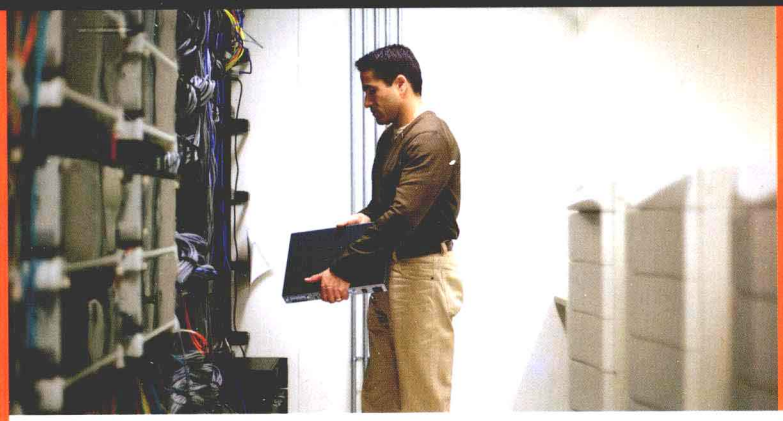
CISCO



SECURITY

IPv6安全

IPv6 Security

Protection measures for the next Internet Protocol

〔美〕 **Scott Hogg**，CCIE #5133
Eric Vyncke 著

王玲芳　李沛　陈海英　李虹　译
王劲林　审

人民邮电出版社
POSTS & TELECOM PRESS

IPv6安全

IPv6 Security

〔美〕Scott Hogg，CCIE #5133 著
Eric Vyncke

王玲芳　李沛　陈海英　李虹　译
王劲林　审

人 民 邮 电 出 版 社
北　京

图书在版编目（CIP）数据

IPv6安全 / （美）霍格（Hogg, S.），（美）维恩克（Vyncke, E.）著；王玲芳等译. -- 北京：人民邮电出版社，2011.5
ISBN 978-7-115-25044-5

Ⅰ. ①I… Ⅱ. ①霍… ②维… ③王… Ⅲ. ①计算机网络－传输控制协议 Ⅳ. ①TN915.04

中国版本图书馆CIP数据核字(2011)第036726号

版权声明

IPv6 安全

◆ 著　［美］Scott Hogg　CCIE#5133　Eric Vyncke
译　王玲芳　李　沛　陈海英　李　虹
审　王劲林
责任编辑　傅道坤

◆ 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　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京鑫正大印刷有限公司印刷

