doi:10.3969/j.issn.1003-3114.2016.02.01
引用格式:孙其博.移动互联网安全综述[J].无线电通信技术,2016,42(2):01-08.

移动互联网安全综述

孙其博
(北京邮电大学,北京 100876)

摘　要: 移动互联网是传统移动通信网络与互联网融合的产物,能够为用户提供更具移动特性、更深入到日常工作生活的应用支撑。针对移动互联网的发展,在介绍移动互联网功能架构的基础上,从传统移动通信网以及传统互联网的角度简要介绍了移动互联网安全问题产生的根源,详细分析了移动互联网智能终端、接入网络以及应用服务面临的主要安全问题,提出了静态安全体系框架与动态主动安全防御相结合的移动互联网安全体系研究思路。

关键词: 移动互联网;智能终端安全;网络安全;应用安全;安全框架;态势感知
中图分类号: TP391.4　　**文献标识码:** A　　**文章编号:** 1003-3114(2016)02-01-8

Overview of Mobile Internet Security

SUN Qi-bo
(Beijing University of Posts and Telecommunications,Beijing 100876,China)

Abstract: Mobile Internet is a product from the fusion of mobile communication network and traditional Internet. It can provide users with the application support which has higher mobility and can penetrate into people's daily work and life. Based on introduction of functional architecture of mobile Internet,this paper describes in detail mobile Internet security problems and their origin. This paper analyzes in detail the main security challenges come from mobile devices,access network,application service,and puts forward the research thinking of mobile Internet security security system based on combination of static security architecture and dynamic active security defense.

Key words: mobile Internet; intelligent terminal security; network security; application security; security framework; situation awareness

0　引言

移动互联网已经成为人们社会生活中的重要网络。据统计,截至2015年6月底,我国网民总数达6.68亿人,其中使用手机终端上网的移动互联网网民达到5.94亿人[1]。

总体而言,当前移动互联网产业环境正在向着“去电信化”和“互联网中心化”的方向演进[2]。随之而来的是应用创新和模式创新正在取代技术颠覆成为移动互联网产业发展的显著特征。

然而随着快速发展,移动互联网也面临着与日俱增的安全威胁以及安全保障方面的挑战,对于其安全技术的研究具有重要的现实意义,需要尽早提出相应的解决方法。

1　移动互联网的定义与技术体系

移动互联网是指互联网的技术、平台、商业模式和应用与移动通信技术结合并实践的活动的总称[3]。中国工业和信息化部电信研究院在《移动互联网白皮书(2011年)》[4]。中指出:“移动互联网是以移动网络作为接入网络的互联网及服务,包括3个要素:移动终端、移动网络和应用服务。”

一个简单的移动互联网的拓扑结构如图1所示。在该模式下,用户使用移动智能终端,通过将传统移动通信网络(包括2G/3G/4G网络)或者通过无线通信网络(包括WLAN、WiMax等网络)作为接入网络,来访问传统互联网中提供的各类能够提供

收稿日期:2015-11-11
基金项目:国家自然科学基金项目(61571066)
专家简介:孙其博(1975—),男,博士,副教授,硕士生导师,教育部新世纪优秀人才,主要研究方向:下一代网络与网络智能化、服务计算与服务安全技术,获国家科技进步二等奖1项,发表SCI/EI检索论文90余篇,专著3本,专利41项,在研国家自然科学基金1项,省部级项目2项,国防科研项目1项。

满足其个性化服务需求的可移动、可定制的应用。

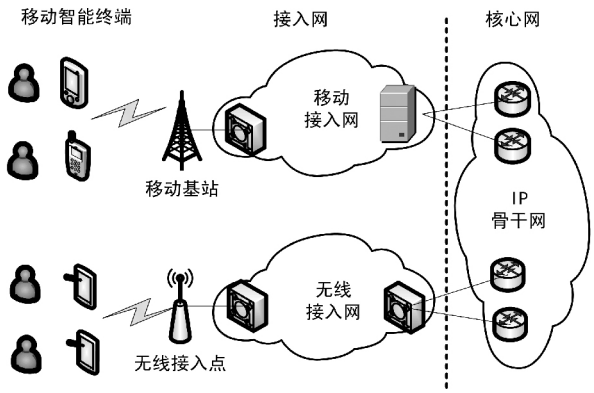

图1 移动互联网拓扑结构示意图

移动互联网的技术体系有3个水平功能层面，分别为云(即应用与服务功能层面)、管(即网络功能层面)、端(即移动智能终端功能层面)和1个垂直功能层面(即安全与隐私保护功能层面)，如图2所示[5]。

