹果前CEOSteveJobs曾经揭示该公司对其生产的每一台iPhone和iPodTouch都掌握有生杀大权，即通过一个内嵌的“killswitch”开关，可以停止或封杀任何公司、网店和iPhone用户的软件，只要它被认为是有害或是恶意的。

**3.4API滥用**

    操作系统为软件开发者提供了API，使第三方应用程序能够调用终端底层功能；如果软件开发人员利用API编写恶意代码，就会对终端造成威胁。

    例如：新浪微博的第三方软件API接口被人利用，通过CSRF漏洞制造了蠕虫病毒，这一病毒可以未经用户授权转发链接，而链接中包括的JS代码则有继续感染其他用户的危害。

**3.5用户数据存储/访问安全机制不足**

    由于其中存储了大量的用户机密信息，因此移动终端中用户数据的存储与访问机制就显得尤为重要，应根据数据与文件的敏感性对其进行分类，并对不同级别的数据、文件采取不同的安全措施。例如：对移动终端中的一些客户个人信息、SMS、MMS和通讯录等数据应该采用更高的安全机制。

**3.6恶意程序**

    恶意程序通常是指带有攻击意图所编写的一段程序，可以分成需要宿主程序的和彼此独立的两类。前者基本上是不能独立于某个实际的应用程序、实用程序或系统程序的程序片段；后者是可以被操作系统调度和运行的自包含程序。恶意程序主要包括：陷门、逻辑炸弹、特洛伊木马、蠕虫、细菌和病毒等。针对其自身特点，移动终端的恶意程序主要的恶意行为有：恶意扣费、远程控制、隐私窃取、恶意传播和资费消耗等，这些恶意行为在绝大多数情况下都没有经过用户同意或授权。

**3.7信令完整性保护/系统加密不完善**

    移动通信系统的主要安全威胁来自网络协议和系统的弱点，攻击者可以利用这些弱点非授权访问/处理敏感数据、干扰/滥用网络服务，给用户和网络资源造成损失。其主要威胁形式有：窃听、伪装、流量分析和破坏数据完整性等。所以，信息的完整性保护或者系统加密的不完善，有可能造成通信过程中的安全问题。

    例如：GSM网络的通话有可能被窃听，就是因为有人成功破解了GSM网络中使用A5/1加密技术加密的信息。

**4 移动终端安全解决方案**

    终端安全是近几年随着智能终端的普及才被大家关注的一个话题，从目前的行业发展状况看，以网秦、腾讯、360为代表的一些安全软件公司已经推出了一系列的终端安全类软件，例如：网秦安全、网秦助手、360手机卫士、QQ手机管家等。这些安全类软件提供了包括查杀毒、恶意扣费、垃圾短信/骚扰电话拦截和私密空间等功能。应该说，各厂家的方案和思路都是采用客户端方式提供杀毒与客户信息的保护功能。

    但是，终端安全是一个综合问题，仅依靠第三方软件的方式并不能解决所有终端安全问题，例如移动终端被盗后的位置追踪、通话被窃听、用户进行数据业务时传输内容被截获等。所以，有必要从多个角度来对移动终端的安全解决方案进行研究。

**4.1可信移动平台MTM**

    可信移动平台MTM（MobileTrustedModules），包括硬件、软件及协议三个部分，主要思路是在硬件平台上引入具有安全存储和加密功能并且可抵制篡改的可信平台模块（TrustedPlatformModule），通过其提供的安全功能使非法用户无法更改其内部数据，从而确保身份认证和数据加密的安全性，提高终端系统的安全，如图1所示。

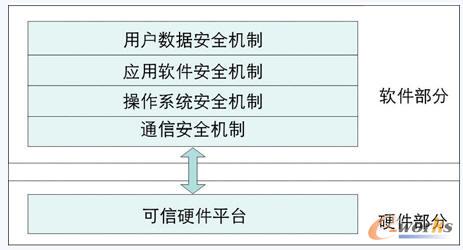
[[](http://articles.e-works.net.cn/articles/articleimage/20129/129914804421560438_new.jpg) [http://articles.e-works.net.cn/articles/images/zoom.gif](http://articles.e-works.net.cn/articles/articleimage/20129/129914804421560438_new.jpg)](http://articles.e-works.net.cn/articles/articleimage/20129/129914804421560438_new.jpg)

