高等职业院校国家技能型紧缺人才培养培训工程规划教材·计算机应用与软件技术专业

计算机信息安全技术应用

陈志雨　主　编

刘　钢
许建潮　副主编

傅连仲　主　审

電子工業出版社

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书内容包括计算机信息安全的成熟技术、网络边缘设备安全技术、局域网安全配置、计算机病毒防治、认证技术和攻防技术实践等。本书通过大量的实例和实训，加强对基本原理的理解，提高实际技术应用能力。

本书内容注重实用，叙述清晰，可作为承担国家技能型紧缺人才培养培训工程的高等职业院校和示范性软件职业技术学院、高等专科学校及本科院校举办的二级职业技术学院的计算机应用与软件技术专业教材，也适合学习计算机信息安全技术和应用的技术人员及从事网络安全的管理人员使用。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目(CIP)数据

计算机信息安全技术应用／陈志雨主编．—北京：电子工业出版社，2005.1
高等职业院校国家技能型紧缺人才培养培训工程规划教材·计算机应用与软件技术专业
ISBN 7-121-00404-6

Ⅰ．计…　Ⅱ．陈…　Ⅲ．电子计算机－安全技术－高等学校：技术学校－教材　Ⅳ．TP309

中国版本图书馆 CIP 数据核字（2004）第 099904 号

责任编辑：洪国芬　　特约编辑：王宝祥
印　　刷：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
经　　销：各地新华书店
开　　本：787×1 092　1/16　印张：13.75　字数：352 千字
印　　次：2005 年 1 月第 1 次印刷
印　　数：　册　定价：　元

髂

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（010）68279077。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。

前　言

计算机信息安全问题涉及到国家安全、社会公共安全，世界各国已经认识到信息安全涉及重大国家利益，是互联网经济的制高点，也是推动互联网发展、电子政务和电子商务的关键，发展信息安全技术是目前面临的迫切要求。

目前，我国计算机安全防护能力处于发展的初级阶段，许多计算机基本上处于不设防状态。在安全存储方面，无论是防范意识还是核心技术、安全产品，几乎是一片空白。每年各种重要数据与文件的滥用、泄露、丢失和被盗，给国家、企业和个人造成的损失数以亿计。这还不包括那些还没有暴露出来的深层次的问题！计算机安全问题解决不好，不仅会造成巨大的经济损失，甚至会危及国家的安全和社会的稳定。

本书的写作目的是帮助读者了解计算机信息安全技术原理和应用实践。通过实训学会如何保护计算机信息的内容，防止黑客和计算机病毒的攻击，如何构建一个完善的计算机信息安全保障系统。

全书共 6 章，从理论、技术及实训的各个角度对计算机信息安全技术进行分析和阐述。使读者对计算机信息安全有一个系统、全面的认识。各章内容简述如下：

第 1 章对计算机信息安全成熟技术及解决方案进行了一般性的介绍。

第 2 章介绍网络边缘设备的种类，路由器的工作原理和安全技术，防火墙的体系结构和安全机制，物理隔离器和隔离卡的安全技术等内容。

第 3 章介绍局域网安全技术，物理分段和虚拟局域网的安全机制，入侵检测系统和扫描技术，操作系统的安全配置等内容。

第 4 章主要讲述计算机病毒的原理，如何防治单机病毒和网络病毒，并介绍了几种局域网防病毒的解决方案。

第 5 章讲述了认证技术的工作原理，路由器上的认证技术及如何使用 Windows Server 2003 构造认证服务器。

第 6 章介绍了日志在线分析的实现技术，端口扫描的实现技术，拒绝服务的实现技术，网络监听的实现技术及木马技术等。

本书在写作过程中力求做到原理和概念明确、理论与实践相结合。读者在学习本教材之前，应具备编程语言、计算机网络、操作系统等方面的基本知识。

本书适合作为计算机软件职业技术学院、高等职业技术院校、高等专科学校、成人高校及本科院校举办的二级职业技术学院和民办高校的计算机及相关专业的教材，还可作为对网络安全感兴趣的初学者的自学教材。

