

硕 士 研 究 生 读 书 报 告



**移动互联网信息安全**

题目 移动互联网信息安全

作者姓名 李阳

作者学号 21651055

指导教师 李启雷

学科专业 移动互联网前沿技术

所在学院 软件学院

提交日期 二○17年 1 月

The Security Of The Mobile Internet Information

A Dissertation Submitted to

Zhejiang University

in partial fulfillment of the requirements for

the degree of

Master of Engineering

Major Subject: Software Engineering

Advisor: qilei Li

By

Yang Li

Zhejiang University, P.R. China

2017

摘要

随着移动通信技术的快速发展，移动互联网产业在我国主要产业中占据着越来越重要的地位，为我国国民经济的发展做出了突出贡献。当前智能手机普及、4G 网络得到推广，我国移动互联网应用呈现出爆发式增长的态势。但是，移动互联网再为广大用户带来便利的同时，也暴露出了严重的网络安全问题。相关工作人员要对移动互联网安全技术深入研究，最大限度的满足移动互联网应用的安全需求。

**关键词**：移动互联网，网络安全，安全需求

Abstract

With the rapid development of mobile communication technology, mobile Internet industry in our country, the main industry occupies a more and more important position, for our country made great contributions to the development of national economy.Promoted the popularization of smart phones, 4 g network, mobile Internet application shows a tendency of explosive growth in China.However, mobile Internet to bring convenience to the users at the same time, also has exposed the serious network security problems.Relevant personnel to the mobile Internet security technology research, the maximum meet the security requirements of mobile Internet application.

**Keywords：**The mobile Internet, network security, demand for security

1 移动互联网面临的安全问题

互联网已成为许多人生活和工作中形影不离的工具。随着智能手机的普及，移动互联网也已渗透到人们的生产生活中，在很大程度上影响着人们的生活方式，包括沟通、娱乐、购物、学习等许多方面。作为互联网的一部分，移动互联网在应用的过程中，随时都在面临着来自于互联网的病毒威胁与安全挑战。伴随着移动通信与互联网技术的融合，所形成的联合IP 地址方便人们使用的同时，也为病毒以及黑客的入侵确立了详细的目标。因为，在互联网网络用户地址公开化的条件下，人们能够很容易的找到网络重要节点的IP地址，这就会存在一定的漏洞。一旦存在非法软件，如“灰鸽子”、“暗黑蜘蛛侠”等对用户发起漏洞扫描，就会带来数据的恶意修改、盗取用户敏感信息，极大的威胁了用户的信息安全，甚至会导致巨大的经济损失。换而言之，IP的开放式结构架构是移动互联网安全问题的根源[1]。

在移动互联网的用户群体中，手机用户占据着最大的比重。因此，某些商家利用该特点，在移动互联网的用户手机中，通过恶意传播病毒等方式，进行篡改破坏、窃密监听、恶意收费甚至是欺骗敲诈，以获得非法收益。目前，针对手机的木马病毒种类有很多，例如“X卧底”等，这些病毒的功能通常较为强大，不仅能够监控到手机用户的通话记录、短信等内容，还能够通过远程协助，代替移动互联网用户自动接打电话。而对于一些配置比较高的智能手机，还能够通过手机自带的卫星定位系统装置进行自动传导，在获取手机用户的位置信息后，用户不仅面临着隐私的泄露风险，还会威胁到生命以及财产安全。

随着我国移动互联网的高速发展，这些相关的安全问题不仅没有获得有效的解决，反而以更加多元化的方式接入移动终端，这使得本就存在的安全隐患变得更为凸显。因此，有效利用移动互联网安全技术，消除移动互联网中的安全隐患，具有重要的现实意义。

2 移动互联网安全策略

2.1运营安全管理

通过对移动互联网中面临的安全问题进行详细的分析可以了解到，当前移动互联网中的安全问题与该产业链中各环节的运营管理存在着一定的联系。因此，应当加强运营安全管理，以有效降低移动互联网应用中的安全风险。首先，可以借鉴互联网安全保障措施，通过网络内容进行监听等方式，实现对于部分安全事件的事前控制，如此可在很大程度上消除安全隐患;其次，在掌握了主要的内容/业务提供方式以后，可在服务器、短/彩信网关等主要环节进行信息的识别、过滤以及阻断，有效防止恶意消息在移动互联网中的进一步扩散;最后，移动互联网具有较好的溯源能力，可以充分利用该特点，有针对性的在移动互联网的特殊节点采取安全监控措施，以进一步加强运营中的安全管理，具体包括以下几点:

1)通过制定统一的安全策略管理，以加强对移动互联网中业务系统间的访问控制;

2)加强对于新运营模式的检查与控制，通过SDK和业务上线要求等方式，将安全因素植入到新业务中，确保安全规划与新业务相匹配，避免存在漏洞;

3)加强移动互联网统一认证的技术应用，以降低移动互联网用户在登录多个业务系统中信息泄露的风险;

4)合理运用IP地址的溯源机制，推进网络接入的实名制;

5)其他预防措施，如过滤不良内容、清洗流量、在关键节点部署DPI、DFI策略等。  
2.2 移动终端安全管理

为了有效降低移动互联网在应用过程中存在的安全风险，不仅需要在运营过程中进行安全管理，还应当对移动终端采取必要的安全防范措施，以进一步加强安全管理。通过分析移动互联网中的安全问题，我们了解到IP的开放式结构架构是移动互联网安全问题的根源，但是，目前尚未有具体的方案来解决黑客IP侵入的问题，因此，只能从手机、笔记本电脑等客户端口做好防御工作，以阻止黑客的侵入。具体的安全加固措施包括:对移动终端进行资料的保密、安全防护、终端的运维管理;在移动终端可以通过安装杀毒、防钓鱼、防ARP欺骗[2]、间谍等软件，或者是设定网络访问权限等方式，加强用户在使用过程中的安全管理;与此同时，可以运用入侵检测IDS与入侵防御IPS，进行必要的安全检测与数据分析;通过安全通信协议识别，对于数据进行筛选，有效避免用户接触到手机病毒，以防产生信息泄露并引发经济损失。

2.3 移动电子商务安全技术应用

随着智能手机的普及，在移动互联网的应用过程中，移动电子商务占据着主体地位，为商家与消费者提供了便利的购物环境。但是，手机病毒的存在使得便利的移动电子商务面临着巨大的威胁。为了保护保护商家与消费者的财产利益，应当加强对移动互联网的安全管理，这就对安全技术提出了更高层次的要求，具体可以采取以下几点措施:首先，通过对内容进行过滤，重点防范不良信息的传播;其次，为了保证业务系统信息的保密性、安全机制的完整性，对于服务的提供方应当采取严格的认证措施;再次，运用GBA/GAA认证架构和业务特定安全机制，进行电子证书的认证;最后，对于手机支付这一关键环节要加大安全管理力度。

3移动互联网安全问题分析及其社会危害性

移动互联网是移动通信网络与互联网相结合的产物,在融合两者特性的同时,也承载了来自移动通信网和互联网各自的信息安全风险。我国移动互联网总体信息安全环境不容乐观,目前还存在着多方面的问题。其中最主要的问题集中在用户安全意识不足、网络安全存在隐患以及相关法律法规不完善三个方面。

3.1用户安全意识不足

低学历水平人群是我国目前移动互联网用户的主要群体,同时高年龄段用户群体的占比也在逐年加大,这两部分用户群体的安全意识相对较弱,我国移动互联网用户总体安全意识存在不足[3]。

3.2网络安全存在隐患

我国网络安全隐患主要体现在安全防护手段落后和技术更新缓慢上。从各国商业公司甚至政府的网络频发的安全事件可以看出,没有绝对安全的系统和技术手段,只有不断保持安全防护技术的更新,才能将自身网络的信息安全维持在一个较高的水平上。如果将安全事件中的黑客和受害者分别作为攻方和守方,那么对于守方而言,需要考量其网络的安全强度与运营成本之间的平衡;对于攻方而言,则是考量其进攻难度与获益之间的平衡。网络技术的更新日新月异的,这两个平衡也在不断变化着。随着技术的不断发展,守方需要不断追加网络安全成本的以维持、提高其网络安全强度,而攻方随着技术门檻的降低和设备性能的一高,对同一网络环境的进攻成本将不断下降。一旦这个平衡无法维持,受利益驱使将存在严重的信息安全隐患。

