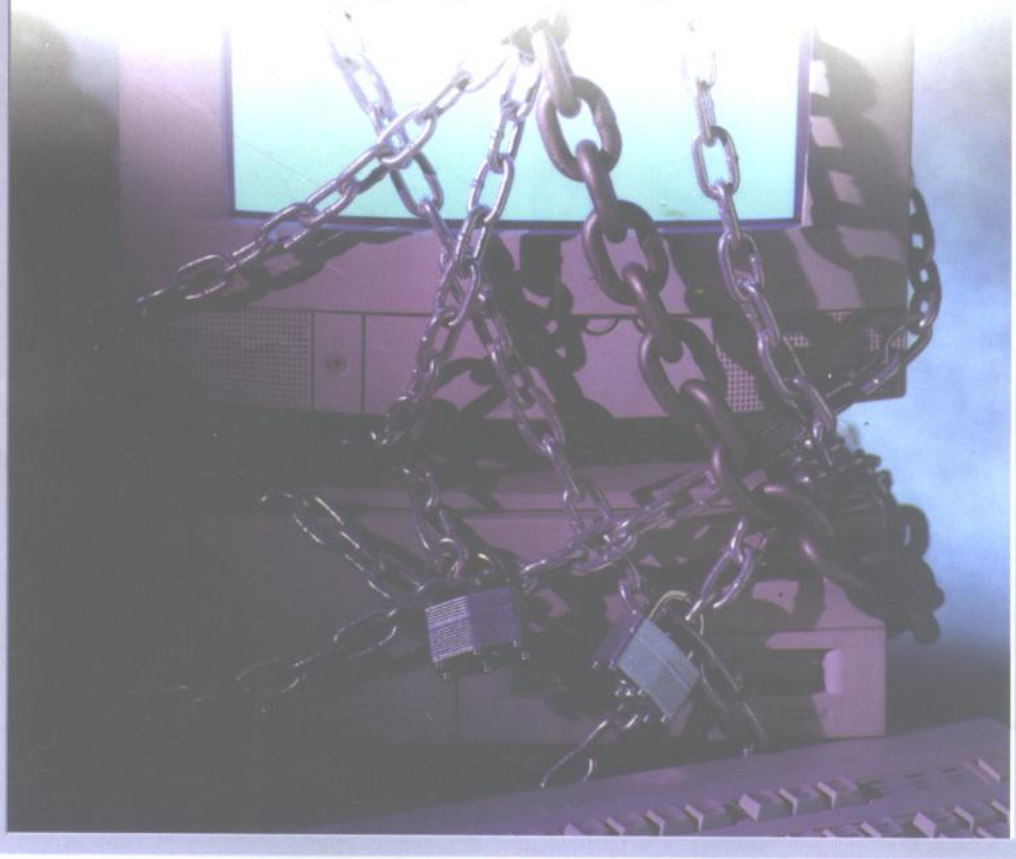
Cisco Systems
Cisco Press

中国计算机学会计算机安全专业委员会推荐参考书

信息与网络安全丛书

网络安全性设计



[美] Merike Kaeo 著

潇湘工作室 译

赵战生 审校

人民邮电出版社
www.pptph.com.cn

中国计算机学会计算机安全专业委员会推荐参考书
信息与网络安全丛书

网络安全性设计

[美] Merike Kaeo 著

潇湘工作室 译

赵战生 审校

人 民 邮 电 出 版 社

中国计算机学会计算机安全专业委员会推荐参考书
信息与网络安全丛书
网络安全性设计

◆ 著　　[美] Merike Kaeo
译　　潇湘工作室
审　　校　赵战生
责任编辑　李　际

◆ 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@ pptph.com.cn
网址　http://www.pptph.com.cn
北京汉魂图文设计有限公司制作
北京鸿佳印刷厂印刷
新华书店总店北京发行所经销