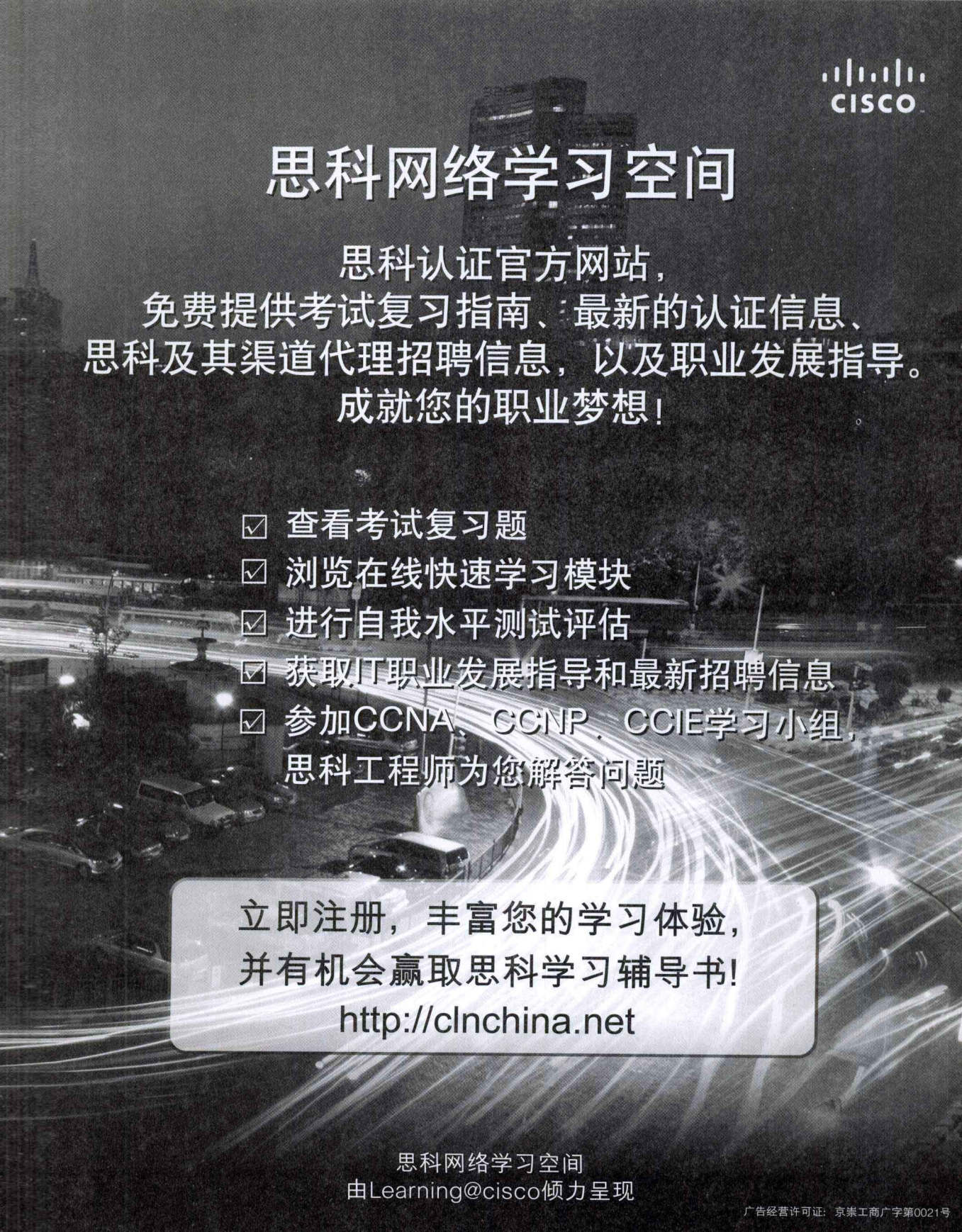
◆ 开本：800×1000　1/16
印张：32.75
字数：679 千字　2011 年 5 月第 1 版
印数：1－3 000 册　2011 年 5 月北京第 1 次印刷

著作权合同登记号　图字：01-2010-3830 号

ISBN 978-7-115-25044-5

定价：88.00 元

读者服务热线：(010)67132705　印装质量热线：(010)67129223
反盗版热线：(010)67171154



内容提要

本书综述 IPv6 网络所面临的威胁，并提供应对这些威胁的解决方案，内容涵盖这些问题和当前的最佳实践。本书首先讲述安全威胁，然后描述应对这些威胁的方式，列出所有的风险，并针对每种威胁指明存在的解决方案。通过本书，读者将学习到攻击者可能用以攻破你的网络的技术以及如何使用 Cisco 的产品保护你的网络。本书的目的是较深入地研究协议，并从一名安全实践人员的角度讨论协议细节。本书涵盖理论知识，也同时给出实践例子。

本书适合负责网络安全的 IT 工作人员和在校学生阅读；另外，本书也可以作为从事网络安全的研究人员和学者的参考书。

关于作者

Scott Hogg，CCIE No.5133，是一名拥有 17 年以上经验的网络计算咨询师。Scott 提供网络工程、安全咨询和培训服务，重点放在提供可靠的、高性能的、安全的和成本有效的网络解决方案。他拥有科罗拉多州立大学计算机科学的学士学位和科罗拉多大学电信硕士学位。除了 CCIE 之外，他还拥有 CISSP（No.4610）和许多其他厂商和行业认证。Scott 曾经为许多大型企业、服务提供商和政府机构设计和实施网络，并对其网络进行故障排除。过去 8 年，Scott 一直在研究 IPv6 技术。Scott 撰写了有关 IPv6 的几篇白皮书，并对 IPv6 技术进行过多次演讲和展示。目前他也是落基山 IPv6 任务工作组的主席，并是全球技术资源公司（GTRI）高级技术服务的总裁（Director），该公司的总部位于科罗拉多丹佛（Denver），是 Cisco 的一个金牌合作伙伴。