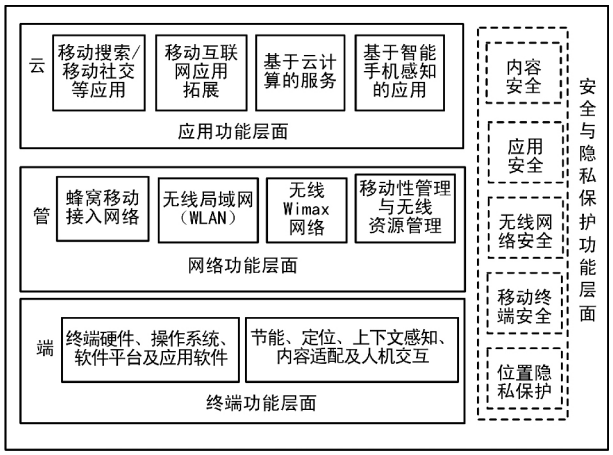

图2 移动互联网的技术框架

1.1 智能终端功能层面

随着信息技术的不断发展，移动智能终端已成为人们日常工作生活中关系最密切的电子设备。

通过将电信服务和互联网服务聚合在一个终端设备中，移动智能终端不仅具备了普通移动终端的语音通话、电信服务和移动性管理能力，而且具有了类似于计算机的处理能力和网络功能，以及更为强大的信息处理和存储空间。

目前，移动智能终端技术已成为影响移动互联网产业发展的最为关键的技术之一。其研究范围包括终端硬件、操作系统和应用软件技术，以及终端定位、节约能耗、上下文感知、内容适配和人机交互等技术。

1.2 网络功能层面

移动互联网的网络主要包括两部分：接入网和核心网。其中移动互联网的核心网是IP骨干信息传输网络，而其接入网络则以传统移动通信网络的接入网络以及无线城域网、无线局域网为主，此外还可以包括卫星通信网络以及使用蓝牙技术的无线个域网。这些采用不同技术体制的接入网络在带宽、覆盖、移动性支持能力和部署成本等方面各有长短[5]。例如，传统移动通信网络的接入网虽然具有移动性管理技术成熟和覆盖范围较大的优势，但却存在着成本过高、带宽较低等缺陷；而无线局域网虽然具有成本较低和带宽较高的优势，但又存在着移动性管理技术还不成熟和覆盖范围有限等缺陷。

移动互联网的高速发展使得接入网络所需要支撑的应用已转变为包含语音、数据、图像在内的多媒体应用，并且需要满足在所需带宽、覆盖区域以及实时性等多个方面的需求。

2 应用服务功能层面

移动互联网以“移动”和“开放”作为主要的发展特征，辅以应用商店引发的应用提供模式的创新，大规模地推动了应用市场的繁荣。

移动互联网的应用具有移动性和个性化等属性：比如用户可以随时随地获得根据其位置、兴趣偏好和环境特征等需求因素进行定制的具有个性化特征的移动互联网应用。而且随着业务和终端平台深度融合的趋势日益明显，移动智能终端对业务能力的支持程度将直接影响移动互联网业务的推广和普及[6]。

目前，移动互联网上的应用发展迅速，移动搜索、移动社交网络、移动电子商务、移动办公应用、智能导航应用等在内的多种应用正得到蓬勃发展。

3 安全与隐私保护功能层面

互联网自被使用以来，安全与隐私保护问题就一直困扰着人们。而与互联网的融合，使传统移动通信网的安全属性也受到很大的冲击。伴随移动互联网的业务多样化、网络开放化、终端智能化等技术特点的变化，安全与隐私保护问题也会出现新的特征，并提出更高的防护需求。

移动智能终端具有终端智能化、服务个性化等特征，更使得安全与隐私保护成为了移动互联网所必须解决的一大紧迫问题。与传统终端不同，移动智能终端与生俱来的用户紧密耦合性决定了其信息

的敏感性，而其具有的移动特性又对于信息安全的保护提出了更高的要求[7]。

4 移动互联网安全问题产生的根源

随着移动互联网的爆炸式发展，受经济利益驱动，移动互联网面临的安全威胁也在近几年迅速增长[8]。究其问题产生的根源，可以从以下两方面进行分析。

(1) 传统移动通信网封闭式的安全模式被打破

传统移动通信网的建设采用“围墙花园”模式，具有网络平台相对封闭、信息传输和管理控制平面分离、网络行为可溯源、终端类型单一且非智能，以及用户鉴权严格的特点，因此安全性相对较高[9]。

