“网管员必读”系列推出之后又一经典力作

网络工程师必读

——网络安全系统设计

NETWORK ENGINEER

王 达 编著
飞思科技产品研发中心 监制

◇ **一本真正全局意义上的安全系统设计类图书**

真正以OSI/RM七层结构为主线的安全系统设计类图书，较全面、系统地介绍了OSI/RM七层结构中各层的主要安全技术及其应用。

◇ **专业的一手技术资料**

本书所介绍的网络安全技术均来自相关技术或者协议的原始资料和真实的应用实践总结，技术原理介绍深入、系统、全面，填补了国内图书在这方面的空白。

◇ **庞大的读者服务体系**

提供了庞大、完善的读者服务体系，方便读者交流。包括11个读者QQ群，两大主流媒体（51CTO和CSDN）的专家博客，两个读者交流技术圈，一个学生大本营。详情参见其中一个博客：winda.blog.51cto.com。

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

王　达　　编著
飞思科技产品研发中心　　监制

网络工程师必读

——网络安全系统设计

NETWORK ENGINEER

必读

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

内 容 简 介

本书从网络工程师的职业角度出发组织和安排内容，非常具有针对性。本书从网络安全系统设计全局出发，以 OSI/RM 的 7 层结构为主线，层层把关，全面、系统地介绍各层的主要安全技术和方案设计思路、方法。

本书从深层次分析了网络安全隐患存在的各个主要方面，然后从这几个方面出发，全面介绍企业局域网安全防护系统的设计方法。其中包括网络安全系统设计综述、物理层的网络安全保护方案、数据链路层的安全保护方案、网络层防火墙安全保护方案、网络层 Kerberos 身份认证方案、网络层证书身份认证、加密和签名方案、网络层 PKI 综合应用方案设计、网络层 IPSec 身份认证和加密方案、传输层 TLS/SSL 身份认证和加密方案、应用层 Web 服务器的综合安全系统设计与配置、WLAN 网络综合安全系统设计与配置，并通过实际可用的安全防护方法来实现网络安全隐患的排除或防护。这些不同方面的安全防护措施形成了一个系统的整体，使得企业网络从各个方面都得到足够的安全保证。以上这些都是网络工程师所必须掌握的基础知识和技能。

本书适合网络工程师参考学习，也可作为高等院校及相关培训机构的教材。

图书在版编目（CIP）数据

网络工程师必读. 网络安全系统设计 / 王达编著.—北京：电子工业出版社，2009.8
ISBN 978-7-121-08336-5

I. 网… II. 王… III. 计算机网络－安全技术－系统设计 IV. TP393

中国版本图书馆 CIP 数据核字（2009）第 052921 号

责任编辑：杨　鸽
印　　刷：北京天宇星印刷厂
装　　订：三河市皇庄路通装订厂
出版发行：电子工业出版社
　　北京海淀区万寿路 173 信箱　邮编：100036
开　　本：787×1092　1/16　印张：48　　字数：1382.4 千字
印　　次：2009 年 8 月第 1 次印刷
印　　数：3 500 册　　定价：89.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

FOREWORD

前　言

朋友，你是否正有打算朝着网络安全工程方面发展，成为一名当前国内外最热门又最紧缺、最有发展前景的 IT 职业人士——网络安全工程师呢？你是否正为没有系统的网络安全系统设计方面的权威指南而发愁呢？本书或许是您很好的选择。

本书是目前国内 IT 图书市场中第一本真正从设计角度系统地介绍网络安全系统设计和综合方案的图书。本书最大的特点就是深入、系统地介绍了许多目前主流应用的网络安全技术体系架构和功能实现原理，如 Kerberos、证书和证书服务、IPSec、TLS/SSL 等。可能有许多读者对深奥的理论不感兴趣，在笔者所接触的网友中，的确有许多网友是这样的，只喜欢实操型的书籍。如果作为网络管理员，这可以理解，但是如果作为网络工程师，有这样的心态就非常不正确了。因为网络管理员的工作基本上都是操作型的，而网络工程师的工作则主要是进行各类系统的设计，是底层的。没有全面、深入、扎实的理论基础，不可能对相应技术有一个本质上的理解和运用，更谈不上利用这些技术来设计解决方案了。这就是网络管理员和网络工程师的一个本质区别。

