IT先锋系列丛书

宽带网络与设备安全

BROADBAND NETWORK & DEVICE SECURITY

Benjamin M. Lail 著
李海燕 雷琳 李高升 等译

Mc Graw Hill Education

人民邮电出版社
POSTS & TELECOM PRESS

IT 先锋系列丛书

宽带网络与设备安全

Benjamin M. Lail 著

李海燕 雷 琳 李高升 等译

人 民 邮 电 出 版 社

图书在版编目（CIP）数据

宽带网络与设备安全/（美）莱尔（Lail,B.M.）著；李海燕等译. —北京：人民邮电出版社，2004.2

（IT 先锋系列丛书）

ISBN 7-115-11049-2

Ⅰ.宽… Ⅱ.①莱… ②李… Ⅲ.宽带通信系统—综合业务通信网—安全技术 Ⅳ.TN915.142

中国版本图书馆 CIP 数据核字（2003）第 124558 号

IT 先锋系列丛书

宽带网络与设备安全

◆ 著 Benjamin M.Lail

译 李海燕 雷 琳 李高升 等

责任编辑 梁 凝

◆ 人民邮电出版社出版发行 北京市崇文区夕照寺街 14 号

邮编 100061 电子函件 315@ptpress.com.cn

网址 http://www. ptpress.com.cn

读者热线 010-67129258

北京汉魂图文设计有限公司制作

北京顺义振华印刷厂印刷

新华书店总店北京发行所经销

◆ 开本：800×1000 1/16

印张：21.5

字数：459 千字 2004 年 2 月北京第 1 版

印数：1－4 000 册 2004 年 2 月北京第 1 次印刷

著作权合同登记 图字：01-2003-1673 号

ISBN 7-115-11049-2/TN・2018

定价：36.00 元

版 权 声 明

Benjamin M.Lail

Broadband Network & Device Security

ISBN: 0-07-219424-3

北京市版权局著作权合同登记图字：01-2003-1673 号

内 容 提 要

本书全面系统地阐述了设计、建立以及实现宽带网络安全的理论与应用。全书分为3个主要部分及两个附录。其中，第1部分为第1～5章，主要内容有：宽带网络的总体概述；密码系统和密码安全机制；存在于公共宽带网络的安全威胁及解决的方法；TCP/IP的脆弱性；OSI及TCP/IP网络参考模型；流行的宽带接入技术；服务质量的概念；现存的宽带服务标准和规范。第2部分为第6～8章，主要内容有：IP安全；安全套接层/传输层安全；Kerberos网络认证安全；安全服务的布局和不同网络层内的机制；为实时多媒体应用而设计的网络安全解决方案的性能、成本和易管理性；严格的QoS需求的其他应用；嵌入装置的安全约束。第3部分为第9～12章，主要内容是大量的实例学习和设计方案，内容包括：有保障高速互联网接入的安全；IP电话技术和实时多媒体应用以及交互式电话。最后从最底层开始，给出了设计宽带网络安全基础架构的各个步骤，并且还提出了两个设计方案来测试读者对全文的理解程度。

本书的最大特点就是：概念清晰易懂，阐述详细透彻，理论与应用紧密相结合，是一部反映当今宽带网络安全这一领域发展和研究水平的难得的佳作。

本书的对象主要是网络安全设计师和硬件设计工程师。当然，网络安全新手们在学习许多重要的安全原理时，也能从此书找到一些普遍问题的答案。更高级的读者将会从密码学、公开密钥基本技术、网络安全威胁和防攻击、网络安全的协议以及目前宽带网络安全标准和规范等方面的详细实例学习中受益匪浅。本书还总结了实际的设计范例，使任何水平的读者都有机会学以致用。

