移动网络安全技术与应用

姜　楠　王　健　编著
陈泽强　　审校

電子工業出版社
Publishing House of Electronics Industry
北京・BEIJING

内 容 简 介

本书从实际应用角度出发，先从整体上对移动网络、移动网络面临的安全威胁、移动网络相对于有线网络的特点等做了简要介绍，并给读者提供了必要的基础知识，然后从移动安全技术、移动安全攻与防、部署移动安全、移动安全应用四个方面对移动网络安全做了细致的描述和讨论。如果读者完整阅读本书，会对移动网络安全有一个全面而深入的了解，能够独立设计针对某种应用环境的移动网络安全系统。读者也可以将本书作为参考书，随时查阅相关内容。

本书结构划分灵活、内容全面，既有一定的深度，又有广泛性，概念清晰，深入浅出，易于理解，适合于移动通信管理者、工程技术人员、研究人员、系统设计人员，高校通信专业高年级学生、研究生，以及其他对移动网络安全感兴趣的读者阅读。

图书在版编目 (CIP) 数据

移动网络安全技术与应用/姜楠，王健编著. —北京：电子工业出版社，2004. 11
ISBN 7-121-00476-3

Ⅰ. 移… Ⅱ. ①姜…②王… Ⅲ. 移动通信—通信网—安全技术 Ⅳ. TN929.5

中国版本图书馆 CIP 数据核字（2004）第 108289 号

责任编辑：王春宁
印　　刷：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1 092　1/16　印张：22.75　字数：576 千字
印　　次：2004 年 11 月第 1 次印刷
印　　数：4 000 册　　定价：32.00 元

髂

前　言

以 Internet 为代表的有线网络安全，以及在此基础上形成的电子商务等应用场景已经得到了人们的广泛关注。可以预见，以移动通信和无线局域网为代表的移动网络安全必将在不久的将来再度掀起网络安全应用的新高潮。

过去，攻击者必须坐在你的计算机前才能阅读你的文档、偷看你的电子邮件或者搞乱你的设置。但是现在，即便他坐在隔壁的办公室里、楼上或者楼下，甚至另外一幢建筑物里，他照样可以像坐在你的计算机前一样搞破坏。无线通信技术的发展极大地方便了我们的生活，提高了我们的工作效率，并且在使用上越来越简单，但同时也给我们的系统和使用的信息带来许多意外的危险。因此移动网络安全技术也要同步发展才行。我们必须解决以下这些问题：网络身份识别和密钥管理；攻击者即使靠得再近也不能窃听你的移动通信网络；除了指定的设备、系统或者人，确保没有任何系统和人可以使用你的移动通信资源。

因此，我们本着“先进、全面、实用”的原则确定了本书的内容，编写的目的是，如果读者完整地阅读本书，会对移动网络安全有一个全面而深入的了解，能够处理移动网络中出现的简单而又典型的安全问题，明白安全工作站、接入点和网关搭建原理、原则和实际操作命令，能够独立设计针对某种应用环境的移动网络安全系统；读者也可以将本书作为参考书，随时查阅相关内容。

前两章作为概论从整体上对移动网络、移动网络面临的安全威胁、移动网络相对于有线网络的特点等做了简要介绍，把我们要讨论的网络环境分为移动通信网络和无线局域网，并给读者提供了必要的密码学基础知识。

第一部分——移动安全技术，包括第 3 章～第 8 章。其中介绍的都是与移动网络安全直接相关的技术或主流协议，这些技术和协议将会在移动网络安全下一步的发展中发挥重要作用。

第 3 章介绍了第三代（3G）移动通信到底采取了哪些措施来保障 3G 的安全，3G 安全机制是一个完整的体系，用来解决 3G 中方方面面的安全问题。第 4 章和第 5 章讲述了 WAP 安全结构，WAP 安全结构由 WTLS, WIM, WPKI 和 WMLScript 四部分组成。第 6 章 OMA DRM 和 OMA 下载解决的是手机中数字多媒体数据的版权管理问题，牵涉到内容提供商、服务提供商、手机用户的利益。第 7 章的 WEP 是 IEEE 802.11 无线局域网中采取的安全措施，不过它已经被发现存在问题，WPA 是对 WEP 的升级，是一种可以解决 802.11 大多数安全问题的标准安全机制。第 8 章介绍了蓝牙体系结构中采取的安全措施，并根据不同的应用场景，论述了如何在不同应用中组织这些安全措施来达到系统的要求。

第二部分——移动安全攻与防，包括第 9 章～第 11 章。

第 9 章对手机病毒的原理、常见病毒和防毒方法做了介绍，并描述了病毒常利用的手机漏洞。第 10 章讲述了 PDA 的弱点和容易遭受的攻击，并给出了安全对策。

IEEE 802.11 是最早的无线局域网标准，也是迄今为止惟一已经赢得了市场的标准。但是安全问题一直是 IEEE 802.11 标准最明显的缺陷，802.11 网络都不同程度地存在安全问题，为攻击者的入侵打开了方便之门，第 11 章讨论的就是如何将这些门关上。