Eric Vyncke 是一名出色的系统工程师，目前以安全技术顾问的身份供职于 Cisco，主要负责欧洲的安全事务。20 年来，他的主要专业知识领域一直是从二层到应用层的安全。他曾经帮助过几家机构安全部署 IPv6。过去 8 年间，Eric 参加了 IETF（他是 RFC 3585 的作者）的相关工作。Eric 作为发言人经常会出现在安全事务活动中（如著名的 Cisco Live[前身是 Networkers]），他还是比利时数所大学安全研讨班的客座教授。他拥有比利时列日大学计算机科学工程的硕士学位，在加入比利时网络研究所（Network Research Belgium）之前，他是该大学的一名研究助理，在比利时网络研究所，他是 R&D 部门的主任；之后他加入西门子公司，并担任安全项目（包括代理防火墙）的项目经理。他曾经与他人共同撰写了 Cisco Press 出版的书籍《LAN Switch Security》。他也拥有 CISSP 认证（No.75165）。

关于技术审稿人

Joseph Karpenko 目前是 Cisco 安全智能工程部门的一名高级工程师。Joseph 是拥有 10 年技术经历的资深人士，专业领域为网络、安全、数据中心和系统管理。目前 Joseph 负责开发可阻止、检测并防止已有的、当前的和即将出现的威胁和攻击的安全解决方案。他也一直是涉及安全主题的多个会议的主题演讲人。

在其职业生涯中，Joseph 曾经客户共同设计、实施大型企业和数据中心网络，以及安全架构。在加入 Cisco 之前，Joseph 作为一名系统管理员和高级工程师，负责对复杂的安全和网络事件进行处理和排错。Joseph 与他的妻子、女儿以及他们毛茸茸的四足家庭成员（chocolate lab）生活在德州，在闲暇时间他喜欢钓鱼。

Darrin Miller 是 Cisco 公司安全技术组的一名工程师。Darrin 负责系统级别的安全架构。他在 Cisco 的主要工作是基于策略的准入、事件响应和下一代架构。在加入安全技术组之前，Darrin 是一名安全研究人员，重点关注身份识别、NAC、IPv6、SCADA、事件响应和信任模型等领域，其工作包括协议安全分析和下一代网络的安全架构。Darrin 写过几本网络安全相关的图书和白皮书。在世界各地举行的各种主题的重要网络安全会议上，Darrin 也作过演讲。在加入 Cisco 公司工作之前，Darrin 曾担任过网络安全团体的多个职务。

献辞

本书献给 David Hogg。我想他将以我为荣。

——Scott Hogg

献给我的家庭、我父母 Ghislaine 和 Willy、我妻子 Isabelle 和我的孩子 Pierre 和 Thibault。

——Eric Vyncke

致谢

我必须首先感谢我的爱妻 Stacy 和我们的孩子 Ian 和 Lauren，感谢我的孩子对他们的父亲沉溺于 IPv6 的支持。也感谢我的父母，感谢他们在 1982 年给我买了一台苹果 II 型计算机，这掀开了我对学习各种数字化事务的挚爱生涯。

我乐意借此机会感谢我在落基山 IPv6 任务组和北美 IPv6 任务组的同事们。感谢 Jeff Doyle，感谢他的鼓励和智慧之言。感谢美国 NTT 的 Chuck Sellers，感谢他的友谊和在 MIPv6 方面的协作。还要感谢 IETF，感谢它在 IPv6 方面所做的工作。我的优势是站在了这些巨人们的肩膀上。

