移动互联网安全问题分析

封 莎 工业和信息化部电信研究院通信标准研究所助理工程师
闵 栋 工业和信息化部电信研究院通信标准研究所工程师

摘要：随着我国移动互联网进入快速增长时期，移动互联网的安全问题已经成为影响其发展的重要因素之一。目前在接入安全保障上主要采用双向认证鉴权、在无线空口采用加强型加密机制以及针对 WiFi 接入用 AES 算法替代 RC4，在承载网上主要部署异常流量监控和清洗技术，以及采用网络溯源技术等来解决安全问题。
关键词：移动互联网，网络安全，终端安全，应用安全

Abstract：As China´s mobile Internet has entered a period of rapid growth, the security of mobile Internet has become important for industry development. Currently, two -way authentication and authorization, enhanced encryption system and AES arithmetic into RC4 are mainly used for ensuring access security,, anomaly flow supervise and cleaning technologies are deployed in bearer network, and the network tracing technology is applied to solve security problems.
Key Words: mobile Internet, security, network security, terminal security, mobile application security

近年来，我国乃至全球的移动互联网进入快速增长期。移动互联网实际上是移动网络的延伸。它可在任何时间和任何地点，使联网设备获得对电子邮件、即时消息传送、万维网乃至语音通信的无线访问。随着国内移动运营商各自 3G 网络的大规模建设，2009 年年底宽带移动互联网已覆盖全国 500 个以上城市。截至 2009 年 9 月，我国手机上网网民已经达到 1.92 亿，较 2008 年增长 62.7%。移动互联网相关的增值服务，作为现代服务业的一项重要内容，在推动经济发展方面有重要的意义。

1 移动互联网发展现状与趋势

移动互联网是指采用移动终端通过移动 / 无线网络接入互联网业务。移动互联网的发展涉及到移动网络、移动终端和业务应用三个方面。

在移动网络方面，3G 增强型技术（3.5G）已成为接入网的主导技术，核心网也在向全 IP 化方向演进。移动网络向宽带化、高速化方向发展，对数据业务的支撑能力大幅度提高。同时，传统的运营商主导的“围墙花园”模式受到了极大的挑战，网络开放逐渐成为业界共识。

移动终端在移动互联网发展中的角色越来越重要，业务和终端平台深度融合的趋势日益明显，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。终

端平台尤其是终端软件平台已经成为移动互联网产业链的中心环节，各产业巨头，包括 Google、微软、诺基亚、中国移动、RIM 公司、苹果公司等都试图通过移动终端平台掌控产业链的话语权。终端软件平台的开放甚至开源正在成为一种发展趋势。

在业务应用方面，移动互联网通过来自移动通信网络和互联网的网络能力融合、数据融合和应用融合，将出现众多的创新应用，如 移动 Mashup 业务、移动 Widget 业务、移动位置类业务等。固定互联网的业务复制是目前移动互联网业务发展的特点，而融合“移动”特征的业务创新则是移动互联网业务发展的方向。

2 移动互联网发展中的主要安全问题

移动互联网在给我们带来巨大发展机遇的同时，也带来网络和信息安全的新挑战。随着移动终端和业务平台的逐步开放，封闭的花园围墙被打破，如果没有良好的防护技术和管理手段及时跟上，那么所有互联网今天面对的安全难题，都会出现在移动互联网上，而各种新的安全隐患也将会在移动互联网世界暴露乃至泛滥。移动互联网无处不在的接入同时也意味安全隐患、有害信息、网络违法行为无处不在的可能，相应的安全管理形势将更加复杂。

2.1 移动互联网网络安全

首先，从移动通信角度看，与互联网的融合完全打破了其相对平衡的网络安全环境，大大削弱了通信网原有的安全特性。原有的移动通信网由于网络相对封闭，信息传输和控制管理平面分离，网络行为可溯源，终端的类型单一且非智能，用户鉴权也很严格，使得其安全性相对较高。而 IP 化后的移动通信网作为移动互联网的一部分，这些安全性优势仅剩下了严格的用户鉴权和管理。面对来自互联网的各种安全威胁，其安全防护能力明显降低。

