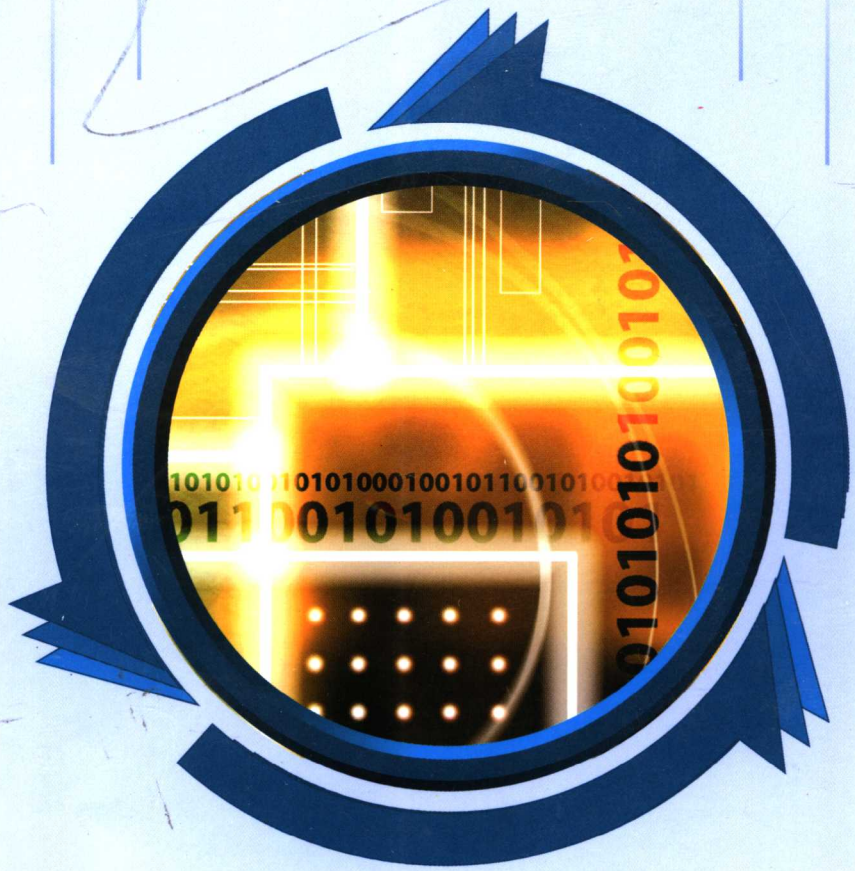
现代通信高技术丛书

移动IP与安全

周贤伟 主编
景晓军 覃伯平 薛 楠 杨 军 编著



国防工业出版社
National Defense Industry Press

现代通信高技术丛书

移动IP与安全

Yidong IP Yu Anquan

周贤伟 主编
景晓军 覃伯平 编著
薛 楠 杨 军

国防工业出版社
http://www.ndip.cn

内 容 简 介

本书从实用和科研的角度出发，比较全面、系统地介绍了移动 IP、移动 IPv6 及相关安全技术的最新发展。

全书共 19 章。内容包括：绪论，移动 IPv4，移动 IP 的切换技术，移动 IP 的组播技术，移动 IP 的安全问题，IPSec 简介，移动 IP 的安全体系结构，移动 IP 的认证，PKI 及其密钥管理，以公钥为基础的安全移动 IP，IKE 密钥交换，移动 IPv6 概述，移动 IPv6 体系结构和切换技术，移动 IPv6 的路由技术，移动 IPv6 安全概述，移动 IPv6 预配置绑定管理密钥，移动 IPv6 认证技术，移动 IPv 源特定组播，以及移动 IPv6 的应用。

本书内容翔实，深入浅出，覆盖面广，具有先进性、科学性和很高的实用价值，适合于高等院校计算机、通信、信息等专业师生和对移动 Internet 感兴趣的科研人员及工程技术人员阅读参考。