我还要感谢我的合著者 Eric Vyncke，感谢他在本书的创作方面为我提供如此卓越的引导和反馈。感谢 Cisco 公司的 Cliff Bruce，感谢他给我提供使用 Cisco 测试设备的机会。

——Scott Hogg

我想要感谢使本书最终得以出版的许多人：我的雇主 Cisco 公司，我的经理 Barb Fraser 和 Jane Butler。没有他们的支持，本书不可能出版。另外，我还要感谢 Cisco 公司中对本书出版工作做出贡献的如下人员：Michael Behringer、Steinthor Bjarnason、Eric Levy-Abegnoli、Benoît Lourdelet、Shannon McFarland、Chip Popoviciu、Gregg Schudel 和 Gunter Van de Velde。我还要感谢 Michel Fontaine、Simon François、Yves Wesche (列日大学)、Patrick Grossetête (Archrock)和所有支持过我的 IPv6 倡议的其他人。没有我的合著者 Scott 的协作和干劲，本书也许将永远不出版。谢谢你，Scott！

——Eric Vyncke

我们也感谢我们的技术审稿人，是他们确保了本书内容的质量：Cisco 公司的 Joe Karpenko 和 Darrin Miller。最后，感谢我们的编辑 Brett Bartow 和 Dayna Isley，以及 Cisco Press 的团队，感谢他们与我们一起工作，并使本书跟上出版的进度。为了提高本书的质量，他们所有人都付出了大量的时间和精力。

——Scott 和 Eric

译者序

IPv6 的前身是人们如今普遍使用的互联网的核心协议 IPv4。自互联网诞生以来，伴随网络环境的逐渐变化，网络从相互协作的团体演变为充满欺骗、盗窃和伪装等互不信任的团体，这也是如今互联网的社会化层面。在不久的将来，IPv4 必将逐步为 IPv6 所替代。在这个过程中，IPv6 互联网除了要面对协议本身的安全问题外，还要应对 IPv4 向 IPv6 迁移过程中存在的安全威胁。针对安全威胁，未雨绸缪往往比亡羊补牢更加有效，即“宁可求稳，以免事后后悔”，这正是作者撰写本书的初衷。

本书综述了 IPv6 网络面临的种种威胁，并提供了应对这些威胁的解决方案和最佳实践。本书首先讲述安全威胁，然后描述应对这些威胁的方式，列出所有的风险，并针对每种威胁指明存在的解决方案。通过本书，读者将学习到攻击者可能用以攻破你的网络的技术以及如何使用 Cisco 的产品保护你的网络。本书的目的是较深入地研究 IPv6 协议，并从一名安全实践人员的角度讨论协议细节。

本书由王玲芳、李虹负责全书统稿和校对工作，李沛（信阳职业技术学院）翻译第 4 章～第 8 章，陈海英（华中农业大学）翻译第 9 章～第 12 章，王玲芳翻译了其他章节。本书内容繁巨，在翻译过程中，董辉、范伟娜、方淑英、冯翔、付铭、甘静宜、高俊梅、龚凯、顾培蒂、郭超海、郝琴、何芳、贺季敏、黄梅、贾春泽、李丹、刘丽、罗莹等同志参与了部分的翻译工作，在此表示感谢。同时感谢人民邮电出版社的编辑和相关同志，没有他们的帮助和鼓励，本书不可能出版。