译 者 序

本书是美国最新出版的电子安全系列丛书之一，内容覆盖了最新的网络安全技术，受到了学者们广泛的关注和高度的评价。

本书的作者 Benjamin M. Lail 是 RSA 安全有限公司中开发方案组的高级系统工程师。专攻宽带网络安全基础结构和解决方案。他还是微软的系统工程师和 CCNA，并且在信息安全性的诸多方面都很有经验，其工作涉及加密学、公开密钥匙基础架构、网络和路由器安全、保护因特网和电子商务交易，以及众多的安全协议和规范。

有人说宽带时代的来临为解决网络泡沫化带来一线生机！事实上，频宽的问题克服后，加上影音资讯传输，的确为网络产业打开了另一扇大门，只是在这扇大门后面，却隐藏许多危机，网络安全就是一项相当重要的议题。网络安全不是只有病毒：病毒固然可怕，而资料安全管理问题更加严峻！对大型网站或大企业而言，网络管理工作很早就是公司经营阶层非常重视的课题，问题是对许多中小企业或传统企业而言，所谓网络安全的观念似乎还是停留在病毒防范阶段，只知道必须安装防毒软件，对于防火墙的架设却常常被忽略。

尤其是当网络与通信结合之后，新的网络安全问题势必产生，这些安全问题绝对不是一般人所能理解与防范的。当多数人把重心放在如何玩宽带的同时，却也悄悄埋下网络安全的"未爆弹"！因此，不管是网站经营者或传统企业经营者，在高高兴兴迎接宽带时代来临的同时，不妨多花一些时间和精力去学习、掌握网络安全发展的新趋势，去学习如何避免安全漏洞的产生，防患于未然。何况网络安全一旦出现问题，很可能就是大问题。人们在开心享受宽带所带来各项便利与商机的同时，别忘了网络安全这个大黑洞，同时也应随时吸收或引进最新网管技术或人员，以确保网络环境的安全。

值得庆幸的是，到现在为止，人们已经建立起来的许多思想是有效的，可以使软件开发者、硬件设计者以及公司和事业机构的 IT 职业人士深入了解设计、建立以及实现安全宽带网络的技术。这样做，企业就能够在保护它们客户隐私的同时确保它们服务的可用性和完整性。

本书是作者为工作在网络安全设计和硬件设计领域的人员精心撰写的，是一部不可多得的佳作。

本书由雷琳、李高升、袁青、齐占杰、刘立业等翻译，李海燕统校全书。陈德莉也给予了我们不少的帮助和支持。译者在此表示衷心的感谢！

在翻译过程中，对于已发现的原书中的少数疏漏和排印错误都一一作了勘正，但限于译者的学识水平，加上时间仓促，错误和不妥之处在所难免，恳请读者批评指正。

译者

序

欢迎阅读本书。这本书是RSA出版社最新出版的关于e-安全的系列丛书之一，其内容覆盖了最新和最关键的网络安全领域。尽管宽带在20世纪60年代有线（电缆）电视出现时就产生了，但直到80年代宽带技术才开始用于计算机网络。在90年代末期，基于宽带的DSL和电缆调制解调器推动了因特网的飞速发展以及音频和视频在Web上的利用。

目前，有4种主要的宽带接入技术：DSL、电缆、固定无线电和双向卫星。它们——以及与它们连接并提供各种各样服务的网络——都易受安全破坏、入侵，以及业务偷窃的攻击。这就使得组织和个体在使用这些技术时要冒很大的风险——从截获未经授权的数据到身份窃取。

有经验的宽带用户可能已经了解到了在他们电脑上安装个人防火墙和反病毒软件的重要性。但是除非根本的宽带网络下部构造得到安全保障，否则没有什么是安全的。其次，此书旨在帮助软件开发者、硬件设计者以及公司和事业机构的IT职业人士来设计、建立并实现安全的宽带网络。这样做，组织机构就能够在保护它们客户隐私的同时确保它们服务的可用性和完整性。

本书由RSA安全高级系统工程师Benjamin M. Lail著述，全书分为3个部分。第1部分向读者介绍了宽带网络的历史和发展，各种安全性威胁，基本的安全服务和对付这些威胁的机制，以及在有线和无线环境中目前所使用的安全标准。这些内容为读者在第二部分全面理解如何为宽带网络设计安全系统提供了背景信息。

