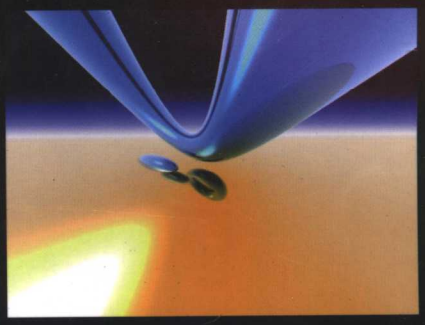
普通高等教育“十一五”国家级规划教材

21世纪高等院校
信息安全系列规划教材

入侵检测技术

曹元大　主编
薛静锋　祝烈煌　阎慧　编著



人民邮电出版社
POSTS & TELECOM PRESS

普通高等教育“十一五”国家级规划教材

21世纪高等院校信息安全系列规划教材

入侵检测技术

曹元大　主编

薛静锋　祝烈煌　阎　慧　编著

人民邮电出版社

北京

图书在版编目（CIP）数据

入侵检测技术 / 曹元大主编；薛静锋，祝烈煌，阎慧编著. —北京：人民邮电出版社，2007.5
（21 世纪高等院校信息安全系列规划教材）

ISBN 978-7-115-16233-5

Ⅰ. 入… Ⅱ. ①曹…②薛…③祝…④阎… Ⅲ. 计算机网络—安全技术—高等学校—教材
Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2007）第 068014 号

内 容 提 要

本书全面、系统地介绍了入侵检测的基本概念、基本原理和检测流程，较为详尽地讲述了基于主机的入侵检测技术和基于网络的入侵检测技术，在此基础上介绍了入侵检测系统的标准与评估，并以开源软件 Snort 为例对入侵检测的应用进行了分析。

本书语言通俗，层次分明，理论与实例结合，可以作为高等学校计算机相关专业或信息安全专业本科生高年级的选修课教材，对从事信息和网络安全方面的管理人员和技术人员也有参考价值。

普通高等教育“十一五”国家级规划教材

21 世纪高等院校信息安全系列规划教材

入侵检测技术

◆ 主　　编　曹元大

编　　著　薛静锋　祝烈煌　阎　慧

责任编辑　邹文波

◆ 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@ptpress.com.cn

网址　http://www.ptpress.com.cn

北京隆昌伟业印刷有限公司印刷

新华书店总店北京发行所经销

◆ 开本：787×1092　1/16

印张：15.25

字数：362 千字　　2007 年 5 月第 1 版

印数：1 –3 000 册　　2007 年 5 月北京第 1 次印刷

ISBN 978-7-115-16233-5/TP

定价：25.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223

21世纪高等院校信息安全系列规划教材

编　委　会

总　序

一、出版背景

随着计算机技术与网络通信技术以及信息产业的高速发展，接入 Internet 的个人和单位主机数量快速增长，尤其是计算机在政府、国防、金融、公安和商业等部门的广泛应用，社会对计算机的依赖越来越大，而计算机系统的安全一旦受到破坏，不仅会导致严重的社会混乱，也会带来巨大的经济损失。世界主要发达国家每年因计算机犯罪所造成的经济损失令人吃惊，远远超过了普通经济犯罪的损失。因此，确保计算机系统的安全已成为世人关注的社会问题，信息安全已成为信息科学的热点课题，信息安全专业也受到了社会各界的普遍关注。

我国信息安全本科专业设置始于 2000 年，教育部首次批准开办信息安全专业。从此以后，每年都有不少高校加入了举办信息安全本科专业的行列。

我国政府对信息安全非常重视，2003 年 9 月，中央《关于加强信息安全保障工作的意见》的 27 号文件，已经把信息安全工作提升到保护公众利益和维护国家安全以及保障与促进信息化发展的高度。2004 年 1 月，国务院召开全国信息安全保障工作会议，特别强调要加强信息安全院系的建设和人才培养工作。信息安全学科专业与信息安全产业必将在中央 27 号文件精神的指引下得到健康、快速的发展。

目前信息安全方面的人才还十分稀少，尤其是政府、国防、金融、公安和商业等部门对信息安全人才的需求很大。具有关部门统计，现在国内从事信息安全的专业人才只有 3500 人左右，并且大多分布在高校和研究院所，而按照信息化发展的状况，社会对信息安全专业的人才需求量达几十万人。要解决供需矛盾，必须加快信息安全人才的培养。人才的培养离不开教材的建设，信息安全专业急需与之教学相配套的教材。