但是，从移动通信的角度看，与互联网的融合在很大程度上削弱了传统移动通信网络原有的安全特性。首先，作为移动互联网的一部分，IP 化后的移动通信网逐渐开放了其原有的封闭体系，导致除了严格的用户鉴权和管理之外，原有的安全性优势所剩无几；其次，由于其应用环境的封闭性，移动通信网络中原有的 IP 化的电信设备、信令和协议较少经受安全攻击方面的测试，其安全性被作为一个缺省项对待，因此也存在着各种可能被有意或者无意利用的软硬件漏洞。其安全防护能力在面对来自互联网的各种安全威胁时，出现明显降低的情形。

(2) 传统互联网的安全问题被引入到移动互联网中

移动互联网作为互联网的一个组成部分，除了接入技术不同，在体系架构上并无本质区别，同样面临着传统互联网的种种安全威胁和挑战。

首先，产生移动互联网安全问题的总根源是其基于传统互联网的开放式 IP 架构。IP 架构使攻击者可以很容易得到网络拓扑，获得网络中任意重要节点的 IP 地址，可以对网络中某一节点发起漏洞扫描及攻击，截获并修改网络中传送的数据，导致网络数据安全没有保障。而且用户对网络不透明、鉴权不严格、终端未经严格鉴权的认证机制即可接入网络；网络对终端的安全能力和安全状况不知情、无法控制；用户地址也可以伪造，无法溯源[10]。

其次，从现有互联网角度看，在融合了传统移动通信网络后，由于大量引入了具有安全脆弱性或者安全漏洞的 IP 化移动通信设备(例如 WAP 网关、IMS 设备等)，同时又增加了无线空口接入模式，导致其产生了新的安全威胁。例如攻击者可以破解空口接入协议进而非法访问网络，可以监听和盗取空口传递的信息，也可以对无线资源和设备进行服务滥用攻击等[6]。

因此，传统互联网服务中信息传播和管控机制在很大程度上不能平滑过渡到移动互联网，信息安全和用户隐私保护已经成为移动互联网用户迫切关心和亟待解决的问题[11]。

5 移动互联网面临的主要安全问题分析

文献[12]中给出了一个简要的移动互联网的安全体系架构，如图 3 所示。

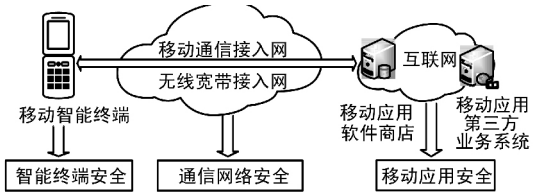

图 3 移动智能终端相关的安全架构

按照攻击发生的位置，对移动互联网的安全威胁可分为对移动终端的威胁、对无线接入网络的威胁和对移动应用的威胁。

5.1 移动智能终端层面临的安全问题

移动智能终端作为未来“无所不在”服务和个人信息的载体，具有移动性、多样性和智能性的特点，而附属于其上的各种应用则呈现出类型复杂、实现机制不公开、数量庞大的特点，这些因素叠加起来，导致其面临的威胁远大于以往[6]。

在表现形式上，移动智能终端的安全问题[8]主要聚焦在以下几个方面：其一是非法内容传播；其二是恶意吸费；其三是用户隐私窃取；其四是移动终端病毒以及非法刷机导致的黑屏、系统崩溃等问题。

下面以移动恶意代码和用户隐私窃取方面的问题为例对此进行说明。

(1) 移动恶意代码问题

由于移动智能终端操作系统在设计及实现上存在的疏忽，导致其或多或少都存在系统漏洞或者脆弱性，有可能会被恶意代码利用。尤其是随着移动互联网黑客技术的不断成熟，以移动智能终端为攻击目标的恶意代码已对其安全构成重大威胁。

移动恶意代码[13,14]是一种具有破坏性的恶意移动智能终端程序，一般利用短信、彩信、电子邮件和浏览网站等方式在移动通信网内传播；同时可利用红外、蓝牙等方式在移动智能终端间传播。

目前，移动智能终端操作系统市场占有率最高的是谷歌公司的 Android 操作系统，其次是苹果公

司的 iOS 操作系统和微软公司的 Windows Phone 操作系统等。随着智能终端操作系统的日趋统一，恶意代码将加速扩张，并由简单吸费向复杂的诱骗欺诈和流氓行为进化，呈现出多发趋势[15]。而且随着移动智能终端与银行账号、第三方支付等金融业务绑定的增加，手机病毒制作和传播正加速向资费消耗、恶意扣费和隐私信息窃取方向发展[12]。

尤其是随着基于 Android 操作系统的快速发展，使用该操作系统的移动智能终端日渐成为黑客攻击的主要目标。2015 年上半年，我国新增 Android 病毒包数达到 596.7 万，同比增长 1741%，感染用户人次达到 1.4 亿，同比增长 58%，其中手机支付病毒感染用户总数达到 1145.5 万[16]。