3.3相关法律法规不完善

我国移动互联网起步较晚,相关的法律法规还在不断适应和完善的过程中,目前对行业的监管和保障仍存在着诸多空白之处。

(1)应用来源缺乏有效监管

移动互联网丰富多彩的内容和功能源自于其应用,目前智能手机主流操作系统安卓和IOS在应用来源上存在较大的区别。使用苹果公司IOS系统的用户,其应用只能够通过该公司旗下的应用商店这一单一来源进行下载,苹果公司会在应用商店内的各种应用上架前进行审核,以保障用户使用该应用的安全性。谷歌公司的安卓系统则相对开放些,使用该系统的用户不仅可以通过谷歌公司旗下Google Play商店下载应用,还能通过第三方应用商店(如百度助手、91助手、豌豆荚等)甚至任意互联网地址自由下载应用,谷歌公司仅对其旗下Google Play商店内上架的应用进行审核。安卓系统并未对用户安装应用的来源进行限制,也未对自己旗下商店之外的应用进行审核,对恶意应用的防护和识别能力较弱,用户在使用过程中存在较高的安全风险。IOS系统限制单一应用来源的方式相对安全,但仍然存在安全风险。其对应用的审核仅仅为公司的商业行为,没有政府以及其他公共管理部门的介入,审核过程仍有可能存在商业管理问题或技术漏洞,用户的合法权益缺乏法律的保障。

(2)数据隐私缺乏有力保障

用户在使用各种移动互联网的应用中,往往需要向应用服务提供商ServiceProvider(简称SP)提供个人信息和相关数据。SP基于互联网向用户提供服务的暴露在互联网的大环境下,与网络运营商一样存在安全强度与运营成本间的矛盾。近年来SP出现安全事件导致用户数据泄露的报道屡见不鲜,包括苹果、索尼影业以及开心网等国内外行业巨头也未能幸免,给用户的数据安全问题敲响了警钟。

(3)违法行为的处置存在漏洞

违法成本极低,法律监管的缺失是信息安全事件一而再再而三爆发的根本。

3.4移动互联网安全问题的社会危害性

随着移动互联网用户规模的急速增长,信息安全问题越来越突出,由此带来的一系列影响也逐渐成为严重的社会问题之一,给社会的平稳发展带来了巨大危害。

3.4.1用户财产、精力遭受损失

信息安全事件往往给用户带来精力、财产和权益等多方面的损失。

3.4.2用户权利受到侵害

我国目前的移动网络运营模式为用户每月支付套餐费用购买运营商的网络服务,并能够通过支付其他附加费用购买增值业务服务,因此运营商有责任为用户提供安全可靠的网络服务。用户所购买的网络服务出现安全问题,相当于合法权益收到了直接的侵害,严重的还将导致用户经济损失和隐私侵害等问题。

伪基站对移动互联网用户具有多种危害性。首先是“绑架” 了用户的网络,使用户在短时间内无法使用运营商的网络服务。其次是伪基站发送的垃圾短信,对用户造成了骚扰,并且相较于其它的诈骗短信更具有迷惑性。最严重的是伪基站可以随意更改发送的号码,一旦被不法分子所利用,冒用政府部门、公共服务组织或知名企业的名义编造和发送虚假信息,将给社会带来难以估量的负面影响。

3.4.3用户隐私面临威胁

移动互联网与现实生活关联越来越紧密的情况下,隐私保护问题日益凸显。智能手机的普及给人们带来了巨大的便利,但其中有不少是以牺牲个人隐私为代价的,比如一些智能推荐服务,都是在用户以往消费偏好、地理区域等方面数据信息基础上做出的判断。虽然隐私窃取往往不会对用户造成直接经济损失,但埋下的隐患和随后有可能形成的一系列连锁反映一旦爆发,将给用户带来更高程度的危害。

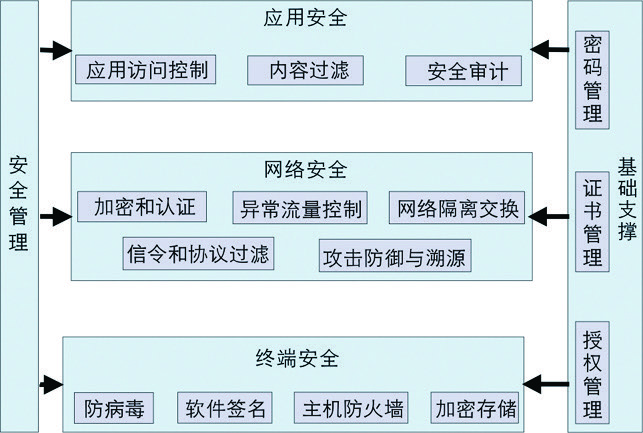
为了扩大市场占有率,一些网络企业会将搜集到的用户信息作为拓展公司业务的资源,有的企业甚至还会将所占有的大量用户信息作为一种商品,直接在地下黑市上进行交易。比如用户名单通讯录、用户商业消费行为偏好等信息数据。但其来源是否合法合规,却难以受到有效及时的监督。同时,数据的购买方是把这些数据用于广告推销,还是用于其他不为人知的用途,同样不得而知。