根据教育部高教司函[2003]141 号文件的精神，教育部高等学校电子信息与电气学科教学指导委员会专家组委托北京邮电大学等五所较早举办信息安全本科专业的高等院校完成了“信息安全专业规范”（以下简称“规范”）。该规范已于 2004 年 7 月，在四川绵阳召开的“全国高校本科信息安全专业规范与发展战略研究成果发布与研讨会”上公开发布。与会老师对信息安全专业的发展、专业规范和课程设置展开了热烈的讨论。在会议上，我们征求了大家对信息安全本科专业教材的意见。在细致研究，反复讨论的基础上，规划了与规范相配套的“21 世纪高等院校信息安全系列规划教材”。

二、教材特色

本系列教材具有以下特色。

1．参照“信息安全专业规范”确定教材题目、组织教材书稿内容。

本系列教材的所有题目是根据“信息安全专业规范”确定的。所有教材严格按照“规范”要求，结合信息安全专业的学制、培养规格、素质结构要求、能力结构要求、知识结构要求撰写，使其所含知识点完全覆盖“规范”中的要求，确保能够达到“规范”中的学习目标。

2．注重套书的整体策划。

由于本系列教材涉及的内容比较多，在教材内容选择时，一方面要考虑教材内容相互的衔接，另一方面要考虑许多课程相互之间有内容交叉的现象。我们在一开始策划时就对这两个方面相当重视，多次召开编委会，审定教材的大纲，落实教材的主要知识点，避免了内容的重复。同时，充分考虑了先进性和成熟性之间的和谐关系，确保教材既能够反映信息安全领域的前沿科研状态，又能使学生掌握基础的核心知识和较成熟稳定的技能。

3．特别注意学生工程实际动手能力的培养。

根据“信息安全专业规范”的要求，本系列教材适当减少理论知识和技术知识层次的学时和要求，增加结合工程实际动手实践和专业应用技能层次的学时和要求。

4．本系列教材的作者都是在我国信息安全领域具有丰富教学和实践经验的一流专家，部分教材已经被评为“普通高等教育‘十一五’国家级规划教材”（以下简称“国家十一五规划教材”）。

本系列教材的书名及作者如下。

21 世纪高等院校信息安全系列规划教材

编号	书　名	作者	作者单位
1	信息安全概论	徐茂智	北京大学
2	信息安全数学基础（国家十一五规划教材）	裴定一	广州大学
3	现代密码学（国家十一五规划教材）	何大可	西南交通大学
4	公钥密码学基础与应用	覃中平	武汉大学
5	安全操作系统原理与技术（国家十一五规划教材）	陈钟	北京大学
6	信息安全工程	方勇	四川大学
7	信息安全管理（国家十一五规划教材）	张红旗	解放军信息工程大学
8	信息安全标准与法律法规	秦玉海	中国刑事警察学院
9	网络攻击与防御技术（国家十一五规划教材）	张宏莉	哈尔滨工业大学
10	安全协议及其分析（国家十一五规划教材）	陈钟	北京大学
11	数字水印基础教程（国家十一五规划教材）	杨义先	北京邮电大学
12	计算机病毒原理与防范（国家十一五规划教材）	秦志光	电子科技大学
13	入侵检测技术（国家十一五规划教材）	曹元大	北京理工大学

5．提供完善的教学服务。

为了方便教学，我们免费为选用本套教材的老师提供以下教学服务。

（1）所有教材的电子教案。

（2）部分教材的习题答案。

（3）信息安全专业本科教学实验室建设方案与实验教学指导咨询（联系单位：“北京邮电大学信息安全中心”，联系方式：100876，北京西土城路十号北京邮电大学 126 信箱，yxyang@bupt.edu.cn）。

（4）信息安全专业本科生实习、实训与技能认证咨询（联系单位："北京邮电大学信息安全中心"；"四川绵阳灵创科技园"，联系方式：621000，绵阳市科创园区九州大道中段灵创科技园内灵创科技有限公司，0816-6336559（传真），6336520，yxyang@bupt.edu.cn）。

本系列教材尽管经过反复讨论修改，但限于作者水平和其他条件限制，难免存在不足和值得商榷之处，敬请批评指正。

21世纪高等院校信息安全系列规划教材编委会

2007年1月

前　言

如今，网络安全问题越来越受到人们的关注，也逐渐成为各相关科研机构研究的热点。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多学科的综合性学科。传统的网络安全技术以防护为主，即采用以防火墙为主体的安全防护措施。但是，面对网络大规模化和入侵复杂化的发展趋势，以防火墙技术为主的防御技术越来越显得力不从心，由此产生了入侵检测技术。

入侵检测技术是网络安全的核心技术之一，它通过从计算机网络或计算机系统中的若干关键点收集信息并对其进行分析，从而发现网络或系统中是否有违反安全策略的行为和遭到袭击的迹象。利用入侵检测技术，不但能够检测到外部攻击，而且能够检测到内部攻击或误操作。本书全面介绍了入侵检测技术，重点讲解了入侵检测的有关理论知识、技术原理和应用案例。全书共分 9 章，主要内容介绍如下。