(2) 用户隐私窃取问题

伴随着移动互联网的普及和发展，用户对个人信息和网络隐私安全的关注程度也越来越高。与传统的个人计算机安全相比较，移动智能终端对用户的重要性更大。一般用户会将其私密、位置、金融等信息存储在移动智能终端中，由于这类信息的敏感性，使其遭受攻击的诱惑性更大，给用户隐私的保护带来了严峻挑战。

根据调研，相当多的移动智能终端在出厂时就被默认捆绑了很多应用，其中部分应用会在用户不知情的情况下收集用户的敏感信息和隐私信息，并且具有向其后门自动上传所收集用户信息的能力。比如，2012 年 11 月，某著名安全防护软件被发现主动收集诸如用户打开过的浏览页面地址等用户隐私信息，并且在用户不知情的情况下利用云端指令，在后台执行规定内容之外的功能[17]。

同样，导航应用几乎是每个智能移动终端用户必用的服务，但是用户在使用这类服务发布的一些位置数据也可能会泄露其位置隐私。比如央视在 2014 年曝光了苹果手机能够精准地记录用户使用过的定位服务功能及其位置的变化信息，包括他们的工作单位和家庭住址，甚至于包括每天去过什么地方、在该地方呆了多长时间的信息，这就涉嫌侵犯了用户的个人隐私。因为如果这些信息被不法分子得到，有可能会危及用户的财产和人身安全。

另外，在基于位置的服务中，还存在轨迹隐私泄露的问题。所谓轨迹，是指某个对象按时间顺序排列的位置序列[18]。通过大数据技术来分析对用户看似毫无用处的轨迹数据，就可能会泄露这些轨迹中含有的敏感位置信息，而依据这类敏感位置可能会得出令人吃惊的结果，比如可能会披露出用户的家庭住址、工作单位，甚至行为习惯、健康状况等更敏感的信息[19]。

但是另一方面，某些移动智能终端为了保护用户的通信隐私所采用的应用层加密技术，也给信息安全监管工作造成很大的挑战[20]。比如黑莓手机采用对数据进行加密后传输的方式来保证用户数据的安全，并且该手机使用的非公开加密算法的保密系数不低于银行数据系统。但是在 2008 年发生的孟买的恐怖袭击事件中，恐怖分子却正是利用了黑莓手机的加密功能逃避了印度政府监管。

5.2 网络层面临的安全问题分析

移动互联网具有的网络开放性、IP 化以及无线传输的特性，使安全成为其接入网以及核心网面对的关键性问题之一。但是受限于现有技术能力，移动互联网尚缺乏对隐藏在所传输信息中的恶意攻击进行识别与限制的能力。

按照攻击的方式，移动互联网的网络面对的威胁方式有窃听、伪装、破坏完整性、拒绝服务、非授权访问服务、否认使用/提供、资源耗尽等[21,22]，这些形形色色的潜在安全问题威胁着正常的通信服务。

(1) 传统移动接入网面临的安全问题

网络协议和系统的弱点是 3G 移动通信系统面临的安全威胁的主要来源，攻击者可以利用此类弱点实现非授权访问敏感数据、非授权处理敏感数据、干扰或滥用网络服务，进而对用户和网络资源造成损失[9]。以通用移动通信系统(UMTS)为例，在其安全机制中存在着许多的安全漏洞，攻击者利用这些漏洞能够对移动通信网发起诸如中间人攻击、流氓基站攻击和拒绝服务攻击等类型的攻击。

4G 移动通信系统由于其异构和基于全 IP 技术的体系结构，也会继承由于 IP 技术具有的特定安全漏洞而产生的安全问题。比如 LTE 的网络架构采用了全 IP 技术，与 GSM、UTMS 采用的网络架构相比，这种平坦的结构易受诸如窃听、注入、修改等方式的攻击，增大了泄露用户隐私的风险。此外，LTE 网络还容易受到 MAC 层位置跟踪、DoS 攻击、数据完整性攻击以及用户设备和移动设备的非法使用的影响。