图1

    可信移动平台的可信计算是通过在终端上绑定一个可信计算模块TPM来保证现有终端的安全性，其主要手段是进行身份确认，使用加密进行存储保护及使用完整性度量进行完整性保护。其基本思想是在系统中首先建立一个信任根，再建立一条信任链，一级测量认证一级，一级信任一级，把信任关系扩大到整个系统，从而确保系统的可信。TPM实际上就是在系统里面加入了一个可信第三方，通过可信第三方对系统的度量和约束来保证系统可信。

    一个可信平台要达到可信，最基本的原则是必须真实报告系统的状态，同时决不暴露密钥和尽量不表露自己的身份。这就需要三个必要的基础特征：保护能力（ProtectedCapabilities）、证明（Attestation）、完整性度量存储和报告（IntegrityMeasurement,StorageandReporting）。

    国际TCG组织2010年发布了MTM（MobileTrustedModules）规范，将可信计算技术在智能手机等移动终端平台上的应用进行了规范。该规范考虑了可信计算技术应用于嵌入式系统的特点，根据移动应用的需求定义了支持移动终端应用的新的命令和数据结构以实现可信计算的安全功能。

**4.2移动终端安全管理控制平台**

    移动终端安全管理控制平台是为客户打造的一个终端安全及管理的综合服务平台，帮助用户解决操作系统漏洞安全问题、移动终端远程信息安全管理问题，同时可以为终端厂家、运营商等提供可用于决策的数据，见图2。

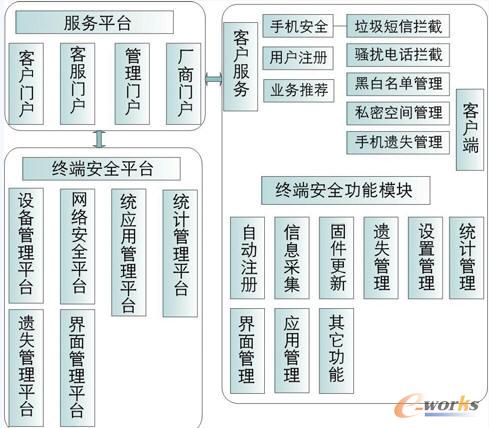
[[](http://articles.e-works.net.cn/articles/articleimage/20129/129914804502855088_new.jpg) [http://articles.e-works.net.cn/articles/images/zoom.gif](http://articles.e-works.net.cn/articles/articleimage/20129/129914804502855088_new.jpg)](http://articles.e-works.net.cn/articles/articleimage/20129/129914804502855088_new.jpg)

图2

    移动终端安全管理控制平台包括3部分：

    （1）服务平台，包括：客户门户、客服门户、管理门户和厂商门户，主要是供客户、客服人员、厂家人员以及管理人员登录的门户。

    （2）终端安全平台，包括：设备管理平台、网络安全平台、应用管理平台、统计管理平台、遗失管理平台和界面管理平台等业务实现平台，是整体安全功能的实现平台，与客户端配合实现各项功能。

    （3）客户端，是运行在终端中直接与客户进行交互的软件。安装客户端后，终端就具备自动注册、信息采集、固件更新、遗失管理、设置管理、统计管理、界面管理、故障诊断和应用管理等功能，每个功能作为一个独立的功能模块存在，并且可以进行扩充；对用户来说，用户可以根据客户端提供的菜单项使用相应的安全功能。客户端与终端安全平台配合实现各项功能。