第三部分——部署移动安全，包括第 12 章～第 14 章。其内容包括工作站安全部署、接

入点安全部署和网关安全部署，并以 Linux, FreeBSD, OpenBSD, Windows 操作系统为例，一步一步告诉读者如何搭建安全的工作站、接入点和网关，应该先做什么，后做什么，应该如何下命令。

第四部分——移动安全应用，包括第 15 章和第 16 章。这两章分别以移动通信网络和无线局域网为背景，把前面讲过的许多安全技术、协议和措施综合起来，实现移动安全支付和安全无线局域网，可以说这两章是前面讲过的内容的应用、综合和举例。

本书主要面向工程技术人员，读者群包括负责移动网络建设的管理人员和技术人员，负责开拓移动增值业务的人员等所有与移动网络相关的人员，高校、科研单位从事这方面研究的教师、科研人员和学生，以及其他对移动网络安全感兴趣的读者。

本书的写作灵感来自于我们在北京邮电大学信息安全中心学习期间的工作，在此要真诚地感谢我们的导师杨义先教授，没有他以及他领导的北京邮电大学信息安全中心，我们不可能接触到多姿多彩的移动网络安全领域。他高屋建瓴的学术眼光、兢兢业业的工作精神，时刻指引着我们走向前方。

移动网络和移动网络安全是一个快速发展的领域，新的技术和应用会不断出现，我们真诚希望能够和大家经常交流。由于我们水平有限，书中错漏之处在所难免，如果大家对这本书有什么意见和建议，或者对移动网络安全和整个信息安全领域有什么要说的话，请来信至 mobilesecurity@163.com，我们欢迎一切善意的来信，但愿它能够成为我们交流的平台。

作者

2004 年 8 月

目　　录

概　　论

第一部分　移动安全技术

第二部分 移动安全攻与防

第三部分 部署移动安全

第四部分　移动安全应用

附　录

概　　论

第 1 章　保护从何处开始

本章要点

要保护移动网络，首先要对移动网络有所了解。

自从 20 多年前移动网络的概念第一次被提出来，移动网络所带来的灵活性和便利性极大地激发了科学家、厂商和用户的想像力，大大改变了人类的生活方式。移动网络主要包括两类：移动通信网络和无线局域网。它们代表了 21 世纪通信网络技术的发展方向。

整本书的讨论都是基于这两类移动网络进行的。读完本章，你可以对移动网络技术和移动网络面临的安全问题有一个完整的理解，使你认识到安全问题在使用移动网络过程中的重要意义和特殊作用。

本章主要包括以下内容：

- ❖ 移动通信网络
- ❖ 无线局域网
- ❖ 移动网络特点
- ❖ 移动网络面临的安全威胁

1.1　移动网络技术概述

移动网络正在改变着我们的生活。随着无线网络技术的发展，我们能够以前所未有的方式接入无线和有线网络，传送的信息从开始的语音、文本等数据向多媒体数据转变。通过手机、PDA、装有无线网卡的笔记本等无线终端设备，我们可以随时随地接入 Internet，查看 Email、浏览股市行情、下载有用信息，把网络装进自己的口袋。

移动网络是继 Internet 之后网络发展的新热点，移动终端的生产量已经超过了个人电脑的生产量，这一点可以从 IDC 的报告中看出来，如图 1-1 所示。

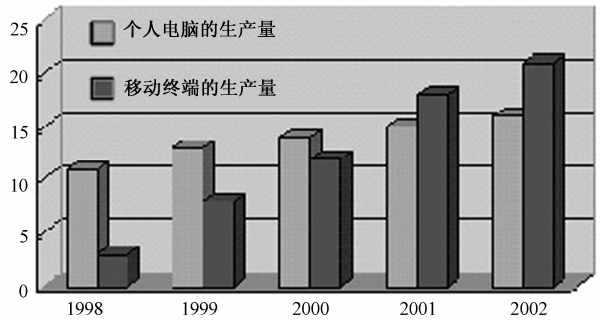

图 1-1　个人电脑和移动终端生产量比较

然而，移动网络是一把双刃剑。由于移动网络把利用空间传播的电磁波作为信息的载体，

电磁波没有明显的界限，因此移动网络比有线网络更容易遭受攻击，任何人都有可能窃听或者干扰信息。移动网络用户拥有更多便利性和灵活性就意味着他们将面临更多风险，这些风险包括搭线窃听、冒充用户、冒充网络、信息篡改、伪造、干扰、新式病毒、盗版等。如何解决这些问题也就是这本书要讨论的内容。

现有的移动网络技术提供了众多的解决方案，所有这些解决方案使用的常用移动网络互连形式可以归结为以下两种：

- 移动通信网络。
- 无线局域网。

移动通信网络是指以手机作为主要终端设备的语音/数据通信；而无线局域网是指以装有无线网卡的台式机或者笔记本为主要终端设备的局域和室内数据通信，无线局域网同时为未来多媒体应用（语音、数据和图像）提供了一种潜在的手段。