除了上述来自网络协议和系统的弱点之外，下面以信令风暴攻击为例对移动接入网面临的运行类安全问题进行说明。

信令风暴攻击[23]是指短时间内针对基站和基站控制器(BSC)发起大量 SYN 扫描所导致的异常流量攻击行为。在这种攻击模式下，攻击者通过对

大量3G用户地址段发起SYN扫描攻击，能够同时激活大量的休眠用户，进而出现无线空口资源的负荷激增的问题。而由于传统移动通信网仅具有有限的无线空口资源，并且这些无线空口资源还要在其覆盖范围内进行共享，因而信令风暴攻击行为将严重影响到移动通信网的服务质量及用户体验。例如，某运营商曾发生过上千个3G用户在短短的10 s内同时登录一个基站，产生大量信令，引发相关设备出现最高负荷过高的问题。目前应对异常流量攻击的检测及封堵技术手段尚不能有效实现对SYN扫描攻击的拦截，在应对信令风暴攻击者对移动网地址段发起的SYN扫描攻击时，均具有其局限性，还不能有效地防范该类攻击。

(2) WLAN接入网面临的安全问题

WLAN技术采用公共的电磁波作为载体，具有标准统一、部署简单、性价比高的特点，同时又具有高灵活性和扩展能力强的特点，成为移动互联网接入的重要手段之一。但是由于其安全体制存在的缺陷，在认证与信息安全、网络安全等方面存在多项安全问题，使得其成为易被攻击和入侵的对象。

随着网络攻击技术的不断翻新，针对WLAN的攻击技术[24,25]中比较有代表性的包括针对秘钥的主动或者被动攻击、伪AP钓鱼攻击、利用DNS端口绕开计费问题、Web Portal安全问题、拒绝服务攻击、欺骗攻击和中间人攻击等等。

下面以针对秘钥的主动或者被动攻击以及分布式拒绝服务攻击为例对WLAN面临的安全问题进行说明。

在WLAN环境中，攻击者可采用主动方式或者被动方式截获用户秘钥。在采用主动攻击方式时，攻击者向接入特定WLAN的某个已知用户发送信息，比如通过有线互联网给某个用户发送电子邮件，然后通过比较加密前和加密后的数据包，就可以获得该用户的密钥。而当采用被动攻击方式时，攻击者只需要被动接收无线信号，并将所截获的加密信息与各种常用的提供未加密信息传输的网络传输协议及数据包格式进行针对性的比较就能获得密钥。

而拒绝服务攻击(Denial of Service，DoS)是指攻击者利用软件(含操作系统)的缺陷和协议的漏洞，通过抢占主机或网络的几乎所有资源的方式，使得合法用户无法获得相应的服务。拒绝服务攻击可以很容易被应用到WLAN接入网络。在这种攻击模式中，攻击者通过发送与WLAN相同频率的干扰信号来干扰无线接入网络的正常运行，进而导致正常的用户无法使用无线资源接入网络。拒绝服务攻击的另一种攻击手段是在短时间内发送大量的同种类型的报文[26]，比如发送大量的非法身份验证请求，此时无线访问接入点(Access Point，AP)会被攻击设备发送的攻击报文淹没，而无法处理正常的移动智能终端(合法用户)的报文请求。

在WLAN领域的安全标准主要是IEEE制定的802.11i标准和国内自主制定的WAPI标准，这两项标准都是用于解决无线接入段(即用户到AP)的认证和加密问题。其中，802.11i标准采用基于共享密钥的方式实现认证，并定义了更加严谨的加密算法，弥补了原有用户认证协议的安全缺陷，而WAPI采用基于数字证书的机制实现认证，并定义了国内自主的加密算法。综合而言，这两大标准在接入控制方面都存在比较明显的缺陷，各有优劣[27]。

5.3 应用层面临的安全问题分析

移动互联网带动了大批具有明显个性化特征，并且带有移动特色的创新型和融合型移动应用的快速发展。这类移动互联网应用一般都具有很强的信息安全敏感度，拥有如用户位置、通信录及交易密码等用户隐私信息。

移动互联网应用的上述特征与其潜在的巨大用户群的综合，导致其面临着更新的攻击目的、更多样化的攻击方式和更大的攻击规模[8]。

按照通行的分类方法，移动互联网应用面临的安全威胁[9]主要包括SQL注入、分布式拒绝服务(DDOS)攻击、隐私敏感信息泄漏、移动支付安全威胁、恶意扣费、恶意商业广告传播、业务盗用、业务冒名使用、业务滥用、违法信息及不良信息等。在内容安全方面，还面临着非法、有害和垃圾信息的大量传播，严重污染了信息环境，并且干扰和妨碍了人们对信息的利用。

此外，移动互联网应用平台由于软硬件存在的漏洞，也极易受到来自外界的攻击。而另一方面，由于进行安全防护将会给应用平台带来附加的检测支出，且不会带来额外收入，导致应用提供商通常缺乏为用户提供安全防护的意愿。