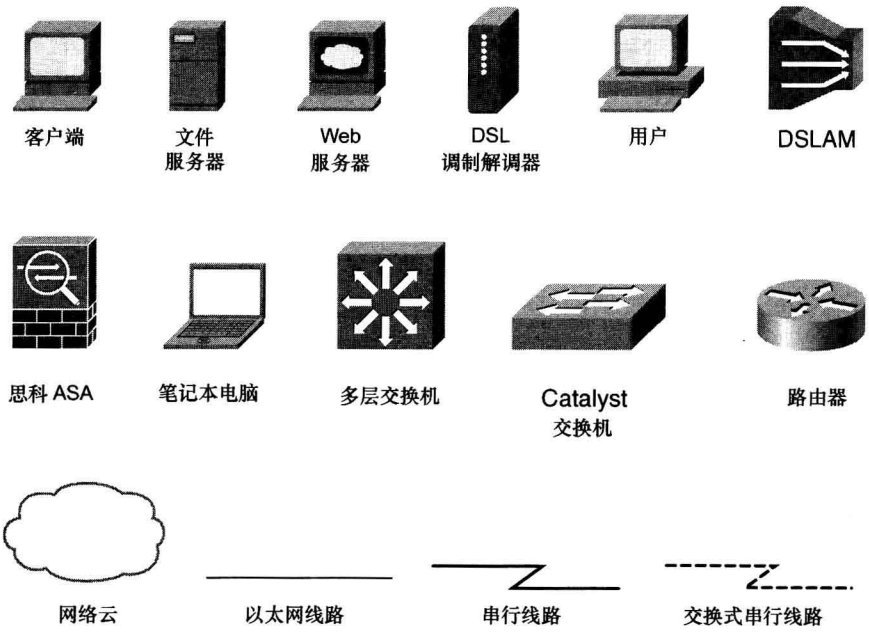
另外，本书的翻译工作得到国家高技术计划项目（2008AA01A317）、国家科技支撑计划项目（2008BAH28B04）和国家自然科学基金项目（60972082）等的支持，在此一并表示感谢。

需要指出的是，本书的内容仅代表作者个人的观点和见解，并不代表译者及其所在单位的观点。另外，由于翻译时间比较仓促，疏漏错误之处在所难免，敬请读者原谅和指正。

译　者

2011 年 4 月于北京

本书使用的图标



命令语法惯例

本书命令语法遵循的惯例与 IOS 命令手册使用的惯例相同。命令手册对这些惯例的描述如下。

- **粗体字**表示照原样输入的命令和关键字，在实际的设置和输出（非常规命令语法）中，粗体字表示命令由用户手动输入（如 **show** 命令）。
- *斜体字*表示用户应提供的具体值参数。
- 竖线（|）用于分隔可选的、互斥的选项。
- 方括号（[]）表示任选项。
- 花括号（{}）表示必选项。
- 方括号中的花括号（[{}]）表示必须在任选项中选择一个。

前言

Internet 协议版本 6（IPv6）是用于 Internet 的通信协议（IPv4）的下一版本。IPv6 是一种已经出现了许多年的协议，但还没有替代 IPv4。IPv4 诞生时，它存在一些当时没有预料到的限制。因为 IPv6 克服了这些限制中的许多限制，所以它是 IPv4 的唯一可用（viable）的长期替代协议。

虽然向 IPv6 的迁移已经开始，但仍然处在迁移的早期阶段。许多国际组织机构已经有了 IPv6 网络，美国联邦机构正在进行向 IPv6 的迁移工作，而其他国家正在思考 IPv6 对他们意味着什么。虽然许多组织机构已经有了运行在他们网络之上的 IPv6，但是他们甚至没有意识到。现在许多计算机操作系统默认地运行 IPv4 和 IPv6，如果其中一种协议的安全性弱于另一种协议的话，这就会造成安全攻击。目前 IPv6 存在安全攻击，随着 IPv6 协议受欢迎程度的增加，其安全威胁的数量也会增加。

当一名安全官员想保证一个组织机构的网络安全时，他必须知道所有潜在的威胁，即使这种威胁是一个已经有 10 年之久的协议，而且该协议的流量甚至小于 2008 年 Internet 总流量的 1%。不要被这 1%欺骗：这个数字在未来数年注定会增加，很可能你的网络已经遭受了一些 IPv6 威胁。宁可求稳，以免事后后悔。

正像许多技术的早期部署一样，安全经常留给实施的最后阶段。我们撰写本书的意图是从早期 IPv6 部署的第一天起就改善它的安全性。正在考虑 IPv6 或已经处在 IPv6 迁移之中的任何组织机构应该都不会想部署刚开始就不安全的新技术。向 IPv6 的迁移是不可避免的，因此本书将帮助你理解存在于 IPv6 网络中的威胁，并为你提供应对这些威胁的方式。因此，本书就如何提高 IPv6 网络的安全性给出了指导。