◆ 开本:787×1092　1/16
印张:21
字数:509千字　　2000年10月第1版
印数:1－6 000册　　2000年10月北京第1次印刷

著作权合同登记　图字:01－2000－0671号
ISBN 7-115-08813-6/TP·1847

定价:37.00元

内容提要

本书是一本实用的网络安全性设计指南，可以帮助读者掌握有关保护公司网络基础设施的各种知识和方法。本书共分为四部分，系统而全面地介绍了有关网络安全的理论基础知识和技术发展状况，通过对影响网络安全方面的各种因素的分析，提出了创建企业网络安全的策略、有关的方法和实施手段。书中还通过对许多具体实例的讲解，指导读者在网络基础设施、Internet 访问以及拨号环境中采取各种保护措施。本书的最后提供了美国关于保护企业网络及信息安全的管理参考资料及法律依据，以供读者参考。

本书适合网络管理员以及关注网络安全的技术人员和各级主管人员阅读。

信息与网络安全丛书 审定委员会

名誉主任：朱恩涛
主　　任：谢模乾
副 主 任：杜肤生
　　顾建国
　　徐修存
委　　员：（以下以姓氏笔划为序）
　　王亚明　冯登国　刘凤昌　吕晓春　杨智慧　屈延文
　　赵世强　赵战生　卿斯汉　高新宇　崔书昆　缪道期

丛书前言

随着科学技术的飞速发展，人们已经生活在信息时代。计算机技术和网络技术深入到社会的各个领域，因特网把“地球村”的居民紧密地连在了一起。如果说“天涯若比邻”在过去只是描写人们心灵上的贴近，那么今天计算机网络已使这句话变成了生活现实。近年来因特网的迅速发展，给人们的日常生活带来了全新的感受，人类社会各种活动对信息网络的依赖程度已经越来越大。

然而，凡事“有一利必有一弊”。人们在得益于信息革命所带来的新的巨大机遇的同时，也不得不面对信息安全问题的严峻考验。1999 年好莱坞推出的以网络为主题的影片《黑客帝国》风靡全球，给人们提示了这个问题的严重性。在人们对网络技术的普及叫好声尚未消失的时候，黑客攻击战在现实生活中也愈演愈烈。国内外众多的网站相继被“黑”，病毒制造者们各显其能。从 CIH 噩梦难醒，到“爱虫”病毒狂吻全球，全球“中毒”者不计其数。这些给各行各业带来了巨大的经济和其他方面损失。除此之外，“电子战”、“信息战”已成为国与国之间、商家与商家之间的一种重要的攻击与防卫手段。因此，信息安全、网络安全的问题已经引起各国、各部门、各行、各业以及每个计算机用户的充分重视。

为了提高我国各级计算机信息网络主管部门的安全意识，普及计算机安全知识，进一步提高国内计算机安全的技术水平，帮助国内技术人员汲取国外计算机安全先进技术和经验，有效保护我国信息网络安全；在公安部公共信息网络安全监察局的大力支持下，我们策划且及时推出了这套《信息与网络安全丛书》。这套丛书采用开放式选题架构，全部是从国外著名出版公司出版的有关信息与网络安全类的权威著作和畅销书中精选而成。这套丛书内容涉及计算机硬件安全、操作系统安全、工作站和服务器的系统安全、网络安全设计、网络入侵检测、网络安全理论等各方面的内容。

由于本套丛书的原版书均是由国外权威人士编写而成，因此在观念上和技术上站在了该领域的前沿。也正因为此，本套丛书受到了有关部门领导和专家的高度重视。由公安部领导和公共信息网络安全监察局及部分计算机安全专家组成的审定委员会对图书进行了审阅，从而保证了丛书的权威性和准确性。当然，由于原版图书所涉及的网络及社会环境等与我国情况不尽相同，读者定会本着批评借鉴的态度结合工作实际进行阅读、参考和分析。