下面以移动互联网应用的发布推广和移动支付安全为例，对移动互联网应用层面临的安全问题进行说明。

移动互联网应用的发布推广渠道中存在着安全审核环节薄弱的问题[2]，使其难以阻挡恶意应用的发布和推广。以当前发展最广泛的Android应用的发布为例，目前采用的方式是由应用开发者自行利

用 Android 平台提供的签名工具生成自签名并对外发布 APK 文件，而不是由权威的第三方机构发放用于标识应用及开发者基本信息的数字证书，这导致了恶意应用程序的开发者难以被追溯。另一方面，由于对上线应用程序的安全审核缺乏有效的管理制度和技术保障，部分渠道甚至完全通过聚合方式推广应用，导致针对 Android 移动终端操作系统的第三方应用商店成为手机病毒泛滥的主要推手。据工业和信息化部电信研究院信测平台对国内部分应用商店上线应用检测数据显示[4]，恶意程序的平均占比超过 4%，部分占比甚至超过 20%。

其次，作为移动互联网的典型应用之一，移动支付类应用中除了存在着如钓鱼、连接中断导致交易失败、用户交易欺诈等安全威胁之外，还面临一些特殊安全风险，如短信交互风险。在移动支付类业务中，很多用户关键信息是通过短信方式传递的，而这些信息很可能在空口传递时被窃听盗取，从而导致用户金融信息以及交易信息的外泄。短信业务还存在丢失和重发的可能，如果应用于支付环节时，将会造成交易问题，如多次支付或者支付失效等。另一方面，基于手机短信验证的移动金融身份认证也存在着安全漏洞[28]。一旦发生手机卡被复制或者是验证短信被劫持转发等情况，攻击人员就能够非法控制被害人的手机银行，甚至可以通过“帮助”被害人注册并开通手机银行的方式来进行犯罪活动。

据统计[16]，2015 年上半年涉及用户资金安全的资费消耗和恶意扣费类病毒类型占比超过 80%，对用户的安全威胁最大；隐私类病毒占比仅为 1.80%，但攻击方式更加多元化，如与短信相结合的“相册”木马病毒通过钓鱼、诱骗、欺诈的方式窃取用户姓名、身份证号、银行卡号、登录账号密码等重要的隐私信息，严重威胁用户财产安全。

目前，对移动互联网应用安全的监管工作起步不久，还缺乏相应的支撑手段以及适用政策和标准，因此，对于移动应用安全的监管尚处于“有心无力”的状态。

6 移动互联网安全体系与标准化研究

目前，业界已提出多种移动互联网安全体系的解决思路。概括而言，本文认为可以采用动静结合的方式制定移动互联网的安全标准体系。所谓静，是研究制定一套移动互联网安全总体架构，设计移动互联网可以采用的安全防护体系；所谓动，是研究移动互联网主动安全防御技术，在网络运转过程中提高对异常流量、攻击流量的防控能力。

6.1 移动互联网的安全框架设计

业界一般认为，移动互联网安全体系架构的设立应当采用物理与信息安全相互分层，并依据其体系结构来构建的原则。图 4 是业界提出的一种移动互联网的安全框架[29]，其中安全管理负责对所有安全设备进行统一管理和控制，基础支撑为各种安全技术手段提供密码管理、证书管理和授权管理服务。

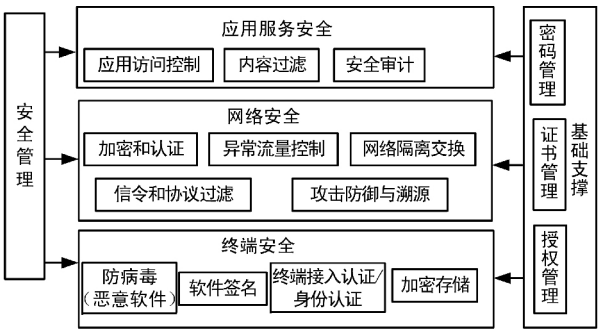

图 4 移动互联网安全框架

但是，业界目前提出的移动互联网安全框架往往仅关注于其安全体系的某一方面，缺乏对于整体化规范的制定。

一般而言，移动互联网统一安全框架体系的制定，需要采用系统化的方法，在整体上把复杂的网络安全相关特征划分为多个构成部分，以便进行相关的安全规范制定。目前，移动互联网的安全体系框架的制定工作涉及多个标准化组织，但是这些标准化组织之间的协同性还存在不足，导致尚缺乏系统性的移动互联网安全体系的标准化工作。

移动互联网安全框架的构建可以参考 ITU－T 的 X.805 建议[30]定义的端到端的安全体系框架和安全尺度模型，该安全体系框架如图 5 所示，包含有 3 个层次、3 个平面和 8 个维度。