其次，从现有互联网角度看，融合后的网络增加了无线空口接入，同时将大量移动电信设备，例如 WAP 网关、IMS 设备等引入了 IP 承载网，从而使互联网产生了一些新的安全威胁。例如通过破解空口接入协议非法访问网络，对空口传递信息进行监听和盗取，对无线资源和设备的服务滥用攻击等。另一方面，移动互联网中 IP 化的电信设备、信令和协议，大多较少经受安全攻击测试，存在各种可以被利用（如拒绝服务和缓冲区溢出等）的软硬件漏洞，一个恶意构造的数据包就可以很容易地引起设备宕机，导致业务瘫痪。

实际上以上网络安全隐患，已经引起了业界广泛关注。在移动通信技术领域，3G 以及未来 LTE 技术研究和网络建设部署中，安全保护机制已有了比较全面的考虑，3G 网络的无线空口接入安全保障机制相比 2.5G 提高了很多，如实现了双向认证的鉴权等。另一方面，针对 Wi- Fi 无线网络标准中的有线等效保密协议（WEP）加密很容易被破解的安全漏洞，WLAN 的标准化组织 IEEE 使用安全机制更完善的 802.11i 标准，用 AES 算法替代了原来的 RC4，提高了加密鲁棒性，弥补了原有用户认证协议的安全缺陷。然而，仅有以上针对认证和空口传输安全的技术标准改进并不足以完全应对移动互联网面对的安全问题。

针对以上安全问题，可采用端到端的加密方式，在应用平台与移动终端之间的网络连接中一直采用 AES 256 或 3DES 等加密算法，确保以无线方式传输信息的保密性和完整性。

2.2 移动终端的安全保护

移动终端面临的安全威胁既有移动通信技术固有的问题，如无线干扰、SIM 卡克隆、机卡接口窃密等，也有由于移动终端智能化带来的新型安全威胁，包括病毒、漏洞、恶意攻击等。移动终端存储大量的用户私密信息，未来终端中的用户数据保护将面临

巨大的安全挑战。相对 PC，移动终端的恶意代码传播途径更多样化，业务应用环节更复杂。而且移动终端存储和计算能力相对 PC 成本高很多，相应安全防护技术的开发就存在很大的局限性，例如终端病毒库的存储和更新将来必然是很大的难题。再有，移动通信永远在线的特性使得窃听和监视行为更加容易。同时较 PC 而言，移动终端对用户的重要性更大，存储的私密、位置、金融信息，也使攻击诱惑性更大。总而言之，移动终端作为“无所不在”服务和个人信息的载体，随着技术发展，未来其安全问题将会比 PC 更复杂。

针对终端数据保护，可以通过手机锁定、输入密码等方式对用户身份进行认证；通过终端数据自动擦除或远端服务器擦除等方式对丢失手机上的数据进行保护。

针对手机病毒、垃圾邮件、恶意代码攻击等，可通过在移动终端上安装杀毒软件、防火墙等防护软件，遏制手机病毒和垃圾邮件的泛滥；针对恶意代码攻击，目前的监测和判断还没有好的技术解决办法，对恶意代码的遏制则可采用数字签名认证机制，通过对 API 的调用进行签名认证，禁止未获得签名的应用软件在移动终端上加载和运行。

2.3 典型移动业务应用的安全

移动互联网的发展带动了大批具有移动特色的新型融合性移动应用的繁荣，例如移动电子商务、定位业务，以及飞信、QQ 等即时或短信业务。这些应用和移动通信传统业务（话音、彩信、短信等）充分融合，业务环节和参与设备相对增加很多。同时由于移动业务带有明显的个性化特征，且拥有如用户位置、通信录、交易密码等用户隐私信息，因此这类业务应用一般都具有很强的信息安全敏感度。正是由于以上特征，再加上移动互联网潜在的巨大用户群，移动业务应用将面临的安全威胁将会具有更新的攻击目的、更多样化的攻击方式和更大的攻击规模。

以典型移动业务移动电子商务应用为例，除了存在如钓鱼、连接中断导致交易失败、用户交易欺诈等安全威胁之外，其还面临一些特殊安全风险，如：

短信交互风险：移动支付类业务很多用户关键信息需要通过移动通信业务（特别是短信）传递，而这些信息很可能在空口传递时被窃听盗取。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。

隐私泄露或滥用风险：很多移动互联网应用（尤其是支付类商务应用），都会捆绑用户手机号码等隐私信息，这些信息在交易过程中和交易过后被泄露或者滥用的安全风险很大。

移动互联网应用平台由于软硬件存在的漏洞，极易受到来自网络方面的攻击。可采用严格的用户鉴权和管理机制，防护非法用户对应用平台系统的侵入和攻击；同时通过设置防火墙对应用平台进行保护。