1.1.1 移动通信网络

移动通信网络以手机作为最主要接入设备，网络建设一般采用蜂窝式解决方案。到目前为止，移动通信网络按照其发展可以分为第一代、第二代和第三代移动通信技术。第一代移动通信技术基于模拟的 FDMA 技术，已经基本被淘汰。随着移动通信技术的发展，又出现了 2G、2.5G、3G，甚至 4G 移动通信技术。

1．2G 移动通信网络

2G 移动通信网络主要指 GSM 移动通信技术。全球移动通信系统（Global System for Mobile Communication，GSM）是欧洲电信标准协会（European Telecommunications Standards Institute，ETSI）为第二代移动通信制定的可国际漫游的泛欧数字蜂窝系统标准。1982 年，公用陆地移动网（Public Land Mobile Network，PLMN）成立了 GSM 工作组，这个工作组的主要目标就是制定一个第二代移动通信标准，以解决欧洲各国因使用 6 个不同的第一代模拟蜂窝系统而造成的无法漫游问题。1989 年，ETSI 接手 GSM。1991 年标准规范制定完成。GSM 综合了语音和数据业务，不仅提供移动电话服务，还提供了一系列的其他业务。表 1-1 和表 1-2 分别给出了 GSM 第一阶段和第二阶段所能提供的各项业务。

表 1-1　GSM 第一阶段业务

业务类型	业务项目	说　明
用户终端业务	电话	全速率为 13kbps 语音
	紧急呼叫	GSM 的紧急呼叫号码是 112
	短消息业务	点到点（两用户之间）和小区广播类型
	可视图文接入	
	智能用户电报、传真等	
承载业务	异步数据	300～9600 bps（透明/非透明传输）
	同步数据	2400～9600 bps 透明传输
	同步分组数据	
补充业务	呼叫转发	当用户不可达时，转移所有呼叫
	呼叫阻塞	限定特定的呼叫

表 1-2　GSM 第二阶段补充的业务

业 务 类 型	业 务 项 目	说　　明
用户终端业务	半速语音编码器	可选择实现
	增强全速率	
补充业务	主叫线路识别	显示或限制呼叫方的 ID
	被连接线路识别	显示或限制被呼叫方的 ID
	呼叫等待	当前通话过程中引入呼叫
	呼叫保持	保持当前通话而进行另一次通话
	多方通信	一次通话中同时进行 5 个呼叫
	封闭用户群	
	收费通知	在线收费通知
	运营商决定呼叫阻塞	运营商限制个人用户的一些功能

GSM 系统有 3 个主要组成部分：移动台（Mobile Station，MS）、基站子系统（Base Station Subsystem，BSS）、网络和交换子系统（Network Switching Subsystem，NSS）。三者之间的关系可以用图 1-2 表示。

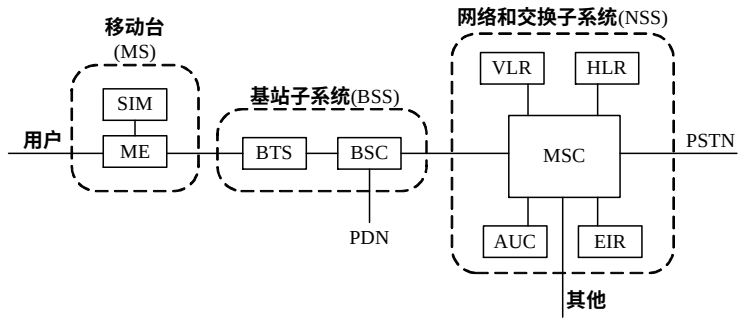

图 1-2　GSM 参考体系结构

GSM 体系结构中更多的部件以及部件间的关系如图 1-3 所示。

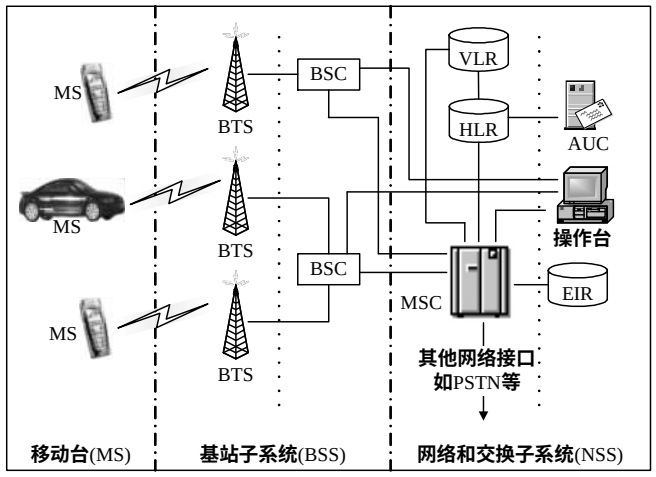

图 1-3　GSM 参考体系结构的各个部分