本书由陈志雨担任主编，刘钢、许建潮担任副主编，傅连仲担任主审。其他参与编写的人员有孙卫佳、唐培丽、张丽娟、徐立新、韩冬、江虹等。

由于编写时间仓促、编者水平有限以及计算机信息安全技术更新速度较快，书中难免有错误和不尽为人意之处，请读者批评指正。编者的 E-mail 地址为 forehead@mail.ccut.edu.cn，lg@mail.ccut.edu.cn。

编　者

2004 年 7 月

此为试读，需要完整PDF请访问：www.ertongbook.com

出 版 说 明

高等职业教育是我国高等教育体系的重要组成部分，也是我国职业教育体系的重要组成部分。社会需求是职业教育发展的最大动力。根据劳动市场技能人才的紧缺状况和相关行业人员资源需求预测，教育部会同劳动和社会保障部、国防科工委、信息产业部、交通部、卫生部启动了“职业院校制造业和现代服务业技能型紧缺人才培养培训工程”，明确了高等职业教育的根本任务是要从劳动力市场的实际需要出发，坚持以就业为导向，以全面素质为基础，以能力为本位，把提高学生的职业能力放在突出的位置，加强实践教学，努力造就数以千万计的制造业和现代服务业一线迫切需要的高素质技能型人才，并且优先确定了“数控技术应用”、“计算机应用与软件技术”、“汽车运用与维修”、“护理”等四个专业领域，在全国选择确定 200 多所高职院校作为承担技能型紧缺人才培养培训工程示范性院校，其中计算机应用与软件技术专业 79 所，软件示范性高职学院 35 所，数控技术应用专业 90 所，汽车运用与维修专业 63 所。为加快实施技能型人才培养培训工程，教育部决定，在 3～5 年内，高职院校学制要由 3 年逐步改为 2 年。

为了适应高等职业教育发展与改革的新形势，电子工业出版社在国家教育部、信息产业部有关司局的支持、指导和帮助下，进行了调研，探索出版符合高等职业教育教学模式、教学方法、学制改革的新教材的路子，并于 2004 年 4 月 3 日～13 日在南京分别召开了“计算机应用与软件技术”、“数控技术应用”、“汽车运用与维修”等 3 个专业的教材研讨会。参加会议的 150 多名骨干教师来自全国 100 多所高职院校，很多教师是双师型的教师，具有丰富的教学经验和实践经验。会议根据教育部制定的 3 个专业的高职两年制培养建议方案，确定了主干课程和基础课程共 60 个选题，其中，“计算机应用与软件技术专业”30 个；“数控技术应用专业”12 个；汽车运用与维修专业 18 个。

这批教材的编写指导思想是以两年制高等职业教育技能型人才为培养目标，明确职业岗位对专业核心能力和一般专业能力的要求，重点培养学生的技术运用能力和岗位工作能力，并围绕核心能力的培养形成系列课程链路。教材编写注重技能性、实用性，加强实验、实训、实习等实践环节。教材的编写内容和学时数较以往教材有根本的变化，不但对教材内容系统地进行了精选、优化和压缩，而且适当考虑了相应的职业资格证书的课程内容，有利于学生在获得学历证书的同时，顺利获得相应的职业资格证书，增强学生的就业竞争能力。为了突出教学效果，这批教材将配备电子教案，重点教材将配备多媒体课件。

这批教材按照两年制高职教学计划编写。第一学期教学所用的基础教材将于 2004 年 9 月前出版。第二学期及之后的教材大部分将于 2004 年 12 月前出版。这批教材是伴随着高等职业教育的改革与发展而问世的，可满足当前两年制高等职业教育教学的需求，教材所存在的一些不尽如人意之处，将在今后的教学实践中不断修订、完善和充实。我们将在教育部和信息产业部的指导和帮助下，一如既往地依靠业内专家，与科研、教学、产业第一线人员紧密结合，加强合作，与时俱进，不断开拓，为高等职业教育提供优质的教学资源和服务。