    以管理员通过移动终端安全管理控制平台进行终端信息采集为例，来介绍一下信息采集的过程，如图3所示：

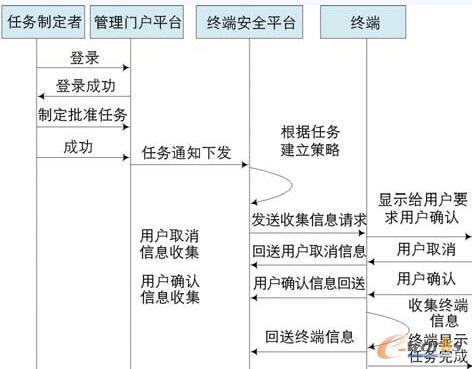
[[](http://articles.e-works.net.cn/articles/articleimage/20129/129914804573179110_new.jpg) [http://articles.e-works.net.cn/articles/images/zoom.gif](http://articles.e-works.net.cn/articles/articleimage/20129/129914804573179110_new.jpg)](http://articles.e-works.net.cn/articles/articleimage/20129/129914804573179110_new.jpg)

图3

**4.3基于用户卡的安全业务平台**

    终端使用的用户卡是全球唯一的，每张卡仅对应一个用户，所以用户卡可以成为终端用户天然的身份识别工具。可以通过用户卡卡号识别用户身份，并且可以利用用户卡存储用户的银行帐号、数字证书等标识用户身份的有效凭证。不仅如此，用户卡还可以用来实现加密算法、数字签名、公钥认证等移动支付领域必备的安全手段。由于用户卡是可控并且安全的，所以可以基于用户卡为移动支付等业务提供安全平台，解决移动支付等业务应用过程中的一系列安全问题，如图4所示。

[[](http://articles.e-works.net.cn/articles/articleimage/20129/129914804646063279_new.jpg) [http://articles.e-works.net.cn/articles/images/zoom.gif](http://articles.e-works.net.cn/articles/articleimage/20129/129914804646063279_new.jpg)](http://articles.e-works.net.cn/articles/articleimage/20129/129914804646063279_new.jpg)

图4

**4.4语音/数据端到端加密**

    前面说到，3G移动通信系统的主要安全威胁来自网络协议和系统的弱点，攻击者可以利用这些弱点非授权访问/处理敏感数据、干扰/滥用网络服务。所以有必要建立一种机制，为所有的数据和语音通信提供完整的端到端加密（在发送端使用加密算法对语音/数据进行加密，在接收端使用解密算法对语音/数据进行解密），保证加密后的用户信息在移动网内的任意中间节点（基站、基站控制器、交换机等）均以密文传输，避免在链路加密中出现的密文在通信节点落地的情况，从而有效防止通信双方的信息被窃听、篡改，安全性将大大优于采用链路加密的保密通信系统。

    目前在国内三大运营商中，中国电信已经推出基于语音加密的加密通信业务，其基本原理就是在终端中增加加密模块，实现对语音的加解密，如图5所示；并且采用加密短信的方式交互密钥，通话一次一密，密钥通过密钥管理中心来分发。除了语音加密，还可以利用该系统，或者重开发新系统对数据类信息（SMS、MMS等）进行加密，从而实现语音/数据的端到端加密。

[[](http://articles.e-works.net.cn/articles/articleimage/20129/129914804727817955_new.jpg) [http://articles.e-works.net.cn/articles/images/zoom.gif](http://articles.e-works.net.cn/articles/articleimage/20129/129914804727817955_new.jpg)](http://articles.e-works.net.cn/articles/articleimage/20129/129914804727817955_new.jpg)

图5

**5 结束语**

    随着移动互联网时代的到来以及智能终端的普及，移动终端将成为人们日常生活中必不可少的设备；移动终端给人们生活与通信带来革命性便利的同时，一些安全风险也随之浮出水面并迅速蔓延。可以预见，移动终端的安全问题未来将成为一个普遍的社会问题，它不仅会影响个人生活，还会带来不同程度的经济损失。所以，有必要在移动终端的安全问题全面爆发之前对该问题进行详细分析与研究，并找到行之有效的解决方法，为用户营造安全的移动互联网环境。