本书主要内容

《网络工程师必读——网络安全系统设计》与笔者在本系列中写的另一部图书——《网络工程师必读——网络系统设计》一样，题目非常大（指其内涵），所涉及的技术、产品和方案非常广。就像我们在写一篇作文一样，题目越大，文章越难写。因为要写，或者可写的内容实在太多、太广，从主题选取，到各主题内容的选取都不是一件简单的事。毕竟就目前来说，网络安全已自成一个庞大的系统，所涉及的技术、产品和方案渗透到了网络领域的各个角落，而无论如何，一本书的篇幅都是非常有限的。所以，在笔者正式写这部书之前，仅写什么和怎么写这两个方面就考虑了非常长的时间。而且在编写这部书之前，总希望能借鉴一些已有的网络安全系统设计类图书的主题选取和写作方法，总希望用有限的篇幅尽可能系统地介绍一些主流的网络安全技术和方案设计思路。但非常遗憾，笔者在网络上查看了近 20 部网络安全类图书的目录，竟然没有一部是希望看到的。所以，笔者最终还是只能靠自己，从头设计本书的主体架构，包括整部图书的章节安排（也可以算是整部图书的体系架构）、各章的主题，以及各章内部的主要内容。综合起来是这样一个基本的写作思路：整部图书的主线是 OSI/RM 的 7 层结构，各章主要针对各主要层次的主要安全技术和方案进行展开，并在本书最后介绍了几个综合的网络安全系统设计和配置方案。

本书共 11 章，具体内容安排如下。

第 1 章 网络安全系统设计综述

本章主要对目前主要的网络隐患、所涉及的主要网络安全技术，以及网络安全系统的设计基本思路进行综合介绍。

第 2 章 物理层的网络安全保护方案

本章主要对基于 OSI/RM 物理层的主要网络安全保护技术和方案进行具体介绍。其中所涉及到的网络安全技术包括计算机网络通信物理介质、线路和设备的屏蔽、网络通信线路的物理隔离、网络通信线路的冗余、数据备份和容灾，以及典型网络物理层的安全保护工具的介绍等。

第 3 章 数据链路层的安全保护方案

本章主要介绍了各种主要的数据链路层可用的加密技术，以及 WLAN 网络中所用的各种数据链路加密、身份验证技术原理和配置方法，如 WEP、WPA、WPA2、IEEE 802.1x 和 IEEE 802.11i 等。还介绍了主流品牌网络设备 MAC 地址绑定和嗅探防护等。至于 VLAN 方面的详细配置在本系列的《网络工程师必读——网络设备配置与管理》（交换机分册）一书中介绍。

第 4 章 网络层防火墙安全保护方案

本章专门根据防火墙设备的主要应用，介绍了内、外围网络中防火墙安全保护系统的设计思路和方法。

第 5 章 网络层 Kerberos 身份认证方案

本章全面、深入地介绍了在 Windows 系统中默认采用的 Kerberos 身份认证技术体系架构、深层身份验证原理、主要应用及基本配置方法。这是目前国内图书市场和网站上极难得到的第一手专业文献。

第 6 章 网络层证书身份认证、加密和签名方案

本章主要以 Windows Server 2003 系统为例全面、深入地介绍了证书和证书服务技术体系架构、深层身份认证、数据加密和电子签名原理，以及证书服务系统的基本设计方法。这也是目前国内图书市场和网站上极难得到的第一手专业文献。

第 7 章 网络层 PKI 综合应用方案设计

本章介绍了各种规模的企业中 PKI 公钥基础结构中的 CA 层次结构设计、证书颁发和吊销、证书配置文件、规划密钥和数据恢复方案配置等几个重要方面内容。

第 8 章 网络层 IPSec 身份认证和加密方案

本章全面、深入地介绍了 IPSec 安全技术体系架构，AH 和 ESP 协议深层加密和身份认证原理，以及 IPSec 方案的设计思路、原则和基本应用配置方法。这也是目前国内图书市场和网站上极难得到的第一手专业文献。

在网络层的像 ACL、NAT、VPN 等其他一些安全保护方案，因为在本系列的丛书《网络工程师必读——网络设备配置与管理》（交换机分册）和《网络工程师必读——虚拟专用网》两书中已有详细介绍，所以不再在本书中介绍。

第 9 章 传输层 TLS/SSL 身份认证和加密方案

本章全面、深入地介绍了 TLS、SSL 技术体系架构、深层加密、数据完整性检查、身份

认证和数字签名原理，以及主流 TLS/SSL 应用方案的配置方法。

第 10 章 应用层 Web 服务器的综合安全系统设计与配置

本章以 IIS Web 服务器为主体，全面、细致地介绍了 Web 服务器网络安全系统设计的基本思路、检查表项和配置方法，着重介绍了各个方面的具体配置方法，可操作性和实用性极强。