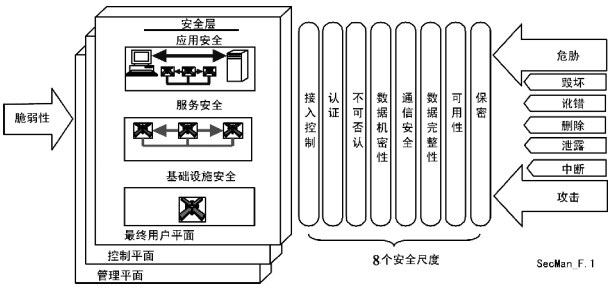

图 5 ITU－T X.805 中的安全体系框架

在此基础上，移动互联网安全框架的构建还可以借鉴传统移动通信网的安全体系框架。为了保障

用户信息的安全，3GPP 和 3GPP2 等标准化组织为传统移动通信网络制定了严格的安全体系框架和安全保障手段[9,10]，其安全机制涵盖了移动终端层面、网络层面、应用层面以及管理层面。这种严谨的安全框架的制定方式为移动互联网安全框架的设计奠定了良好的参考基础。

除了安全体系框架之外，业界还提出了制定相应的移动互联网安全评测体系的需求。比如我国已制定了针对移动智能终端的安全评测体系[9]，该安全评测体系包括两大部分，一是移动智能终端自身的安全评测，二是移动应用软件的安全评测。通过安全评测体系的建立，对移动互联网相关设备、软件以及应用的入网提供必要的安全保证。

6.2 主动安全防御技术的研究

随着移动互联网面临的安全事件正在向规模化、复杂化、分布化和间接化的趋势发展，单纯依靠部署在局部范围内的传统安全产品或技术来识别和发现整个网络中的安全事件，已经变得非常困难或有失准确性，因此迫切需要一种能够主动监控大规模网络的安全态势并进行安全防御的新技术。

针对该需求，业界提出了主动安全防御技术[31,32]，并积极进行相关产品与系统的研发。主动安全防御技术能够帮助用户预先识别网络系统脆弱性以及所面临的潜在的安全威胁，根据安全需求来选取符合最优成本效应的主动安全防御措施和策略，从而提前避免危险事件的发生[33]。

方滨兴院士也提出[34]："主动实时防护模型与技术的战略目标是通过态势感知、风险评估和安全检测等手段对当前网络安全态势进行判断，并依据判断结果实施网络主动防御的主动安全防护体系。"

作为主动防御技术的一个重要组成，大规模网络态势感知通过综合各方面的安全因素，对网络安全信息进行深度挖掘和信息关联，及时发现已经发生的和正在发生的安全事件，并在此基础上提供一种直观的安全威胁态势图，在反映出网络整体安全状况变化的前提下，能够对其下一步的发展趋势进行预测和预警，可以方便管理人员进行准确及时的决策，并为网络安全性的提升提供一套可靠的参照依据。

在概念上，大规模网络的安全态势感知需要解决态势要素获取、态势理解和态势预测 3 个重要环节[35]。其中，态势要素获取负责收集安全事件，包括主动和被动两种收集模式；态势理解则负责分析安全事件，需要对上述态势要素获取步骤所得到的安全事件进行数据融合和关联分析，以获取具有表现网络运行状况的特性的数值。态势预测则根据网络安全威胁发展变化的实际数据和历史资料，运用科学的理论、方法和各种经验、判断、知识去推测、估计、分析其在未来一定时期内可能的变化情况[36]。

目前在标准化组织中尚未进行大规模网络安全态势感知技术的探讨，但是其在学术界则已成为研究的热点方向之一[37,38]。

7 结束语

近年来，移动互联网的网络规模和用户规模都呈现出爆炸性增长的态势。而当前移动互联网的安全问题也呈现出快速发展的态势，其原因主要来自于移动互联网终端受限制的计算能力、接入网络受限的防攻击能力以及业务应用有限的安全防护手段等。可以预期，针对移动互联网安全的研究将在很长一段时间内成为信息安全研究的重点和热点。在当前移动互联网发展的初期阶段，在通盘考虑移动互联网安全需求与安全保障技术的基础上，完全有机会设计结构严谨的移动互联网安全框架，使其变得更加安全。

参 考 文 献

[1] Theodore新华网. 我国网民数量已达 6.68 亿人 [OL]. http://news.xinhuanet.com/fortune/2015-07/23/c_1116022351.htm，2015.

[2] 中国工业和信息化部电信研究院. 移动终端白皮书(2014 年) [R]. 北京：中国工业和信息化部电信研究院，2014.

[3] 百度百科. 移动互联网 [OL]. http://baike.baidu.com，2015.