图书在版编目(CIP)数据

移动 IP 与安全／周贤伟主编；景晓军等编著．—北京：国防工业出版社，2005.9

（现代通信高技术丛书／周贤伟，邓忠礼，郑雪峰主编）

ISBN 7-118-03966-7

Ⅰ.移… Ⅱ.①周…②景… Ⅲ.移动通信-通信协议-安全技术 Ⅳ.TN915.04

中国版本图书馆 CIP 数据核字(2005)第 059065 号

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号）

（邮政编码 100044）

腾飞胶印厂印刷

新华书店经售

*

开本 787×1092 1/16 印张 16½ 365 千字

2005 年 9 月第 1 版 2005 年 9 月北京第 1 次印刷

印数：1—5000 册 定价：28.00 元

（本书如有印装错误，我社负责调换）

国防书店：(010)68428422 发行邮购：(010)68414474

发行传真：(010)68411535 发行业务：(010)68472764

《现代通信高技术丛书》编委会

序

当今世界已经进入了信息时代，信息成为一种重要的战略资源，信息科学成为最为活跃的学科领域之一，信息技术改变着人们的生活和工作方式，信息产业已经成为国民经济的主导产业，作为信息传输基础的通信技术则成为信息产业中发展最为迅速，进步最快的行业。目前，个人通信系统和超高速通信网络迅猛发展，推动了信息科学的进一步发展，并成为21世纪国际社会和全球经济的强大动力。

随着通信技术日新月异，学习通信专业知识不但需要扎实的专业基础，而且需要学习和了解更多的现代通信技术和理论，特别是数字通信、卫星通信以及传感器网络的现代通信技术方面的知识。从有线通信到无线通信，从固定设备间的通信到移动通信，从无线通信到无线因特网，到传感器网络技术。未来的通信将为人们提供全方位以及无缝的移动性接入，最终实现任何人在任何地方、任何时间进行任何方式的通信，使得通信技术适应社会的发展需要呈现经久不衰的势头。

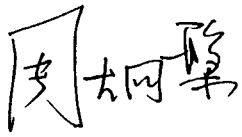
网络技术的飞速发展，通信技术在经济发展中的重要地位日趋重要，世界各国特别重视通信技术的理论研究和通信技术专业人才的培养，国外有关通信领域的文献资料和专著较多。就国内来讲，通信专业人才大量急需，为适应社会经济发展的需要，各高校和科研单位都在培养社会所需的通信专业人才。

为了增进通信及安全技术领域的学术交流，为了满足通信及信息安全专业领域的读者的需要，提供一套能系统、全面地介绍和讲解通信技术原理及新技术的系列丛书，北京科技大学等组织编写了这套《现代通信高技术丛书》。这套丛书内容涵盖了通信技术的主要专业领域，既可作为高等院校通信类、信息类、电子类、计算机类等专业高年级本科生或研究生的教材，又可作为有关通信技术和科研人员的技术参考书。

我觉得这套丛书的特点是内容全面、技术新颖、理论联系实际，针对目前

我国通信技术发展情况与目前已有的相关出版物之间已有一定距离这一情况，本丛书立足于现在，通过对基本的技术进行分析，由浅入深，努力反映通信技术领域的新成果、新技术和进展，是国内目前较为全面、技术领先、适用面广的一套丛书。在我国大量培养通信专业人才的今天，这套丛书的出版是非常及时和十分有益的。

我代表编委会对丛书的作者和广大读者表示感谢！欢迎广大读者提出宝贵意见，以使丛书进一步修改完善。



2005 年 3 月 20 日

前　言

随着 Internet 国际互联网以惊人的速度发展，人类生活节奏的加快，越来越多的人成为了移动办公的一分子，包括远程计算人员、移动售货人员以及其他一些经常需要跑来跑去的人。这些人急切地需要在任何地点、任何时候都能获得 Internet 网络的服务。不断增加的移动办公人群、移动计算技术的发展和人们对网络技术越来越强的依赖，这 3 方面一起推动着将移动计算机与其他计算机相连的需求，包括与固定的和移动的计算机连接。这使得提供移动的 Internet 接入成为当前 Internet 技术研究的热点之一。

由于 Internet 网络本身设计的缺陷及其开放性，Internet 极易受到黑客的入侵。计算机网络是一种有着广泛应用的信息传输系统，它是计算机与通信相结合的产物，它的安全性至关重要，特别是以 Internet 网络为代表的计算机网络正在成为未来全球信息系统最重要的基础设施，它的安全性将直接影响社会稳定和国家安全。移动 IP 是在原来 IP 协议的基础上为了支持节点移动而提出的解决方案，让人们在任何地点都可以随时连接 Internet。它的主要设计目标是移动节点在改变网络接入点时，不必改变网络的 IP 地址，能够在移动过程中保持通信的连续性。移动 IP 在网络层实现移动互动，同样也带来了潜在的安全问题。基于此，本书对移动 IP 进行全面概述的同时，详细地介绍了移动 IPv4 以及移动 IPv6 的安全问题，主要分析移动 IP 的安全体系、因特网协议安全(IPSec)体系和实施、移动 IP 认证技术、密钥管理以及应用等。