电子工业出版社
高等职业教育教材事业部
2004 年 8 月

参与编写“高等职业院校国家技能型紧缺人才培养培训工程规划教材”的院校及单位名单

吉林交通职业技术学院
长春汽车高等专科学校
山西交通职业技术学院
湖南交通职业技术学院
云南交通职业技术学院
南京交通职业技术学院
陕西交通职业技术学院
浙江交通职业技术学院
江西交通职业技术学院
福建交通职业技术学院
南京工业职业技术学院
浙江工贸职业技术学院
四川职业技术学院
郴州职业技术学院
浙江师范大学高等技术学院
辽宁铁岭农业职业技术学院
河北承德石油高等专科学校
邢台职业技术学院
保定职业技术学院
武汉工交职业学院
湖南生物机电职业技术学院
大庆职业学院
三峡大学职业技术学院
无锡职业技术学院
哈尔滨工业大学华德应用技术学院
长治职业技术学院
江西机电职业技术学院
湖北省襄樊机电工程学院
河南漯河职业技术学院
吉林电子信息职业技术学院
陕西国防工业职业技术学院
天津中德职业技术学院
河南机电高等专科学校
平原大学
苏州工业园区职业技术学院
九江职业技术学院
宁波大红鹰职业技术学院
无锡轻工职业技术学院
江苏省宜兴轻工业学院
湖南铁道职业技术学院
顺德职业技术学院
广东机电职业技术学院
常州机电职业技术学院
常州轻工职业技术学院
南京工程学院数控培训中心
上海市教育科学研究院
深圳职业技术学院
深圳信息职业技术学院
湖北轻工职业技术学院
上海师范大学
广东技术师范学院
包头职业技术学院
山东济宁职业技术学院
无锡科技职业学院
钟山学院信息工程系
合肥通用职业技术学院
广东轻工职业技术学院
山东信息职业技术学院
大连东软信息技术学院
西北工业大学金叶信息技术学院
福建信息职业技术学院
福州大学工程技术学院
江苏信息职业技术学院
辽宁信息职业技术学院
华北工学院软件职业技术学院
南海东软信息技术职业学院
天津电子信息职业技术学院
北京信息职业技术学院
安徽新华学院
安徽文达信息技术职业学院

杭州电子工业学院软件职业技术学院
常州信息职业技术学院
武汉软件职业学院
长春工业大学软件职业技术学院
淮安信息职业技术学院
上海电机高等专科学校
安徽电子信息职业技术学院
上海托普信息技术学院
浙江工业大学
内蒙古电子信息职业学院
武汉职业技术学院
南京师范大学计算机系
苏州托普信息技术学院
北京联合大学
安徽滁州职业技术学院
新疆农业职业技术学院
上海交通大学软件学院
天津职业大学
沈阳职业技术学院
南京信息职业技术学院
南京四开电子有限公司
新加坡 MTS 数控公司
上海宇龙软件工程有限公司
北京富益电子技术开发公司
安徽职业技术学院
河北化工医药职业技术学院
河北工业职业技术学院
河北师大职业技术学院
北京轻工职业技术学院
成都电子机械高等专科学校
广州铁路职业技术学院
广东番禺职业技术学院
桂林电子工业学院高职学院
桂林工学院
河南职业技术师范学院
黄冈职业技术学院
黄石高等专科学校
湖北孝感职业技术学院
湖南信息职业技术学院
江西蓝天职业技术学院
江西渝州科技职业技术学院
江西工业职业技术学院
柳州职业技术学院
南京金陵科技学院
西安科技学院
西安电子科技大学
上海新侨职业技术学院
四川工商职业技术学院
绵阳职业技术学院
苏州工商职业技术学院
天津渤海职业技术学院
宁波高等专科学校
太原电力高等专科学校
无锡商业职业技术学院
新乡师范高等专科学校
浙江水利水电专科学校
浙江工商职业技术学院
杭州职业技术学院
浙江财经学院信息学院
台州职业技术学院
湛江海洋大学海滨学院
天津滨海职业技术学院