[4] 中国工业和信息化部电信研究院. 移动互联网白皮书(2011 年) [R]. 北京：中国工业和信息化部电信研究院，2011.

[5] 罗军舟，吴文甲，杨 明. 移动互联网：终端、网络与服务 [J]. 计算机学报，2011，34(11)：2029-2051.

[6] 封 莎，闵 栋. 移动互联网安全问题分析 [J]. 现代电信科技，2010(4)：5-8.

[7] 吴吉义，李文娟，黄剑平，等. 移动互联网研究综述 [J]. 中国科学：信息科学，2015，45(1)：45-69.

[8] 李勇辉，王晓箴，贾亦辰. 移动互联网安全威胁及策略研究 [J]. 邮电设计技术，2013(10)：10-13.

[9] 林东岱，田有亮，田呈亮. 移动安全技术研究综述 [J]. 保密科学技术，2014(3)：4-25.

[10] 陈尚义. 移动互联网安全技术研究[J]. 信息安全与通信保密,2010(8):34-37.
[11] 李 晖,李凤华,曹 进,等. 移动互联服务与隐私保护的研究进展[J]. 通信学报,2014,35(11):1-11.
[12] 中国工业和信息化部电信研究院. 移动终端白皮书(2012年)[R]. 北京:中国工业和信息化部电信研究院,2012.
[13] 李 根. Android系统恶意代码检测技术研究[D]. 黑龙江:哈尔滨工业大学,2014:27-31.
[14] 落红卫. 移动恶意代码分析及检测技术研究[J]. 信息通信技术,2015(01):34-38.
[15] 刘立新. 智能终端漏洞和恶意代码分析及安全性评估研究[D]. 北京:北京邮电大学,2015:19-23.
[16] 中国信息通信研究院. 移动终端白皮书(2015年)[R]. 北京:中国信息通信研究院,2015.
[17] 中国工业和信息化部电信研究院. 移动终端白皮书(2013年)[R]. 北京:中国工业和信息化部电信研究院,2013.
[18] 秦建华;罗洪莉. 基于位置服务中用户隐私泄露与保护[J]. 电脑编程技巧与维护,2015(8):113-114.
[19] 张 承. 移动互联网隐私泄露研究[D]. 北京:北京邮电大学,2012:15-20.
[20] 柳 青. 移动互联网安全问题分析[J]. 卫星电视与宽带多媒体,2011(09):36-37.
[21] 赵大伟. 移动网络安全若干关键问题研究[D]. 北京:北京邮电大学,2014:32-35.
[22] 明 芳,彭亚雄. 移动互联网安全问题分析及策略[J]. 通信技术,2013,46(04):19-21.
[23] 罗志强,史国水,沈军,等. 移动互联网安全热点技术研究[J]. 电信科学,2013(Z1):254-256
[24] 张彬彬. 无线局域网攻击技术研究[D]. 湖北:华中科技大学,2006:55-59.
[25] 戴 伟. 大规模集中式无线局域网安全研究[D]. 河南:解放军信息工程大学,2012:36-41.
[26] 汤鹏杰. WLAN拒绝服务攻击仿真及其防御研究[D]. 江西:南昌大学,2008:27-35.
[27] 张 帆,马建峰. WAPI认证机制的性能和安全性分析[J]. 西安电子科技大学学报,2005,32(2):210-215.
[28] 刘会议. 移动互联网中身份认证技术的研究[D]. 山东:山东大学,2014:
[29] 贾心恺,顾庆峰. 移动互联网安全研究[J]. 移动通信,2011(10):66-70.
[30] ITU-T X.805 Recommendation,Part 6:Security dimension[S],2003.
[31] 高晓飞,申普兵. 网络安全主动防御技术[J]. 计算机安全,2009(1):38-40.
[32] 向林宏. 主动防御技术的研究与实现[D]. 成都:电子科技大学,2011:51-55.
[33] 姜 伟,方滨兴,田志宏,等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报,32(4):817-827,2009.
[34] 方滨兴. 解读信息安全创新突破点[DL]. http://www.eert.org.en/articles/news/common/2007051823317.shtml,2008.
[35] 杨光华. 2011移动互联网安全热点分析[J]. 中国信息安全,2011(07):48-50.
[36] 李 硕,戴 欣,周渝霞. 网络安全态势感知研究进展[J]. 计算机应用研究,2010,27(9):3227-3232.
[37] 司震宇. 融合多种网络层拓扑发现技术的网络安全态势感知方法研究[J]. 东北农业大学学报,2012,43(11):122-128.
[38] 李玉超,徐锡山. 网络信息系统的风险评估研究现状分析[J]. 科技信息(学术研究),2008(03):187-188.