本书是在作者多年从事移动通信、网络安全教学和科研工作经验体会、研究成果和吸收了国内外现有相关著作中许多精华的基础上编写而成的。它既有国内外专家观点和理论的精华浓缩，也包含作者从事信息安全研究和开发工作的总结，希望能给读者带来一些启迪和帮助。

全书分为 19 章。第 1 章主要概要介绍了移动 IP 基础知识。第 2 章详细分析了移动 IPv4 技术，包括代理发现、注册和路由技术。第 3 章介绍移动 IP 的切换技术。第 4 章从固定网络组播技术、移动 IP 组播现状及路由协议等方面全面介绍移动 IP 组播技术。第 5 章从网络安全入手，分析移动 IP 安全问题。第 6 章概述了 IPSec 技术，内容包括 IPSec 协议、体系和实施。第 7 章介绍移动 IP 的安全体系结构。第 8 章详细分析了移动 IP 的认证技术。第 9 章从 PKI 基本组成、作用及其算法分析等方面全面阐述 PKI 技术及其密钥管理。第 10 章针对公钥理论分析安全移动 IP 技术。第 11 章从 IKE 的机制、安全方面分析入手，主要阐述 IPSec 密钥交换技术。第 12 章概述移动 IPv6 技术。第 13 章详尽分析移动 IPv6 体系结构和切换技术。第 14 章分析了移动 IPv6 的路由技术，内容包括移动 IPv6 的关键路由技术分析和优化路由方案。第 15 章描述移动 IPv6 安全目标和受到的威胁，并推荐了几种当今比较成熟的认证方法。第 16 章从适用性和安全性考虑，分析移动 IPv6 与配置绑定管理密钥技术。第 17 章描述了移动 IPv6 的认证技术，主要研究 Child - proof

认证，内容涉及到产生背景、家乡代理和整合 CAM 技术等。第 18 章研究了移动 IPv6 的源特定组播技术，主要分析当前的标准和研究状况。本文的最后，在第 19 章介绍了移动 IPv6 在 FreeBSD 平台和 Linux 平台上的一些应用，同时介绍了 Linux - MIPL 项目、CMU Monarch 项目以及 Lancaster 项目。

本书参考或直接引用了国内外的一些论文和著作。编写过程中得到了国防工业出版社及北京科技大学的大力支持和帮助，在此一并深表谢意。

移动 IP 与安全是一门发展迅速的新兴技术，由于作者学识与水平有限，不妥之处在所难免，诚望读者批评指正。

编著者

2005 年 5 月于北京

目　录

第1章 绪 论

目前世界传统电话业务每年的增长率为8%，数据通信业务增长率超过100%，Internet增长速度更快，尤其是进入20世纪90年代中期以来，其业务量一直以300%的速度在爆炸性地增长。“数据为王”已成为众多电信业务运营商和设备供应商的共识，他们纷纷将其投资的重点转移到数据通信网络和设备上。因此，IP技术作为数据业务的主要技术将最终战胜其他各种网络技术而成为网络竞争的大赢家。与此同时，能与Internet的发展相提并论的只有移动通信。移动通信技术的发展首先改变了人们话音通信的方式和观念，使话音的移动通信变得司空见惯，人类进入了个人通信的初级阶段。现在，IP技术和移动通信技术的完美结合，使得数据通信发生与话音通信一样的变革。它将缔造人类个人通信的美好蓝图：人类将实现在任何时间、任何地点，可以用任何一种媒体与任何一个人进行通信的梦想。

1.1 OSI 7层协议模型与TCP/IP协议模型

在一个网络中，所有的网络组件必须保持同步，以确保正常通信。国际标准化组织(ISO)制定了一套叫做开放系统互连(OSI)模型的规范，用于设计无需考虑底层硬件体系结构就能正常运行应用软件的网络体系结构。这种参考模型描述了计算机间的通信系统应该如何设计。OSI模型促进了更高效的网络体系结构的产生，并支持不同配置的计算机间的互操作。

OSI参考模型是不同开放系统的应用进程之间通信所需功能和协议的抽象描述。其基本构造技术是分层技术，利用层次结构，把开放系统的信息交换问题分解到一系列较易控制和实现的层次中，每个层次都在完成信息交换的任务中充当一个相对独立的角色，具有特定的功能。对于每层，都有服务定义和协议规范2个标准，前者规定该层提供的服务，后者详细描述该层协议的动作和有关规程，以确保实现所能提供的服务。OSI的参考模型具有7层结构，如图1-1所示。这7层有如下主要功能。

