ICSA 国家信息中心 启明星辰公司 策划

Internet / Intranet

网络安全结构设计

启明星辰公司
许锦波 严望佳 编著

计算机网络安全系列丛书

清华大学出版社
http://www.tup.tsinghua.edu.cn

计算机网络安全系列丛书

Internet/Intranet
网络安全结构设计

启明星辰公司
许锦波　严望佳　编著

清华大学出版社

(京)新登字 158 号

内 容 简 介

本书主要讲述 Internet/Intranet 的安全结构，首先从构成 Internet/Intranet 的基本部件的安全性着手，分别叙述了它们各自的安全问题和安全措施，然后从总体上介绍一个综合运用各部件的实际安全网络方案，该方案有机地糅合了各个安全部件，从而使大家进一步认清各个安全部件的相互关系。本书内容覆盖了 TCP/IP 协议、域名系统、防火墙技术、电子邮件系统、WWW 系统、网络管理系统、数据库管理系统和办公自动化系统等各部分的安全。本书行文流畅、示例丰富、讲解清晰、介绍全面，必能让读者受益匪浅。

图书在版编目（CIP）数据

Internet/Intranet 网络安全结构设计/ICSA 启明星辰公司著. —北京：清华大学出版社，1998
(计算机网络安全系列丛书)
ISBN 7-302-03293-9

I .I… II .①I… ②国… III 计算机网络-安全技术-结构设计，IV .TP393

中国版本图书馆 CIP 数据核字（98）第 37543 号

出版者： 清华大学出版社（北京清华大学校内，邮编 100084）
http://www.tup.tsinghua.edu.cn
印刷者： 北京市清华园胶印厂
发行者： 新华书店总店北京发行所
开　本： 787×1092 1/16　**印张：** 32.25　**字数：** 573 千字
版　次： 1999 年 2 月第 1 版　1999 年 2 月第 1 次印刷
书　号： ISBN 7-302-03293-9/TP・1766
印　数： 0001～5000
定　价： 53.00 元

谨以此书献给我们的老师

严望佳

丛 书 序

全球信息高速公路的建设，Internet/Intranet 的发展，将对整个社会的科学与技术、经济与文化带来巨大的推动与冲击，同时也给我们带来了许多的挑战。Internet/Intranet 信息安全是一个综合的系统工程，需要我们在网络安全技术的研究和应用领域做长期的攻关和规划。

在 Internet/Intranet 的大量应用中，Internet/Intranet 安全面临着重大挑战。事实上，资源共享和信息安全历来是一对矛盾。近年来随着 Internet 的飞速发展，计算机网络的资源共享进一步加强，随之而来的信息安全问题日益突出。据美国 FBI 统计，美国每年因网络安全问题所造成的经济损失高达 75 亿美元。而全球平均每 20 秒钟就发生一起 Internet 计算机侵入事件。

一般认为，计算机网络系统的安全威胁主要来自黑客攻击、计算机病毒和拒绝服务攻击 3 个方面。目前，人们也开始重视来自网络内部的安全威胁。

黑客攻击早在主机终端时代就已经出现，随着 Internet 的发展，现代黑客则从以系统为主的攻击转变到以网络为主的攻击。新的手法包括：通过网络监听获取网上用户的帐号和密码；监听密钥分配过程，攻击密钥管理服务器，得到密钥或认证码，从而取得合法资格；利用 UNIX 操作系统提供的守护进程的缺省帐户进行攻击，如 Telnet Daemon、FTP Daemon 和 RPC Daemon 等；利用 Finger 等命令收集信息，提高自己的攻击能力；利用 SendMail，采用 debug、wizard 和 pipe 等进行攻击；利用 FTP，采用匿名用户访问进行攻击；利用 NFS 进行攻击；通过隐蔽通道进行非法活动；突破防火墙等等。目前，已知的黑客攻击手段多达 500 余种。

计算机病毒与“蠕虫”程序有所不同，它们主要的区别是，“蠕虫”寄生于操作系统之上，而计算机病毒寄生于一般的可执行程序上。计算机病毒种类繁多，极易传播，影响范围广。它动辄删除、修改文件，导致程序运行错误，甚至死机，已构成对 Internet/Intranet 的严重威胁。

拒绝服务攻击是一种破坏性攻击，最早的拒绝服务攻击是“电子邮件炸弹”。它的表现形式是用户在很短的时间内收到大量无用的电子邮件，从而影响正常业务的运行。严重时会使系统关机、网络瘫痪。