在移动互联网的云应用方面,用户可以随时将数据传输到云端,云端信息不仅敏感,还更加详细、相关和连续,具有极强的挖掘性。云存储安全也是大家很关心的问题,与APP应用泄密重视程度旗鼓相当。轰动全球的好莱坞“艳照门”可以说是迄今影响最大的“云隐私”泄露事件,对云隐私安全敲响了警钟。移动互联网时代对个人隐私信息的保护,在法律实践等多个层面都有不少难题待解。

4移动互联网安全框架

移动互联网安全威胁存在于各个层面，包括终端安全威胁、网络安全威胁和业务安全威胁。智能终端的出现带来了潜在的威胁，如信息非法篡改和非法访问，通过操作系统修改终端信息，利用病毒和恶意代码进行系统破坏。数据通过无线信道在空中传输，容易被截获或非法篡改。非法的终端可能以假冒的身份进入无线通信网络，进行各种破坏活动;合法身份的终端在进入网络后，也可能越权访问各种互联网资源。业务层面的安全威胁包括非法访问业务、非法访问数据、拒绝服务攻击、垃圾信息的泛滥和不良信息的传播等。

移动互联网安全框架如下图所示，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。



4.1应用安全

移动互联网业务可以来自互联网、移动网以及移动网与互联网结合所得的创新业务，包括移动浏览、移动Web2.0、移动搜索、移动地图、移动音频、移动视频、移动广告、移动Mashup等业务。应用安全主要采用如下措施保证移动互联网业务的安全:

4.1.1应用访问控制

由于互联网上资源众多，资源的种类和信息量日益增加，使用环境也越来越复杂，必须有严格的安全认证手段，以防止对手控制资源的非法访问和非授权访问。应用访问控制为应用系统提供统一的基于身份令牌和数字证书的身份认证机制、基于属性证书的访问权限控制，保护受控制的信息不被非法和越权访问，并对事后的追踪提供可靠的依据。应用访问控制采用安全隧道技术，在应用的客户端和服务器之间建立一个安全隧道， 并且隔离客户端和服务器之间的直接连接，所有的访问都必须通过安全隧道，没有经过安全隧道的访问请求一律丢弃。

4.1.2内容过滤

Web内容过滤:内容过滤基于分类库的URL进行访问控制，对色情、反动等多种负面网站按类别进行选择控制;对Web网页关键字和Java、JavaScript、ActiveX 等移动代码过滤;以黑名单/白名单、通配符、正则表达式的方式进行网址过滤。反垃圾邮件:对收发邮件的地址、附件名、附件内容、主体、正文内容、收发邮件人姓名等关键字匹配过滤;对中转垃圾邮件进行识别和过滤;具备反垃圾邮件功能，在线查询垃圾邮件服务器， 阻断垃圾邮件源。

4.1.3安全审计

安全审计一般包含两类审计策略:系统审计策略控制哪些事件应该作为系统相关的活动被记录，包括主体鉴别、改变特权以及管理安全策略的事件(如修改访问 控制数据)等;应用审计策略控制应用程序应该审计哪些事件。

4.2网络安全

移动互联网网络主要分两部分，接入网及IP承载网 /互联网。接入网采用移动通信网时涉及基站(BTS)、基站控制器(BSC)、无线网络控制器(RNC)、移动交换中心(MSC)、媒体网关(MGW)、服务通用分组无线业务支持节点(SGSN)、网关通用分组无线业务支持节点(GGSN)等设备以及相关链路，采用WiFi时涉及接入(AP)设备。IP承载网/互联网主要涉及路由器、交换机、接入服务器等设备以及相关链路。

4.2.1加密和认证

加密和认证体系可以参考WPKI认证体系。WPKI (WAP Public Key Infrastructure)借鉴PKI标准的主要思想，并针对WAP安全规范和移动互联网的特别环境做了必要的改动。WAP安全规范包括WAP传输层安全规范WTLS、WAP应用层安全规范、WIM规范和WAP证书管理规范。