第 11 章 WLAN 网络综合安全系统设计与配置

本章全面、细致地介绍了网络安全相对脆弱的 WLAN 无线网络的安全系统设计方法。其中不仅综合用到了本书第 3 章中介绍的各种基于当前主流 WLAN 安全技术（如 WEP、WPA、WPA2、802.1x），还用到了有线网络中所用的一些主流网络安全技术和方案（如 IPSec、RADIUS、PKI 等）。本章还着重介绍了综合的 WLAN 网络安全方案设计思路和方法，并介绍了典型的配置示例，可操作性和实用性极强。

本书主要特色

正如有以上整体规划，所以才使本书具有非常鲜明的特色，具体体现在以下几个方面。

- 真正的“设计”视角

在目前的图书市场中，尽管也有的书以“网络安全系统设计”命名，但极少是真正从设计角度进行章节和内容编排的，基本上都是在谈各方面的软件漏洞修补、黑客攻击原理、工具使用、加密算法等。笔者认为，这些对于完善的网络安全系统设计来说并不是最重要的，因为软件漏洞时刻在变化，而且每天都有一些软件退出历史舞台，也有大批新的软件发布上市，与之相对应的各种黑客攻击方法和工具也会不断变化。而每款软件都有它自身的 Bug，也就必然存在一些安全漏洞，尽管我们自己可以通过一些补丁程序来修补漏洞，但更多的还是要依赖开发相应软件的公司。如果我们的安全系统主要考虑这个方面，就太被动了，也本末倒置了，必然造成我们的安全系统需要不断地修改，紧跟这些软件漏洞进行修复。事实上，软件系统本身的漏洞完全可以通过我们网络安全系统中的一个极小部分（也就是及时更新软件补丁，有分离式的，也有集中式的，如部署 WUS 服务器）来全面解决，网络通信中要解决的真正的安全问题不是这些终端的安全问题，而是通信过程中的安全问题。

本书从网络安全系统设计全局出发，以 OSI/RM 的 7 层结构为主线，层层把关，较全面、系统地介绍各层的主要安全技术和方案设计思路、方法。

- 专业、深入

本书介绍了许多大型的网络安全技术和方案，主要包括物理层的各种介质，线路屏蔽技术和方案，数据链路层加密技术和方案，WLAN 无线网络安全系统方案，防火墙系统方案，Kerberos 身份验证技术和方案，证书的加密、签名、身份验证技术和方案，IPSec 加密、身份验证技术和方案，PKI 公钥基础结构系统设计，ACL、NAT、VPN 等技术，TLS/SSL 加密、身份验证技术和方案，WLAN 综合安全系统设计，Web 服务器安全系统设计等。

而且在介绍技术原理时，不再像同类书那样仅停留在表面上，而是深入挖掘了各技术的体系结构及各子技术的工作原理，使读者对相应技术有一个全面、深入的了解。其中像 Kerberos、证书和证书服务、TLS/SSL 等都是取材自 IETF、Netscape 和 Microsoft 英文官网上的第一手专业资料，在此非常感谢这些国外的公司为我们提供如此专业的技术参考文献。笔

者同时对内容进行了展开和具体化，使枯燥的原理也具有了灵气。

- 实用性和可读性强

即使在介绍技术时，本书也是结合实际的应用进行介绍的，所以读者在全面了解本书所介绍的技术后，就可以掌握相应技术的主要应用，应用于自己的设计方案中。另外，本书也从真正设计视角介绍了一些典型网络安全系统的设计方法，如 WLAN 无线网络的安全系统设计、PKI 公钥基础结构系统设计、Web 服务器安全系统设计等。所以，本书的实用性和可读性比较强，希望能使读者做到学以致用。

本书提供的服务

本书由王达主笔并统稿，参加编写、校验和排版的人员有：何艳辉、王珂、沈芝兰、马平、何江林、刘凤竹、卢京华、周志雄、洪武、高平复、周建辉、孔平、尚宝宏、姚学军、刘学、李翔、王娇、李敏、吴鹏飞等，在此一并表示由衷的感谢。由于编者水平有限，加之时间紧张，尽管我们花了大量时间和精力校验，但书中可能还存在一些错误，敬请各位读者批评指正，万分感谢！另提供了 7 个读者 QQ 群：73417650、17201450、21566766、32354930、5208368、13836245、4789821，2 个网上培训专用 QQ 群：17838740、57828783，以及 VIP 读者群：54435786。最新资讯请看我的博客：http://winda.blog.51cto.com/。

编　著　者

联系方式

咨询电话：（010）88254160　88254161-67

电子邮件：support@fecit.com.cn

服务网址：http://www.fecit.com.cn　　http://www.fecit.net

通用网址：计算机图书、飞思、飞思教育、飞思科技、FECIT

CONTENTS

目　录