(1) 物理层。提供为建立、维护和拆除物，以及拆除物理连接所需的机械、电气、功能和规程的特性；给出有关在物理链路上传输的位(bit)流及物理链路故障检测指示。

(2) 数据链路层。为网络层实体提供传送数据的功能；提供数据链路的流控制；检测和校正物理链路产生的差错。

(3) 网络层。控制分组传送操作，即路由选择、拥塞控制、网络互连等。根据传输层的要求来选择服务质量，并向传输层报告未恢复的差错。

(4) 传输层。提供建立、维护和拆除传输连接的功能；选择网络层提供的最适宜的服务；在系统间提供可靠、透明的数据传输，提供端到端的流控制和错误恢复。

(5)会话层。提供2个进程间建立、维护和结束会话连接的功能；提供交互会话的管

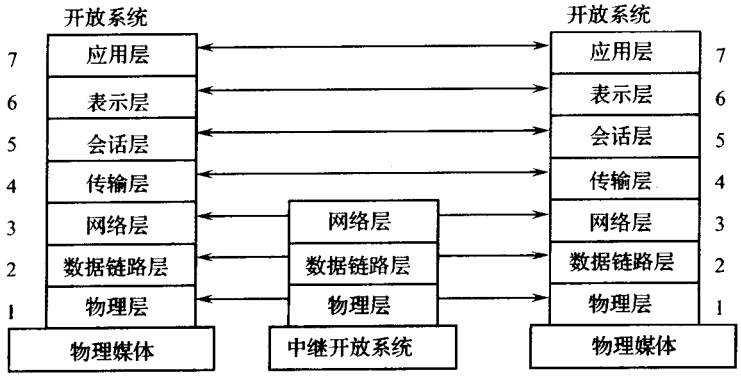


图 1-1 OSI 7 层参考模型

理功能,有 3 种数据流方向控制模式,即单工模式、半双工模式和全双工模式。

(6)表示层。表示应用进程数据、协商数据语法,完成数据格式转换和文本压缩。

(7)应用层。提供用户服务,例如事务处理、文件传送和网络管理程序等。

除 OSI 参考模型外,在市场上还流行着一些其他著名的体系结构,这就是美国早就在 ARPANET(美国国防部高级研究计划局网)中使用的 TCP/IP、IBM 公司的 SNA 以及 Digital 公司的 DNA。TCP/IP 体系常简称为 TCP/IP。TCP/IP 并非国际标准,但它在计算机网络体系结构中占有非常重要的地位。这是因为,尽管 OSI 的体系结构从理论上讲是比较完整的,其各层协议也考虑得很周到,但实际上,完全符合 OSI 各层协议的商用产品却极少进入市场,不能满足各种用户的需求。在这种情况下,使用 TCP/IP 协议的产品却大量涌入市场,几乎所有的工作站都配有 TCP/IP 协议,这就使得 TCP/IP 成为计算机网络的事实上的国际标准,有人也称它为工业标准。TCP 是传输控制协议,规定了一种可靠的数据信息传递服务。IP 协议又称互联网协议,是支持网间互连的数据包协议。它提供网间连接的完善功能,包括 IP 数据包规定的互联网络范围内的地址格式。TCP/IP 是一个允许不同软硬件结构计算机进行通信的协议族,Internet 就是建立在 TCP/IP 协议之上的。一个协议族通常是由不同的层次所组成,TCP/IP 参考模型如图 1-2 所示。

TCP/IP 协议分为 4 层,即网络层、网际层、传输层和应用层。

1) 网络层

网络层又称为数据链路层、网络接口层,负责处理不同通信媒介的细节问题,与具体设备如以太网、令牌环网、网卡等有关。

2) 网际层

网际层负责网络中的数据包传送,并定义了通用数据包格式和 IP 协议:IP 提供了非面向连接的、非可靠的数据包服务;每一个 Internet 上的接口都必须有一个惟一的 IP 地址;网际层同时处理数据包路由和拥塞避免等事务。

3) 传输层

传输层给源主机和目的主机之间的进程通信提供数据流(一个无报文丢失、重复和失序的正确数据序列)。当一个源主机上运行的应用程序要和目的主机联系时,它就向传输层发送信息,以数据包的形式送到目的主机。传输层同时还处理流控、拥塞控制等事务。在传输层有 2 个端到端的协议:TCP 和 UDP。TCP 为通信应用提供了可靠的数据流。UDP