目　　录

此为试读，需要完整PDF请访问：www.ertongbook.com

第 1 章　计算机信息安全技术概述

计算机信息安全技术是目前热门的研究领域之一。随着网络的飞速发展，人们越来越多地关注信息的安全性。本章将对计算机信息安全技术进行一个概要的描述，探讨计算机信息安全的必要性，简单介绍目前成熟的安全技术，并给出企业信息安全技术的解决方案模板。

理论环节

- 了解计算机信息安全技术
- 掌握计算机信息安全技术的必要性
- 掌握计算机信息安全技术的解决方案

1.1　引言

随着科学技术的飞速发展，我们已经生活在信息时代。20 世纪人类的两大科技成果——计算机技术和网络技术，均已深入到人类社会的各个领域，诸如政治、军事、科研、经济等各种活动对信息网络的依赖程度已经越来越强。

然而科学技术是一把双刃剑，我们在享受着网络技术所带来的便利的同时，也面临着安全性所带来的巨大威胁：黑客的泛滥、越来越多的网络犯罪活动、出于各种目的的系统入侵

此为试读，需要完整PDF请访问：www.ertongbook.com

等等。Internet 的飞速发展对网络安全提出了前所未有的挑战。

那么，什么是信息安全呢？我国在 1997 年 7 月 1 日实施了《计算机信息系统安全专用产品分类原则》，在这一原则中明确地对信息安全做了定义：信息安全是指防止信息财产被故意的或偶然的非授权泄露、更改、破坏或使信息被非法的系统辨识、控制，即确保信息的完整性、保密性、可用性和可控性。

从技术的角度来说，信息安全是一个综合利用数学、物理、通信、计算机和网络等诸多学科的综合、交叉性学科，已经发展为“攻（攻击）、防（防御）、测（检测）、控（控制）、管（管理）、评（评估）”等多方面的基础理论和实施技术。

1.1.1 信息安全技术的必要性

您的计算机是否感染过病毒？您公司的网络是否遭受过入侵或攻击？笔者的计算机在通过 ADSL 连入 Internet 时，平均每 5 天就会有 1～2 次面临着木马攻击（幸好笔者的计算机安有防火墙并针对安全做了配置）。目前，越来越多的网站因为各种安全性问题而瘫痪，公司的机密被窃取，造成巨大的经济损失。这些都不能不说明信息安全技术是一个不容忽视的大问题，对信息安全技术的研究是必要的。

1．操作系统的漏洞

世界上没有绝对安全的操作系统，漏洞是避免不了的，无论是 Windows，还是 UNIX 或 Linux，这是我们不得不面对的一个残酷的现实。只要电脑连入到 Internet，就面临着被攻击的危险。“冲击波”、“震荡波”不就是利用了操作系统的漏洞而对计算机进行攻击的吗？目前的方法是定期地去操作系统网站进行安全更新。

2．应用程序的缺陷

同操作系统一样，应用程序也存在着这样或那样的安全缺陷。程序设计、编码的失误，甚至是“后门”都给应用程序的安全带来了隐患。IE(Internet Explorer),Outlook,OICQ,SQL Server 都成为过黑客攻击的对象或病毒传播的载体。即使是一个非网络应用的软件，也会存在内存溢出等问题。

3．网络协议的问题

网络协议也是不安全的，每个协议都有一定的设计缺陷。不然的话，也就不会有诸如包洪水（Package Flood）、死亡之 Ping（Ping of Death）这样的网络攻击了。