第2部分是本书的核心部分。它从讨论通信协议特性开始，向读者介绍了大量的安全协议，包括IPSec、SSL/TLS以及Kerberos。后继的章节提出了宽带网络中安全防范的物理措施，实现网络中这些组件而造成的冲突和影响（包括性能、代价、互用性和易处理性），以及为弥补这些冲突而采取的措施。

在第3部分中，通过实例学习来阐明保障宽带接入、IP应用中的声音和随选多媒体服务的安全所需的实际步骤。这些设计方案一步一步地引导读者从头开始来分析和建立一个安全性基础架构。本书有两个有价值的附录——“TCP/IP入门”和提出了TCP/IP协议族、数字证书和PKI概念的“数字证书和公开密钥的基本结构”。

我们希望读者将会从RSA出版目录中的这一主题和其他主题的阅读中有所收益。我们永远欢迎您对本书提出意见和建议。有关RSA安全的更多信息请参阅我们的网页www.rsapress.com。

Victor Chang
Vice President，Engineering
RSA Security Inc.

关 于 作 者

Benjamin M. Lail 是 RSA 安全有限公司中发展方案组的高级系统工程师，专攻宽带网络安全基础结构和解决方案。他是微软系统工程师和 CCNA，并且在信息安全性的诸多方面都很有经验，其工作涉及加密学、公开密钥匙基础架构、网络和路由器安全、保护因特网和电子商务交易，以及众多的安全协议和规范。在加入 RSA 之前，Ben 是 Advance Micro Devices 公司的系统管理员和戴尔计算机公司的技术经理，他也是企业会议和研讨会的经常发言人。

致　谢

首先，我要感谢我的家人和朋友，感谢他们在我编写此书期间对我的支持。编写此书期间，我有时会感到有很大的压力，有时甚至忘记了编写这本书对身旁的人会造成很大的影响。我也要感谢我的父母，Mike 和 Debi，感谢他们对我的教育和事业的热情支持。感谢我的弟弟——Torry，使我尽可能地努力奋斗成最好的行为榜样。特别要感谢我的妻子—— Anastasia 是她的爱陪伴我度过了许多紧张的日子和无眠的夜晚。

此外，我还要感谢所有为此书作出贡献的人。感谢 Osborne/McGraw-Hill 的每个人为完成此书作出的特别努力。感谢 Jane Brownlow、Emma Acker 和 Julie Smith（我的责任编辑、合作者以及项目编辑）的悉心引导，确保了我按时完成此书。感谢我的初审员 Nancy McLaughlin，他的细心校正让我看起来好像有地道的英语水平。感谢排序员 Kelly Stanton-Scott 和 John Patrus 以及插图画家 Lyssa Wald 和 Michael Mueller，他们让此书栩栩如生地呈现在读者面前。感谢 Eric Rosenfeld 给与此书广泛的领域洞察力和专业技术评论。最后，但不是最少的，我要特别致谢我的同事 Peter Yee、Steve Schmaiz、Jim Gray 和 Martin Euchner，他们的帮助确保了本书技术材料的正确性。

前　言

宽带是网络领域中顶尖的时髦词语。但是它不仅仅是一个时髦的词语，高性能宽带网络确实提供了许多令人激动的机会。宽带网络使服务提供商能够提供那些对带宽需求量大的多媒体应用，这些应用不仅是刺激感官，而且还改善了我们的日常生活。宽带网络还为我们提供了大量信息以及娱乐、通信和商业服务。这些无所不在的信息存取和接入服务并不是免费的，然而，服务的多样性和持续可用性却意味着同时存在着窃取者、故意破坏者和偷听者的频繁威胁，他们意在用你的费用来获得他们的非法所得。