目标和方法

当前，尽管网络基础设施已经为支持 IPv6 传输而准备到位，但许多组织机构还是放慢了向 IPv6 迁移的进程，原因是他们意识到 IPv6 的安全产品也许还不充足。他们意识到，在没有首先评估这个新协议的安全性之前，他们不能部署 IPv6。本书的意图是综述 IPv6 网络面临的威胁，并提供应对这些威胁的解决方案。本书涵盖了这些问题和当前的最佳实践。

本书首先讲述安全威胁，然后描述应对这些威胁的方式。通过列出所有的风险，并针对每种威胁指明存在的解决方案，这样迁移到 IPv6 时，你可能感觉更舒心、放心。你将学习到攻击者可能用以攻破你的网络的技术以及使用 Cisco 的产品保护你的网络。

但是，指明攻击而不给出解决方案，从社会角度看是不负责任的，所以本书重点关注当前可以使 IPv6 网络更安全的技术，以及最佳实践。通过阅读本书，读者可以全面理解 IPv6 的各种安全主题。

本书读者

负责保护计算机网络安全的 IT 工作人员是本书的阅读对象。读者应该已经具备 IPv6 和网络技术的基础知识。本书不是 IPv6 的介绍性书籍，市面上已经存在 IPv6 的入门类图书和在线资源，也已经存在与计算机网络安全相关的许多经典巨著，读者可以根据需要进行阅读。

本书的目的是较深入地研究 IPv6 协议，并从一名安全实践人员的角度讨论协议细节。本书是由专家撰写的针对专家的一本书。本书涵盖理论知识，也同时给出了可以实施的案例。

本书的组织结构

本书以 IPv6 协议安全特征的基础开始描述。本书的前面一些主题是如下安排的：从一个组织机构网络的外围周边设备向内深入到 LAN 和服务器群。本书后面的章节讲解高级主题。读者可以从开头到结尾的方式阅读本书，也可以跳跃式地阅读本书。读者最好阅读完每个章节，以获得相关主题内容的全面知识。

本书的一些信息（例如表格和命令）是用于参考的。在具体实施的时候，你应该返回来参考本书。这就为读者提供了可遵循的放之四海而皆准的例子，它们应该与保障 IPv6 安全的当前最佳实践相一致。读者不要仅仅浏览本书，而要实践所列出的每条命令。读者可在这些命令上进行一些基础研究，从而确保它们能按照预期执行。

IPv6 安全是一个极活跃的研究领域，在本书撰写之后，人们将不断开发出新的协议和新的产品。我们希望本书会有多年的“书架寿命”，原因是即使 Cisco 公司的安全产品随着威胁态势而持续演化，本书的概念将仍然有效。在本书出版之时，我们将尽其所能保证本书的内容是最新的，但仍然建议读者在阅读时检查是否出现了新的方法。随着 IPv6 得到更广泛的部署，IPv6 安全领域会快速地发生演化。

