关于移动互联网安全技术的研究应用

马永丹 郭 润
天津市公安局网安总队，天津 300021

摘要：随着电子信息科学技术的快速发展，移动互联网产业有了日渐广阔的前景。然而，目前移动互联网的安全存在着极大的隐患。本文对移动互联网面临的安全问题做出了简单的介绍，并提出了几点安全管理措施，供相关人员参考借鉴。
关键词：移动互联网；安全技术；研究应用
中图分类号：TN929.1;TN929.5 文献标识码：A 文章编号：1671-5519（2016）11-0273-01

引言

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[1]。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。

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[2]。

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、恶意吸费甚至是欺骗敲诈，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 移动互联网安全部署架构

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[3]。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、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。

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。

4 结语

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。

参考文献

[1]陈尚义.移动互联网安全技术研究[J].信息安全与通信保密，2010，08:34-37.
[2]李宪彬，何东升.移动互联网安全技术研究及应用[J].硅谷，2012，13:139+181.
[3]盛小宁，谭檣，杜鹏，赖磊洲.移动互联网安全技术研究[J].电子技术与软件工程，2014，17:46+55.