当我们越来越依赖于宽带网络以及它们所提供的服务时，网络基础结构的安全性也变得极为重要起来。未经授权揭露秘密信息、拒绝可用性以及窃取服务都会对用户、公司和服务提供商造成极大的威胁，尤其是在财政损失和名誉毁坏方面。网络结构正变得越来越复杂，而且将比以前支持更加多样化的应用。因此，安全技术师必需精通宽带网络安全设计和实现的基本原理。

除了反网络威胁以外，实时多媒体应用是服务提供商、企业和网络设备制造商在安全设计中必须考虑的另一因素。为了确保成功运行实时应用，安全防范设计还必须解决每个应用的单个服务质量特性。当使用不恰当时，安全机制可能会反过来影响多媒体内容的及时传输，甚至更糟的是，可能会使网络服务难于使用，并且在实现和维护上造成浪费。同时，考虑安全性与 QoS、代价和易管理性之间的关系也是信息安全专家的职责。

本书提出了以上所涉及的所有内容，旨在作为设计宽带网络安全的实际指南。同样地，为了实现实际和及时的应用安全技术，本书尽量避免涉及了数学上的理论推导和其他无关的内容。安全设计富有挑战性，但是利用此书提供的信息和方法，读者将会得到设计、实现以及建立更安全、更高性能以及成本更低的网络安全性结构的方法。

读者

这本书的对象主要是网络安全设计师和硬件设计工程师，使他们能更加清晰地理解安全的功能性、性能、代价以及易管理性。然而，并不是只有这些人才能受益于此书。虽然这本书覆盖了许多先进的主题，但是当网络安全新手们在学习许多重要的安全原理时，他们也能从此书中找到一些常见问题的答案。更高级的读者将会从密码学、公开密钥基本技术、网络安全威胁和防攻击、网络安全协议以及目前宽带网络安全标准和规范等方面的详细实例中受益匪浅。本书总结了实际的设计例子，以使任何水平的读者都有机会学以致用。

从本书中您将学到什么

此书分为3个主要部分及两个附录。第1部分向读者介绍网络及网络安全的基础知识，这正是后续章节要讨论的问题的必备知识。第1章给出了宽带网络的总体概述，讨论了它的发展及重要性。第2章主要介绍了安全服务问题，即密码系统和密码安全机制。第3章讨论了存在于公共宽带网络的安全威胁及解决的方法，而且阐述了TCP/IP的脆弱性。第4章介绍了OSI及TCP/IP网络参考模型，讨论了最流行的宽带接入技术，包括电缆、xDSL、固定无线上网和人造卫星，而且介绍了服务质量的概念，包括带宽、响应时间、信号抖动、信号损失、信号的有效性以及这些因素如何影响多媒体内容的传送。第5章概述了已存在的宽带服务的标准和规范。

第2部分讨论了宽带网络安全的设计技术。第6章讨论了一些流行的、普遍应用的协议，包括：IP安全、安全套接层/传输层安全、Kerberos网络认证服务——应用于许多网络环境中的商业安全。第7章讲解了安全服务的布局和不同网络层内的机制，讨论了对于特定的场合是基于主机的安全合适还是网关安全合适。第2部分的最后一章，第8章分析了为实时多媒体应用而设计的网络安全解决方案的性能、成本和易管理性，及有严格的QoS要求的其他应用，同时讨论了嵌入装置的安全约束问题，及怎样平衡这些装置的安全和性能。

第3部分提供了大量的实例和设计方案，给读者提供应用第1部分和第2部分中所讨论的安全原理和高级设计技术的机会。实例致力于当前电缆工业中的安全主动权，讨论了保障高速互联网接入的安全（第9章），IP电话技术和实时多媒体应用（第10章）以及交互式电话（第11章）等问题。第12章给出了设计宽带网络安全基础架构的各个步骤，从最底层开始，并且还提出了两个设计方案来测试读者对全文的理解情况。

书后的两个附录提供了大量关于TCP/IP协议族（附录A）、数字证书和公开密钥基础架构概念的附加信息。

目　录

第 1 部分　宽带网络安全的基本原理