DOI:10.13992/j.cnki.tetas.2010.02.020



# 移动互联网安全威胁分析与防护策略

段伟希[1] 周智[2] 张晨[1] 李刚[3]

(1 中国移动通信集团设计院有限公司 北京 100080)
(2 中国移动通信集团公司 北京 100032)
(3 中国移动通信集团设计院有限公司黑龙江分公司 哈尔滨 150080)

**摘 要** 本文简述了移动互联网的体系结构，分析了其所面临的安全威胁。针对安全威胁，详细分析了安全域的划分方式，以及各安全域的防护策略。

**关键词** 移动互联网 安全域 安全威胁 防护策略

移动互联网是以宽带 IP 为技术核心，可同时提供语音、数据、多媒体等业务服务的开放式基础电信网络，它是全国性 Internet 骨干网络之一。

移动互联网由全国骨干网和省网组成，主要覆盖全国省会及地市级城市。其中含核心骨干层节点和汇接骨干层节点，核心骨干层节点和汇接骨干层节点实现跨省业务的有效疏通；其他省会节点作为骨干网的一般骨干层节点，负责转接各省业务；同时，还部署了互联网网间互联节点，通过设置 NAP 点、国内和国际出入口节点，分别实现与国内、国外运营商的互联互通。

目前，运营商在移动互联网上承载了以下多种数据业务：移动、固定数据业务互联网接入、移动数据中心、GPRS 承载业务等。因此，全面分析移动互联网所面临的安全威胁，明确移动互联网安全域的划分原则，并对各安全域制定相应的防护策略对于移动互联网的安全至关重要。

## 1 威胁分析

### 1.1 基础设施层安全威胁

#### 1.1.1 服务主机

服务主机是指移动互联网中用于承载 DNS、Radius 和其它网络服务的主机。其所面临的威胁如下。

(1) 攻击者利用服务器的漏洞，获取管理员权限、访问受限文件等；

(2) 攻击者利用系统本身或其守护进程有缺陷或设置不正确所造成的漏洞，无须登录即可对系统发起拒绝服务攻击，使系统或相关的应用程序崩溃或失去响应能力；

(3) 利用系统程序中的漏洞，攻击者可以收集到对于进一步攻击系统有用的信息。

#### 1.1.2 网络设备

移动互联网中包含的网络设备主要有路由器和交换机等。其所面临的威胁如下所示。

(1) 弱口令；

(2) IOS 缺陷；

(3) 路由器、防火墙和其它提供集中认证和授权服务的产品中存在安全漏洞；

(4) RIP、BGP 和 OSPF 等路由协议中存在安全漏洞。

#### 1.1.3 网络服务

网络服务主要指的是 DNS 服务，其所面临的威胁如下所示。

(1) 拒绝服务攻击，使 DNS 停止提供服务；

(2) DNS 设置不当，导致网络拓扑结构的泄露；

(3) 利用被控制的 DNS 服务器入侵整个网络，破坏整个网络的安全完整性；

(4) 利用被控制的 DNS 服务器，绕过防火墙等其它安

全设备的控制。

### 1.2 网络服务层安全威胁

网络服务层的安全威胁包含骨干网的安全威胁和接入网的安全威胁。骨干网的安全威胁主要是拒绝服务攻击；接入网的安全威胁包含病毒、垃圾邮件和恶意网址访问等。

## 2 安全域划分和安全防护策略

### 2.1 移动互联网安全域划分

安全域是指同系统内有相同的安全保护需求和安全等级，相互信任，并具有相同的安全访问控制和边界控制策略的子网或网络。相同的安全域共享一样的安全策略。划分安全域，可以限制系统中不同安全等级域之间的相互访问，满足不同安全等级域的安全需求，从而提高系统的安全性、可靠性和可控性。

通过对移动互联网现状和安全威胁进行的分析，移动互联网总体安全架构可分为骨干网和省网两个层面，其具体安全域划分如图 1 所示。

如图 1 所示，互联网安全域划分为骨干网安全域、省网安全域。省网安全域又可细分为省网核心域、IDC 安全域、城域网安全域、业务安全域、MDCN 安全域、PS 域安全域、DNS 安全域。