-注释-

有关包洪水、死亡之 Ping 的内容将在第 3 章和第 6 章介绍。

4．非法入侵者的恶意行为

非法入侵者是指在未经访问授权的情况下进入远程计算机网络的人，包括黑客和骇客两种。

黑客（Hacker）是随着网络的发展而出现的。原指热心于计算机技术，水平高超的电脑专家，尤其是程序设计人员。他们通常拥有操作系统、编程语言和网络协议等多方面的丰富

知识，一般没有恶意企图，不会对系统造成破坏。

骇客（Cracker），指那些怀有恶意企图或搞恶作剧的黑客们，通常会对系统造成一定程度的破坏。

这种恶意行为会导致网络的瘫痪或重要信息的泄漏，还可能会把计算机或网络变成它的操控对象，以便实施分布式的拒绝服务攻击。


-注释-

有关分布式拒绝服务攻击的内容将在第 6 章介绍。

5．企业网站的建设问题

大多数企业在进行网站建设的时候没有一个合理的规划，没有充分利用路由器、防火墙、认证服务器的优势。甚至，有的企业没有专职的网络管理员。这样安全性极差的网络自然也就成了黑客们的攻击目标。

1.1.2 信息安全技术现状

目前，人们已经增强了信息安全的意识，从各个不同的方面研究信息安全技术，包括：

- 安全体系结构理论与技术；
- 网络安全与安全产品；
- 密码理论与技术；
- 安全协议理论与技术；
- 信息对抗理论与技术。

尤其是国外，已经有一批成熟的技术、规范或产品。信息安全技术也成为当今最热门的研究领域之一。

我国的信息安全在技术、产品和管理等方面相对落后，所以信息安全问题变得十分重要。为了增强信息安全意识，我国先后出台了《中华人民共和国计算机信息系统安全保护条例》等一系列信息安全方面的法令、法规，主要涉及到信息系统安全保护、国际联网管理、商用密码管理、计算机病毒防治和安全产品检测与销售等几个方面。而且国家正在加大力度积极研究信息安全技术，同时涌现出了一批从事安全产品研究的公司，如江民、瑞星、金山等。

1.2 计算机信息安全成熟技术

计算机信息安全技术是针对信息在应用环境下的安全保护而提出的，是信息安全基础理论的具体应用。它包括两个方面：安全技术和平台安全。

1.2.1 安全技术

安全技术是对信息系统进行安全检查和防护的技术，包括：防火墙技术、漏洞扫描技术、入侵检测技术、防病毒技术等。

1．防火墙技术

防火墙技术是一种安全隔离技术，它通过在两个安全策略不同的域之间设置防火墙来控制两个域之间的互访行为。隔离可以在网络层的多个层次上实现，目前应用较多的是网络层的包过滤技术和应用层的安全代理技术。包过滤技术通过检查信息流的源地址和目的地址等方式确认是否允许数据包通行，而安全代理则通过分析访问协议、代理访问请求来实现访问控制。

2．漏洞扫描技术

漏洞扫描是针对特定信息网络中存在的漏洞而进行的。信息网络中无论是主机还是网络设备都可能存在安全隐患，有些是系统设计时考虑不周而留下的，有些是系统建设时出现的。这些漏洞很容易被攻击，从而危及信息网络的安全。由于安全漏洞大多是非人为的、隐蔽的，因此，必须定期扫描检查、修补加固。操作系统经常出现的补丁模块就是为加固发现的漏洞而开发的。由于漏洞扫描技术很难自动分析系统的设计和实现，因此很难发现未知漏洞。目前的漏洞扫描更多的是对已知漏洞检查定位。

3．入侵检测技术

入侵检测是指通过对网络信息流提取和分析发现非正常访问模式的技术。目前主要有基于用户行为模式、系统行为模式和入侵特征的检测等。在实现时，可以只检测对某主机的访问行为，也可检测针对整个网络的访问行为，前者称为基于主机的入侵检测，后者称为基于网络的入侵检测。