数据加密。移动终端和服务器初次通信时，它们通过WTLS握手协议商定一组会话状态的密码参数，包括协议版本号、选择密码算法、可选择的相互鉴别，使用公开密钥加密技术生成共享密钥。在应用数据阶段中，所生成的共享密钥(预主密钥)将首先被转换成主密钥，主密钥再被转换成加密密钥和MAC密钥，加密密钥为客户机和服务器所共有，使用它对传输数据进行对称加密，保证了机密性，并提高了加密速度。移动终端的 弱计算力将影响加密算法的选择和实现。由于移动终端 CPU的处理能力有限，所以椭圆曲线算法(ECC)特别适用于移动互联网公钥体系。

身份认证。在进行安全握手时，服务器的证书会通过无线网络传到移动终端。对无线网络而言，定义一种缩微证书格式是很有必要的，这既能减轻传输负载，也可以减轻移动终端的处理负载。WTLS证书是X.509证书的缩微格式，适用于无线网络环境。电子商务应用需要一种证书取消机制，在无线网络环境下，可以采用短时效证书来实现证书取消。对内容服务器或WAP网关依旧采用长时效信用验证，但同有线网络不同的是，在时效期间，不是自始至终用一对密钥。证书颁发机构每天都向内容服务器或WAP网关颁发新的证书，如果证书颁发机构决定取消对服务器的信用，就不再颁发证书。

4.2.2异常流量控制

异常流量控制对协议、地址、服务端口、包长等进 行流量统计，基于地址特征进行会话数统计，基于策略进行流量管理和Diffserv服务等级设置，还可以进行最大/最小/优先带宽控制和DSCP服务级别设置，以及上下行双向流量控制。

4.2.3网络隔离交换

网络隔离交换能够实现两个互联网络的安全隔离，并只允许指定的数据包在两个网络之间进行交换。通过设置两个独立的网络处理单元，每个网络处理单元对应一个连接的网络，各网络处理单元间具有惟一的隔离数据通道;两个网络处理单元在物理上是两个独立的实体，二者通过隔离通道实现数据交换，任何一个网络处理单元都不能控制另一个网络处理单元的运行;各处理单元之间交换的对象不是IP数据报文，而是经专用内部协议封装的应用层数据报文，任意原始IP数据报文不可能通过该通道实现数据交换。

4.2.4攻击防御与溯源

攻击防御能检测并抵抗DDoS/DoS攻击，积极防御syn flood、ping flood、arp flood、udpflood、teardrop、sweep、land-base、ping of death、smurf、winnuke、ipspoofing、sroute、queso、sf\_ scan、null\_scan等(D)DoS攻击[4];基于内置事件库对 各种攻击行为进行实时检测;在发现攻击行为后能追溯攻击源，便于事后跟踪和监察。

4.2.5信令和协议过滤

移动通信网由基站、核心网设备等功能单元组成，能够提供移动电话业务;固定电话网由端局、汇接局等主要功能单元组成，能够提供固定电话业务;移动通信网环境和固定电话网通过七号信令实现网络互联和业务互联。信令和协议过滤能防御针对七号信令和各种通信协议的攻击，在安全管理系统的管控下完成信令和协议安全防护功能。

4.3终端安全

4.3.1防病毒

移动互联网终端多属智能设备，通常具备操作系统，应当对常见的病毒如木马、钓鱼和针对操作系统、应用程序漏洞的攻击具备一定的防范能力。防病毒支持 HTTP、FTP、POP3、SMTP、IMAP协议的病毒防护;可过滤邮件病毒、文件病毒、恶意网页代码、木马后门、 蠕虫等多种类型的病毒;能对Blaster、Nachi、Nimda、 Redcode、Sasser、Slapper、Sqlexp、Zotob等主流蠕虫病毒进行过滤和拦截;对灰色软件、间谍软件及其变种进行阻断。

4.3.2软件签名

通过签名手段对软件进行完整性保护，防止软件被非法篡改。一旦检测到应用程序被非法篡改，可以向安全管理设备报警。

4.3.3主机防火墙

通过在智能终端上进行主机防火墙的控制，可以通过白名单/黑名单对呼入呼出号码进行控制，对进出终端的数据包进行基于五元组等特征的控制。

4.3.4加密存储

移动互联网终端的信息自身安全主要是指存储在终端中的用户隐私信息和个人信息(包括通信录、通话记录、收发的短信/彩信、IMEI号、SIM卡内信息、用户文档、图片、照片在内)不被非法获取。重要信息加密存储在终端上，防止被非法窃取，并且加解密是低延迟的，对用户透明。