第 1 章～第 12 章涵盖如下主题。

- **第 1 章，“IPv6 安全介绍”**：本章重新介绍了 IPv6，描述了 IPv6 部署得有多广泛，讨论了它的弱点，并讲解了黑客已经知道的有关 IPv6 的知识。本章给出一些初步的缓解技术。
- **第 2 章，“IPv6 协议安全弱点”**：本章讨论了 IPv6 协议自身具有的安全隐患，讲解了与 ICMPv6 和 IPv6 首部结构有关的安全问题。本章展示了协议弱点，并给出缓解那些风险的解决方案。本章也讲解了 IPv6 网络勘查和地址欺骗的安全问题。
- **第 3 章，“IPv6 Internet 安全”**：本章讲解了针对 IPv6 Internet 的大型威胁，并描述了可防止那些威胁的网络周边（perimeter）过滤技术。除了其他服务提供商所关注的安全实践措施外，本章还详细描述了 BGP 端对端的安全问题。IPv6 MPLS 安全、客户设备的安全、IPv6 前缀指派（delegation）安全和多宿方等内容也在本章中有所讲述。
- **第 4 章，“IPv6 周边安全”**：本章讲解 IPv6 的周边网络所存在的安全威胁，以及部署在网络周边的常见过滤技术。本章还讲解了 IPv6 访问列表、IOS 防火墙特征集合和 PIX/ASA/FWSM 防火墙。
- **第 5 章，“局域网安全”**：本章仔细讲解了针对 LAN 的威胁。IPv6 接入网络上存在许多弱点，本章在讲解这些弱点的同时也一并讲解了缓解这些弱点的许多解决方案。本章讲解了 LAN 中的邻居发现协议、自动配置寻址和 DHCPv6 通信等问题，还回顾了 SEND，并描述了实施 SEND 的方法。
- **第 6 章，“加固 IPv6 网络设备”**：本章讲解了可对运行 IPv6 的网络设备实施的安全改进，回顾了保障网络设备安全的相关技术。本章还讲解了保护路由协议的方式，以及第一跳路由冗余协议的知识。除了讲解控制网络流量的方式外，本章还详细给出控制设备资源的技术。
- **第 7 章，“服务器和主机安全”**：本章讲解了保护运行 IPv6 的计算机的方式，其中，重要的是加固 IPv6 节点，使之远离目前存在的威胁。本章详细讲解了 Microsoft、Linux、BSD 和 Solaris 操作系统的 IPv6 安全技术，还讲解了如何使用基于主机的防火墙和 Cisco 安全代理（CSA）来保护 IPv6 主机。
- **第 8 章，“IPSec 和 SSL 虚拟专网”**：本章讲解了 IPSec 的基础知识，还回顾了使用 IPv6 设置站点到站点 VPN 链路、动态多点 VPN 以及远程接入 VPN 的各项技术。本章还讲解了在 IPSec 客户端连接之上使用 ISATAP 的方法，以及 AnyConnect 客户端使用 SSL VPN 的方法。
- **第 9 章，“IPv6 移动性安全”**：本章讲解了移动 IPv6，并描述了保障这个协议的安全是多么具有挑战性。本章回顾了移动 IPv6，并讨论了移动 IPv6 的安全隐患。本章还给出了如何负责任地和安全地使用移动 IPv6 的建议，讲解了支持 IPv6 的移动解决方案和它们的安全隐患。
- **第 10 章，“保障迁移机制安全”**：本章讨论用于帮助组织机构从 IPv4 迁移到 IPv6

的各项技术。本章讲解了双栈、隧道和 NAT 迁移技术，以及它们的安全问题。这些技术都有其自身的安全隐患和保障流量安全的解决方案。本章通过给出一名攻击者如何试图侵入一个网络的例子，讲解了各种安全威胁。本章还讲解了在迁移过程中可用来保持网络安全的安全保护措施。

- **第 11 章，“安全监视”**：本章讲解了目前可用于监视 IPv6 网络安全的各种系统。监视一个网络以及这个网络上的计算机是任何安全实践措施的一个必备核心方面，IPv6 网络也是如此。因此应该合适地对其加以管理。本章还讲解了法庭证据（forensics）、入侵检测和防御、安全信息管理和配置管理等内容。
- **第 12 章，“IPv6 安全结论”**：本章综述了整本书讨论的常见主题，讨论了 IPv4 安全和 IPv6 安全之间的共性。本章包含了有关创建 IPv6 特定安全策略的讨论。本章还回顾了 IPv6 安全在未来是什么样子的，给出了 IPv6 安全建议的一个合并（consolidated）列表。

本章讲解如下主题。

- 重温 IPv6：IPv6 的简短回顾。
- IPv6 知识更新：描述 IPv6 的当前应用状态。
- IPv6 弱点：描述 IPv6 中的弱点，这是本书关注的重点。
- 黑客经验：讲解攻击工具和技能的当前状态。
- IPv6 安全迁移技术：介绍保障 IPv6 安全的高级方法。