3 移动互联网网络安全保障思路

对移动互联网网络安全的保障，可以根据网络结构划分为对网络接入的安全保障和对 IP 承载网络的安全保障。

3.1 接入的安全保障

移动互联网的接入方式可分为移动通信网络接入和 Wi-Fi 接入两种。针对移动通信接入网安全，3G 以及未来 LTE 技术的安全保护机制有比较全面的考虑，3G 网络的无线空口接入采用双向认证鉴权，无线空口采用加强型加密机制，增加抵抗恶意攻击的安全特性等机制，大大增强了移动互联网的接入安全能力。针对 Wi-Fi 接入安全，Wi-Fi 的标准化组织 IEEE 使用安全机制更完善的 802.11i 标准，用 AES 算法替代了原来的 RC4，提高了加密鲁棒性，弥补了原有用户认证协议的安全缺陷。

3.2 IP 承载网安全保障

针对移动互联网 IP 承载网络面临的运营环境和安全挑战，主要可以采取以下几种保障思路：

⑴ 部署异常流量监控和清洗技术

目前移动 IP 承载网络异常流量监测技术（如 DPI、DFI）主要可以应用于骨干网监测、城域网监测以及 IDC 网络监测之中。

骨干网数据流量大、范围广，可采用分布式流量监测方式，通过异常流量监测系统和流量自学习功能掌握正常流量模型，在此基础上，分析和判断带宽型“垃圾”流量攻击，例如 SQL Slammer 蠕虫攻击等垃圾流量大量占用骨干链路资源的情况。

城域网流量监测主要监测城域网核心层和汇聚层的设备流量情况，及时发现和定位来自城域网内部的蠕虫攻击、DDOS 攻击、网络滥用行为(如网络扫描)、垃圾邮件等安全问题。

IDC 是电信 IP 网络的重要网络系统，主要承载电信集团客户的资源。因此，对 IDC 网络进行监测是十分必要的。IDC 网络监测主要是检测 IDC 出口的流量，并将大客户资源的网络访问作为监测的重点，以及时发现针对大客户网络资源的攻击行为，并及时采取响应措施。在 IDC 网络环境中，部署异常流量监测系统的同时，还可以将异常流量过滤系统纳入其中，提高响应速度。

在部署异常流量监测系统的基础上，还可部署流量过滤系统，与异常流量监测系统进行联动。一旦发现有异常流量，可立即将异常流量引入流量过滤系统进行“清洗”，以保护重要系统或重要客户网络资源，降低异常流量对系统的冲击。

⑵ 部署网络溯源技术

针对网络攻击和不良信息发布等不法行为，可部署网络溯源技术，追溯到该行为的发起者。基于溯源和威慑的安全模式将有利于移动互联网的网络攻击监控以及有害信息控制。

目前，移动互联网溯源技术分如下几类：

网络层溯源：根据发给 CP 实施相关行为（例如发帖）的 IP 包的源地址以及发送时间溯源；

会话层溯源：WAP/Web 网关与 CP 用服务器建立 HTTP 会话（例如浏览、上传等）连接时可能发送的手机号或者手机号被扰码 / 加密变换后的 ID 溯源（手机应用或者 GGSN 也有能力发送，但是现阶段手机应用和 GGSN 都不支持）；

应用层溯源：根据应用中 ID（登录名、QQ 号、昵称等）溯源，可能的方式是实名 ID、ID 后台绑定手机号、ID 后台绑定身份、ID 社会关系分析、ID 行为分析等。

通过移动通信网使用互联网业务时，每个终端都拥有唯一性标识 IMSI 号，且终端私密性较传统互联网更强，因此移动运营商通过对防火墙、WAP 网关等网络设备进行改造，能够对不法用户在移动互联网上所有行为追溯到 IMSI 号，配合手机实名制或者移动定位技术，甚至可以精确定位到不法用户个人。

⑶ 利用设置业务网关 / 代理 / 平台的方式，在移动互联网网络边界构建网络用户 UNI，规范用户对网络侧系统和设备的访问行为，提高承载网络拓扑安全。

4 结 语

目前，随着 3G 牌照发放、中国运营商采取下调资费或推出多样化套餐等方式吸引用户，移动互联网在用户数量上将会出现大幅度的提高。因此，我们应该对移动互联网的安全尽早进行全面规划，从网络安全和信息内容安全角度最大程度地满足移动互联网的安全需求。 MSTT