4．防病毒技术

病毒是一种具有传染性和破坏性的计算机程序。自从 1988 年出现 morris 蠕虫以来，计算机病毒成为家喻户晓的计算机安全隐患之一。随着网络的普及，计算机病毒的传播速度大大加快，破坏力也在增强，出现了智能病毒、远程控制病毒等。因此，研究和防范计算机病毒也是信息安全的一个重要方面。

5．智能卡技术

智能卡技术是与数据加密技术紧密相关的。所谓智能卡就是密钥的一种媒体，就像信用卡一样，由授权用户所持有并由该用户赋与它一个口令或密码。该密码与内部网络服务器上注册的密码一致。当口令与身份特征共同使用时，智能卡的保密性能还是相当有效的。

6．认证技术

认证（Authentication）是用户向系统出示自己的身份证明并由认证系统来核实的过程。它是判明和确认通信双方真实身份的重要环节。目前流行的认证系统有：

- 基于公共密钥的身份验证；
- 基于 DCE/Kerberos 的身份验证；
- 基于询问/应答（Challenge/Response）的身份验证。

1.2.2 平台安全

1．物理安全

物理安全是指保障信息网络物理设备不受物理损坏，或者是损坏后能及时修复或替换。通常是针对设备的自然损坏、人为破坏或灾害损坏而提出的。目前常见的物理安全技术有备份技术、安全加固技术和安全设计技术等。如保护 CA 认证中心、采用多层安全门和隔离墙，对核心密码部件还要用防火、防盗柜加以保护。

2．网络安全

网络安全的目标是防止针对网络平台的实现和访问模式的安全威胁。在网络层，大量的安全问题与连接的建立方式、数据封装方式、目的地址和源地址等有关。例如，TCP/IP 协议在建立连接时要求三次握手，这就导致了通过发起大量半连接而使网络阻塞的 SYN-Flood 攻击。网络安全的内容主要有：安全隧道技术、网络协议脆弱性分析技术、安全路由技术和安全 IP 协议等。

3．系统安全

系统安全是各种应用程序的基础。系统安全关心的主要问题是操作系统自身的安全性问题。信息的安全措施是建立在操作系统之上的，如果操作系统自身存在漏洞或隐蔽通道，就有可能使用户的访问绕过安全机制，使安全措施形同虚设。因此系统自身的安全性非常重要。系统安全的主要内容包括安全操作系统模型和实现、操作系统的安全加固、操作系统的脆弱性分析等。

4．数据安全

数据是信息的直接表现形式，数据安全的重要性则不言而喻。数据安全主要关心数据在存储和应用过程中是否会被非授权用户有意破坏，或被授权用户无意破坏。数据通常以数据库或文件形式存储，因此，数据安全主要是数据库或数据文件的安全问题。数据库系统或数据文件系统在管理数据时采取什么样的认证、授权、访问控制及审计等安全机制，达到什么安全等级，机密数据能否被加密存储等，都是数据安全问题。数据安全技术的主要内容有：安全数据库系统、数据存取安全策略和实现方式等。

5．用户安全

用户安全问题有两层含义：一方面，合法用户的权限是否被正确授权，是否有越权访问，是否只有授权用户才能使用系统资源。例如，一个普通的合法用户可能被授予了管理员的身份和权限。另一方面，被授权的用户是否获得了必要的访问权限，是否存在多业务系统的授权矛盾等。用户安全技术的主要内容有：用户账户管理、用户登录模式、用户权限管理等。

6．边界安全

边界安全关心的是不同安全策略的区域边界连接的安全问题。不同的安全域具有不同的安全策略，将它们互连时应该如何设置以保证原有安全策略的有效性，应该采取什么样的隔

离和控制措施来限制互访，各种安全机制和措施互连后满足什么样的安全关系，这些问题都需要解决。边界安全技术的主要内容是安全边界防护协议和模型、不同安全策略的连接关系问题、信息从高安全域流向低安全域的保密问题等。