我们真诚希望本套丛书能够为信息与网络安全管理和技术人员提供帮助，为我国的信息安全建设做出贡献。

编者

2000 年 7 月

版权声明

前 言

新型的商务活动促使企业网络在各个方面都发生了巨大的变化。随着各个公司逐步理解和着手控制与快速发展的商务应用相关的风险，以及在实际部署公司网络基础设施方面的风险，“企业网络安全性”一词已经变得越来越流行了。网络安全性这个主题相当复杂，它是包罗万象的安全策略的一个发展环节。在当今世界上，随着安全策略的不断发展，我们需要不断更新与安全问题有关的安全技术。从最近的情况来看，虽然基础安全技术还相当复杂，但在公司网络中实现安全措施已经更为轻松了。

目前有许多很不错的书介绍有关计算机安全性方面的内容，其范围从适用于非专业人员理解某个领域的最简单的介绍性读物，到针对安全性产品的实现者掌握错综复杂的技术细节的高级参考书。在对负责设计和运作公司网络基础设施的人们讲授网络安全性的基础知识时，我发现，要介绍的内容实在是太多了，这些信息分散在许多不同的书中，对于非专业人员来说，把它们摘取出来相当困难。这些书通常都集中介绍有关主机的安全问题，或者是专门说明连接到 Internet 时的安全问题。没有哪一本书专门介绍有关加密的基础知识，完整地概括当前正在使用的和最新开发的安全性技术，并给出如何使用这些技术及利用公司的安全策略来提供安全的网络基础设施。对于初步接触安全性的人员，本书提供了有关加密技术和安全性技术的详尽的基础知识。读者将能够很好地理解这些技术和问题，确定创建公司安全性策略的基本需求，并使用策略作为指南，来实现安全的公司网络基础设施。如果读者要了解更为详细和深入的内容（例如防火墙），可以参考其他参考书，附录 A 中提供了有关的参考书目。

本书的重点在于保护公司的网络基础设施。在理想的安全连网环境中，安全性是基于主机的，而且，所有安全性服务都在信息的发起方与接收方之间实现。但是，在实际应用中，许多公司都没有对桌面系统进行完整的控制。公司的安全策略必须通过所有部门加以实施，而且不同的部门有不同的控制级别。

在许多公司中，都有一些部门来处理下面的任务：

- 网络基础设施。
- 桌面需求。
- 安全性需求。

网络基础设施部门设计并实施公司的整体网络设计；桌面需求部门确定所有桌面计算机（PC 和工作站）及其支持的应用的规范；安全性需求部门评估安全性风险，并制订公司其他所有部门实施的适当的安全策略。所有部门都需要寻求在其控制领域内实现的安全性量度方法。本书重点介绍可用来保护网络基础设施和传送数据的安全服务。

我认为，没有任何事情是绝对安全的。就像在电影《The Avengers》中所说，“没有任何事情是不可能的，只有数学上不可能的事情”。在一个网络被人们称为安全网络时，通常人们会误以为它是不可能被侵入的，或者是没有安全缺陷。实际上，安全网络意味着其中的机制可以减轻许多公司资产方面的风险。网络中总会有一些薄弱环节，但是，只要能够认识到而且了解了这些薄弱环节，就可以适当地进行处理。

本书介绍了许多相当好的方法，并在其中一章中介绍了有关安全性的错误看法。Richard P. Feynman 先生是诺贝尔物理学奖的获得者，在本书中，Feynman 先生叙述了他发现攻击安全性和文件柜（里面是有关原子弹的秘密）有多么容易。在多数情况下，他都能够成功，因为人们没有将文件柜锁上、没有更改默认的密码组合、在明显的位置写下密码组合或者是在多个安全位置的密码组合均相同。他指出了闯入系统的简单方法，没有人考虑这些，因为人们总是将精力集中在指出问题上。在创建有效的公司安全性策略时，必须考虑到所有威胁和薄弱环节。

一、本书的目标

本书的目的是帮助读者更好地理解保护网络基础设施的基础知识。不管是已经具有安全性的基础知识，还是刚刚接触这个主题，本书都可以提供设计与实现公司安全基础设施的详细信息。在学习完本书之后，读者将能够完整地理解基本的加密技术、应用最广泛的安全性技术以及新涌现的安全性技术。对于任何公司环境来说，读者都将能够理解风险管理所需要的具体过程及细节，以指导实施安全策略的体系结构并付诸实践，而且，为了实现给定的网络策略，你将能够指定网络基础设施中所需要的特征。