5移动互联网安全问题的防范方法

5.1应用软件保护技术

软件保护技术的主要目的是对软件进行加密，让移动互联网用户者的隐私安全得到保护，使损失降到最低，现在比较常见两种软件保护技术主要是硬件保护技术和软件保护技术。硬件保护方式是由数据加密、访问控制、密钥生成、可靠数据传输、硬件识别等功能组成，主要的产品包括设置独特密码、加密锁等方式。而软件保护方式主要是通过注册码、电子许可证，授权码等方式对产品进行保护的方式，其主要优点就是使用成本相对比较低，但对安全问题的保护程度上面远不及硬件保护方式，对其的攻破性比较强[5]。

5.2制定防止位置隐私泄露方法

移动电子产品定位功能的发明对移动互联网起着突飞性的发展作用，结合位置服务、LBS与SNS等的各项功能，进一步形成了一种所被广大民众所接受的新型模式，在人们 生活中处处可见。在其原有定位功能的基础上，设定独特功能，制定出一种让“黑客”无法探测出真实位置从而给其制造出一种虚拟位置的假象，对真实位置进行层层防卫，加以施密，让隐私得到应有的保护，防止泄露的方法。

5.3不要盲目使用公共场所的免费Wifi

普通用户很难分辨这些免费Wifi的真伪，同时大多数该类Wifi都无法对用户发送的信息进行加密，因此一旦存在对网络进行监听的攻击者，用户很难保护自己的隐私信息及网银账密不被泄露。

5.4进一步完善相关法律法规

为保障移动互联网信息安全，应结合我国移动互联网发展现状和需求，建立健全适用于我国国情的移动互联网法律监管体系。首先应当制定虚拟社会信息安全监管条例，重点围绕青少年身心健康以及网络隐私、网络诈骗、反动违法等内容制定处罚条例，并严格落实，违法必究。其次，针对网络信息进行立法，并设立专门的监管部门依法进行信息管理，从而为移动互联网等网络信息的安全提供可靠的保障体系，并全面提升法律的威严性及其对违法犯罪分子的震慑力[6]。

5.5加大对移动互联网安全服务方面的投入

移动互联网体系在实际运营过程中，电信运营商及服务供应商应当加大在安全防护工作方面的投入，从网络运营、设备管理、服务内容优化升级等多个层面提升移动互联网安全管理与防护能力。比如说运营商可以加强网络信息安全管理制度的建设，全面提升网络信息的安全管理水平，确保信息产品的安全品质;服务供应商和运营商还可以增加用户体验、试运行等，用来检验服务的安全性。

5.6建立移动互联网信息安全汇报处理体制

为了有效提升移动互联网安全管理水平，并且保证能够及时发现并妥善处理网络信息安全问题，我们必须建立起一套囊括汇报、审查以及管制在内的汇报处理体制。其中在汇报环节，可以设置网络通信、电话等多种方式让用户直接向管理机构汇报信息安全事件;在审查环节，管理机构接到用户投诉之后，应当组织专家委员会以及相关单位、组织机构等妥善处理投诉申请;而在管制环节，如果投诉属实，管理机构应当严格按照相关法律法规对信息安全问题进行处理，以此不断提升移动互联网的安全管理水平。

6结束语

总而言之，移动互联网给人们生活带来便利的同时也存在着很大的安全隐患。相关技术人员要加强对移动互联网安全技术的研究与应用，保证移动互联网产业在为人们带来便利的同时，其自身可以安全、科学、稳定的发展。同时，政府也应该充分发挥其公共管理和公共服务的职能,构筑全方位机制,提高我国移动互联网信息安全水平,为产业的发展和广大民众的移动互联网生活提供一个健康安全的环境。

参考文献

[1]何跃鹰. 互联网规制研究[J]，2010年移动通讯安全年会

[2]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

[3]李宪彬,何东升.移动互联网安全技术研究及应用[J].硅谷，2012

[4]张桔娴.移动互联网安全现状及应对措施[J].网络安全技术与应用，2015

[5]杨海.移动互联网的安全问题及对应策略[J].科技致富向导。2013

[6]杜元胜.移动互联网安全问题及对应策略探讨[J].电子技术与软件工程，2014