1.3 计算机信息安全技术解决方案模板

1.3.1 基本的策略

1．操作系统的安全更新

前面已经提到了，没有一个操作系统是绝对安全的。而且，操作系统的漏洞也被频繁地发现。这就需要我们定期地到操作系统网站上去下载、安装安全补丁，以增强系统的安全性。

2．应用程序的安全更新

用户及时的更新应用程序也是非常必要的，尤其是对网络安全产品，如杀毒软件、防火墙软件等。这些安全产品可以更有效地防御病毒、木马程序和攻击。

3．合理设置网络

要合理地构建企业的网络，有效运用防火墙、路由器、认证服务器等设备和安全协议，降低被入侵或攻击的概率。

4．监听与入侵检测

监听与入侵检测是主动的安全手段之一。实时地监听网络并进行入侵检测可以防患于未然，在第一时间抵御黑客的入侵与攻击。

5．审计与记账

审计与记账也是主动的安全手段之一。通过审计与记账功能，管理员能够监视关键的网络访问和与安全相关的操作，并为入侵检测、追踪黑客提供依据。

6．人员问题

这是企业安全策略中最为重要的一点。上至企业的经理，下至每一个员工都要树立强烈的安全意识。要牢记安全问题是每一个人的责任。对于人员问题来说，应该做到以下几点：

- 定期地对企业员工进行安全培训；
- 聘请专职的网络安全人员进行网络维护与管理；
- 要严防企业内部人员对系统的破坏。

正所谓“家贼难防”，攻击在很大程度上是由于内部人员的疏忽、破坏甚至是内外勾结造成的。因此不要忽略了内部员工的危险性。当然，绝大多数员工是不会做这种事情的。

7．事故响应策略

事故响应策略对企业来说也至关重要，就像每个国家都有一套重大突发事件的预案一样。我们要对所有可能发生的安全问题制订一系列的补救措施，提高随机应变的能力。

1.3.2 企业网络设置

为了增强企业网络的安全性，我们要对它进行划分。将网络划分成内部网络与外部网络是目前普遍采用的一种安全技术。

1．外部网络的设置

外部网络是连接内部网络与 Internet 的通道，也是抵御攻击和端口扫描的首要屏障。用户可能会通过拨号、远程网络或其他的方式连接到外部网络。

图 1.1 给出了外部网络设置的一个例子，它包含如下的几个服务器：

- 防火墙：该防火墙具有状态包过滤功能，能有效阻止诸如死亡之 Ping、包洪水等攻击，也可以防止 Nmap 等工具的端口扫描；
- 拨入服务器：对远程的拨号连接进行处理；
- AAA 服务器：对远程用户的访问进行认证、授权与记账；
- 入侵检测服务器：检测是否有入侵。

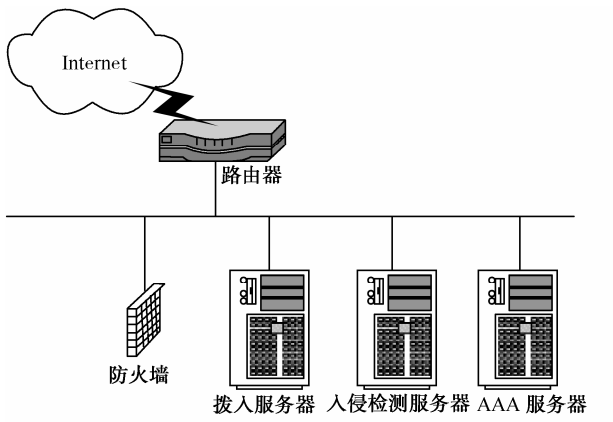

图 1.1 外部网络设置举例


-注释-

有关 AAA 服务器方面的内容将在第 5 章介绍。

2．内部网络的设置

内部网络主要用于企业内部的数据访问，但也不能忽视了其安全性。

图 1.2 给出了一个内部网络设置的例子，采用分段的方式将内部网络划分成不同的子网：

- 域名服务器；
- 入侵检测服务器；

此为试读，需要完整PDF请访问：www.ertongbook.com