二、本书的读者

本书适用于负责为企业网络基础设施设计和维护安全性服务的互连网络专业人员。对于具有安全性协议和技术的基础知识的网络工程师、设计或技术人员，在考虑设计和实现各种程度的安全性策略时，本书均可提供实用的指导。

本书还适用于为客户设计公司网络的顾问、系统工程师和销售工程师。本书面向的读者范围相当广泛，这是因为在任何网络设计过程中，都要考虑安全性服务。

三、本书的组织

本书分为四部分。第一部分介绍技术和法律方面的问题；第二部分重点介绍公司环境，例如如何确定可能的薄弱环节，以及创建适当的安全策略；第三部分演示了对 Cisco 设备进行配置的实际操作；第四部分列出了有关网络安全性的更多的参考信息。

第一部分，“安全基础”。

第一部分专门解释加密术的基础、广泛应用的安全性技术以及不断发展的法律因素。第 1 章重点介绍加密术基础，解释不同的加密术的功能差异以及它们的实际应用方式。本章的目的是提供详细的信息，以使读者理解稳固环节和薄弱环节之间的相对性，并理解人们大肆宣传的安全技术。我们尽量避免说明许多数学上的复杂性，因为这些内容适合于安全性产品的实现者。如果对此感兴趣，读者可以从附录 A 中列出的参考书中查找加密术专家所写的详细信息。

第 2 章详细介绍不断涌现而且广泛应用的安全性技术。本章介绍的范围比较广泛，而且是最难以表述的，因为这一章的内容本身就可以单独写一本书。本章以合理的方式进行组织，可以帮助你在决定何时实现给定的安全策略时作出决策，以选择最合适的技术。我在本章介绍的许多技术是相互重叠的，因为它们对类似的问题提供了类似的解决方案。在这些方案中，许多都是用以实现更安全的解决方案的手段，而那些解决方案在过去是相当难以实现的。

第 3 章详细说明在全球环境中部署安全性时应当考虑的法律问题。

第二部分，“企业安全策略”。

在确定安全策略时，理解薄弱环节和风险是最为重要的。本书的第二部分重点介绍如何制订安全策略，即在设计适用于特定环境的策略时实际应当考虑的因素。第 4 章介绍对网络基础设施可能的威胁和常见的攻击方式。第 5 章详述安全性策略的考虑因素，并描述如何进行风险管理分析。第 6 章说明在完成风险分析后如何设计安全性策略，这里提供了一些公司应当遵循的指南和过程。第 7 章专门介绍如何在安全性被破坏的情况下进行恢复。

第三部分，“具体实现”。

本书第三部分专门解释具体的实现。这里给出了 Cisco 设备的具体配置示例。根据所建立的安全性策略的不同，这些实现将有很大的变化，但在考虑实现给定公司的安全性策略时，可以参考这些信息。第 8 章重点介绍了内部公司基础设施的安全性需求，以保证对网络基础设施设备和网络区域的访问是受限的、机密的。第 9 章集中介绍保护 Internet 访问以及任何确定的网络边界。第 10 章说明保护拨入环境方面的内容。

第四部分，“附录”。

附录 A 列出了更多的信息来源，其中包括专门介绍加密术和防火墙的书籍，指出了一些 IETF 工作组的 Web 站点，其中给出了有关当前安全性技术的详细信息。此外还给出了一些创建网络安全策略和事故反应团队的信息。

附录 B 给出了报告和预防工业间谍和网络侵入的应急计划指南。本附录是由 C.Smith 编写的，可以帮助有关组织确立防止网络偷窃和网络侵入的规划，并知道在发生网络入侵时应当如何保护资产并阻止进一步的侵害。

附录 C 列出了由 IANA（Internet Assigned Numbers Authority）分配的与第 2 章讨论的安全技术有关的端口号。

目 录