总而言之，对 Internet/Intranet 安全构成的威胁可以分为以下若干类型：黑客入侵、来自内部的攻击、计算机病毒的侵入、秘密信息的泄漏和修改网络的关键数据等，这些都可以造成 Internet 瘫痪或引起 Internet 商业的经济损失等等。人们面临的计算机网络系统的安全威胁日益严重。

黑客攻击等威胁行为为什么能够经常得逞呢？主要原因在于 Internet/Intranet 系统内在安全的脆弱性；其次是人们思想麻痹，没有正视黑客入侵所造成的严重后果，因而舍不得投入必要的人力、财力和物力来加强 Internet/Intranet 的安全性，没有采取有效的安全策略和安全机制。另外，缺乏先进的网络安全技术、工具、手段和产品等原因，也导致网络的安全防范能力差。

由于我国网络研究起步晚，网络安全技术还有待整体的提高和发展。我很高兴看到这套丛书的诞生，该丛书系统全面地介绍了计算机网络安全各方面的问题，并且从一些新的角度进行探讨，例如，如何针对 Internet/Intranet 系统的安全威胁建立正确的安全策略；如何提出 Internet/Intranet 系统安全的整体解决方案；如何严格规范建立 Internet/Intranet 系统的安全机制等。这对提高我国网络安全防范能力将有重要的参考作用。

这套由国家信息中心、国际计算机安全协会(ICSA)以及启明星辰信息技术有限公司(Vtech)策划的网络安全系列丛书具有起点高、技术覆盖面广等特点。包括了对业界最新的网络安全技术、操作系统漏洞和防范方法、网络安全工具以及黑客攻击手段等的详细分析和介绍。读者可以带着各种问题、从不同的角度来了解这些技术，一定会有所收获。

中国工程院院士　沈昌祥

前　言

从国家提出建设“三金工程”以来，因特网（Internet）开始在我国逐渐得到重视。许多部委、事业单位、科研单位等机构开始建立 Internet 的接入网，并在信息科学的推动下开始重组机构内部的信息结构。

但是，当人们真正使用 Internet 的时候，一方面被 Internet 的技术和能跨越空间索取信息所折服，另一方面则对 Internet 网络安全技术感到失望。Intranet 泛指机构内部网，在这里，机构可以是工商企业、事业单位、行业部门和区域部门等。Intranet 其实是指在有限的范围内，利用 Internet 的一系列成熟标准所构筑的机构内部的网络系统。它和数据库技术、多媒体技术以及开放式的群件系统相互融合连接，形成一个能有效地解决信息系统内部信息的采集、共享、发布和交流的，易于维护管理的信息运作平台。与 Internet 相比，Intranet 的安全性则显得更为重要，Intranet 的解决方案应当具有严格的网络资源管理机制、网络安全保障机制，同时还应当具有良好的开放性。

本书主要讲述 Internet/Intranet 的安全结构。首先从构成 Internet/Intranet 的基本部件的安全性着手，分别叙述它们各自的安全问题和安全措施，然后从总体上介绍一个综合运用各部件的实际安全网络方案，该方案有机地结合了各个安全部件，从而使人们进一步认清各个安全部件间的相互关系。

本书内容主要分为十二个部分：

第一部分：Internet/Intranet 安全基础（第一章至第七章）

第二部分：域名系统的安全（第八章）

第三部分：防火墙技术（第九章至第十五章）

第四部分：电子邮件系统的安全（第十六章至第十九章）

第五部分：WWW 系统的安全（第二十章）

第六部分：网络管理系统（第二十一和第二十二章）

第七部分：数据库管理系统的安全（第二十三章至第二十五章）

第八部分：高可用技术（第二十六章）

第九部分：办公自动化系统的安全（第二十七章至第三十章）

第十部分：报表系统（第三十一章）

第十一部分：综合应用实例（第三十二章）

第十二部分：附录

除了最后一个部分外，其余各部分内容基本上是独立的，阅读每一部分都不需要其他部分的知识。

这套丛书的策划和出版得到以下朋友的热情支持和帮助，谨在这里表示我们诚挚的谢意：中国信息安全专业委员会李正男主任、刘世键主任、吴亚飞秘书长，中国信息大学执行董事刘建国先生，国家信息大学信息安全处叶红、董小玲、张翔和孙卫红，美国格莱瑞技术公司严立。

目　录