移动互联网骨干网安全域主要包含核心骨干节点负责骨干数据转接和互联互通数据转接；汇接骨干节点，负责各区域转接业务；以及其它节点作为一般骨干节点，负责转接各省业务。

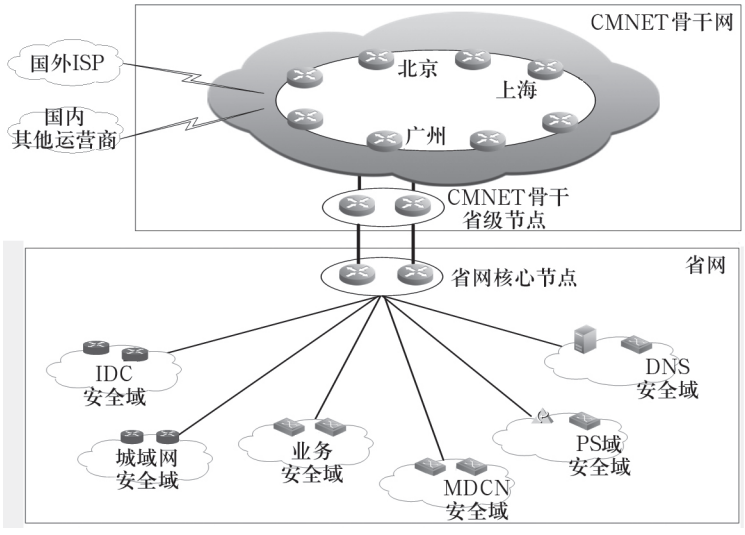


图1 移动互联网安全域划分示意图

省网核心域主要包括省网的边界路由器，各省通常设置两个节点的路由器。

省网 IDC 安全域主要包括 IDC 边界路由器、IDC 核心交流、业务服务器等。

省网城域网安全域主要包括城域网边界路由器、接入网相关设备、认证服务器等。

省网业务安全域主要包括 WAP、MMS、LBS 等数据业务。

省网 MDCN 安全域主要包括网管系统、计费系统、办公系统等支撑系统。

省网 PS 安全域主要包括 Gn 域、Gp 域、Gi 域、Gom 域和计费接口域等。

省网 DNS 安全域主要包括负载均衡设备、DNS 服务器等。

### 2.2 安全防护策略

安全防护策略主要从上述安全域的网络边界控制、网络设备自身安全加固和安全技术手段等 3 个方面展开。

#### 2.2.1 骨干网安全防护策略

##### 2.2.1.1 边界控制

骨干网层面的边界主要是与其他运营商互联边界、与国外运营商互联边界、各省网的互联边界等，为保证全网正常的业务流量骨干网边界仅对典型蠕虫端口进行控制。

##### 2.2.1.2 网络设备自身安全加固

骨干网安全域的设备主要包括有路由器、防火墙、流量监控设备和 DDoS 清洗系统等。在边界控制基础上，需要对骨干网中以上网络设备的高风险安全漏洞进行修补和加固，然后从账号、口令、安全策略、协议安全等内容对网络设备的安全配置进行加固。

##### 2.2.1.3 安全技术手段

安全技术应用流量分析技术，对骨干网层面互联边界和 8 大区域核心节点进行网络流量分析，主要包括与其他运营商的互联边界、国外运营商互联边界，以及各区域节点，识别出正常业务流量、异常攻击流量等内容；为配合进行流量分析，在上述流量分析节点部署技术手段，实现对 DDoS 攻击的防护，在互联边界主要防护来自

于其他运营商、国外运营商的攻击流量，各区域核心节点主要防护来自于其它区域节点、本区域节点内部省份之间的攻击流量。

#### 2.2.2 省网安全防护策略

##### 2.2.2.1 边界控制

省网主要由省网核心节点、城域网安全域、DNS 服务域网接入、PS 域接入、内部应用接入、IDC 接入等构成，其边界控制包括如下几个方面。

（1）核心路由器与 DNS 服务器边界进行严格的访问控制策略，仅开放 DNS 应用所需要的协议端口；

（2）核心路由器与城域网接入边界需要对典型蠕虫传播的端口进行限制；

（3）核心路由器与内部应用接入边界，采用防火墙进行策略控制，对于外部访问仅开放业务所需端口，对典型蠕虫传播的端口进行限制；

（4）核心路由器与 IDC 接入边界，需要对典型蠕虫传播的端口进行限制。

##### 2.2.2.2 网络设备自身安全加固

省网安全域的设备主要包括有路由器、防火墙、DNS 服务器、流量监控设备和 DDoS 清洗系统等。在边界控制基础上，需要对省网中以上网络设备、服务器的高风险安全漏洞进行修补和加固，然后从账号、口令、安全策略、协议安全等内容对网络设备的安全配置进行加固。

##### 2.2.2.3 安全技术手段

（1）省网核心节点采用流量分析技术，对省网与移动互联网骨干网的流量、省网内部各安全域之间的流量进行分析，识别出正常业务流量、异常攻击流量等内容；

（2）省网核心节点采用流量清洗技术，建立流量清洗中心，对来自于移动互联网骨干网、省网内部其它安全域的 DDoS 流量进行清洗(特别是来源于城域网的攻击流量)；

（3）在省网核心节点采用 Botnet 检测技术，实现对省网内僵尸网络的发现；针对 DNS 服务，需要专项的安全防护。

## 3 结束语

本文从基础设施层和网络服务层对移动互联网面临的威胁做了深入的分析。在此基础上，对移动互联网进行了安全域划分，并详细阐述了每一个安全域所应实施的防护策略。希望通过本文的工作，能够为移动互联网提供安全方面的指导和依据。

## Analysis and Prevention Policy of Security Threats of Mobile Net

**Duan Weixi[1] Zhou Zhi[2] Zhang Chen[1] Li Gang[3]**

(1 China Mobile Group Design Institute Co., Ltd., Beijing 100080)

(2 China Mobile Communications Corporation, Beijing 100032)

(3 China Mobile Group Design Institute Co., Ltd. Heilongjiang Branch, Harbin 150080)

**Abstract** The paper describes the infrastructure of the mobile net, and analyzes the security threats faces. According to those security threats, the paper also analyzes the method of dividing the security domain of mobile net as well as the protection policies of each security domain.

**Keywords** mobile net, security domain, security threat, protection strategy

（收稿日期：2010 年 1 月 1 日）