第 1 章主要介绍了入侵检测的相关基础知识，包括入侵检测的产生与发展历程、入侵检测的基本概念、作用以及研究入侵检测的必要性。

第 2 章主要介绍了常见的入侵方法与手段，包括黑客的入侵模型与原理，以及几种常见的入侵攻击方法，其目的是让读者了解黑客入侵的典型方式，这样才有助于部署入侵检测相关设备和工具，查找攻击源，阻击黑客。

第 3 章主要介绍了入侵检测系统的相关知识，包括入侵检测系统的基本模型、入侵检测系统的工作模式和分类方法以及入侵检测系统的部署方式。以使读者了解入侵检测系统的基本轮廓。

第 4 章主要介绍了入侵检测的基本流程，包括入侵检测的过程、入侵检测的数据源、入侵检测的分析模型和方法以及入侵检测的告警与响应方式。以使读者掌握入侵检测的全过程。

第 5 章主要介绍了基于主机的入侵检测技术，包括审计数据的获取和预处理、各种基于主机的入侵检测方法以及基于主机的入侵检测实例。

第 6 章主要介绍了基于网络的入侵检测技术，包括网络数据包的捕获、检测引擎的设计以及基于网络的入侵检测实例。

第 7 章主要介绍了入侵检测系统的标准与评估，包括入侵检测的标准化工作、影响入侵检测性能的参数、评价检测算法性能的测度和评价入侵检测系统性能的标准，在此基础上，介绍了关于网络入侵检测系统的测试评估、测试环境和测试软件，另外还对入侵检测评估现状进行了分析。

第 8 章主要对开放源代码的入侵检测软件 Snort 进行了详细的分析。Snort 是当前使用广泛的具有典型特性的入侵检测软件，通过对 Snort 的介绍与分析可以使读者对入侵检测技术有一个全面的了解。

第9章主要介绍了入侵检测的发展趋势，包括入侵检测技术现状分析以及正在发展中的入侵检测技术。以使读者对入侵检测技术的发展前景有所了解和认识。

本书可以作为高等学校计算机相关专业或信息安全专业本科生高年级的选修课教材，对从事信息和网络安全方面的管理人员和技术人员也有参考价值。阅读本书时，读者应学习过计算机网络、操作系统、信息安全基础等方面的基础知识。本书作为教材使用时，建议课时为32学时，各章学时分配如下。

章	学时数	章	学时数
第1章	2	第2章	3
第3章	3	第4章	6
第5章	4	第6章	4
第7章	4	第8章	4
第9章	2		

本书由北京理工大学曹元大教授主编，北京理工大学薛静锋副教授、祝烈煌博士和装备指挥技术学院阎慧副教授编写。本书在写作过程中得到了北京理工大学王勇博士、李志强老师的热情帮助，在此一并表示感谢。

由于编者水平有限，书中难免存在错误之处，敬请广大读者批评指正。

编者

2007年3月

于北京理工大学

目　录

▶▶▶ 第 1 章

入侵检测概述

1.1 网络安全基本概念

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多学科的综合性学科。本节介绍网络安全的基本概念。

1.1.1 网络安全的实质

计算机网络安全问题是随着网络特别是 Internet 的发展而产生的，直到近年来才得到普遍关注。计算机网络的连通性和开放性给资源共享和通信带来了很大的便利，同时也使本不乐观的安全问题雪上加霜。标准化和开放性使许多厂商的产品可以互操作，也使入侵者可以预知系统的行为。

尽管网络安全的研究得到越来越多的关注，然而，网络安全问题并没有因此而减少。相反，随着网络规模的飞速扩大、结构的复杂和应用领域的不断扩大，出于各种目的，盗用资源、窃取机密、破坏网络的肇事者也越来越多，网络安全事件呈迅速增长的趋势，造成的损失也越来越大。

一般认为，计算机网络系统的安全威胁主要来自于黑客（Hacker）的攻击、计算机病毒（Virus）和拒绝服务攻击（Denies Of Service，DOS）3 个方面。目前，人们开始重视来自网络内部的入侵攻击。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。而且随着攻击工具的完善，攻击者不需要专业知识就能够完成复杂的攻击过程。

总之，人们面临来自计算机网络系统的安全威胁日益严重。安全问题已经成为影响网络发展、特别是商业应用的主要问题，并直接威胁着国家和社会的安全。

网络安全的实质就是要保障系统中的人、设备、设施、软件、数据以及各种供给品等要素避免各种偶然的或人为的破坏或攻击，使它们发挥正常，保障系统能安全可靠地工作。因而网络系统的安全应当包含以下内容。

- 要弄清网络系统受到的威胁及脆弱性，以便人们能注意到网络的这些弱点和它存在的特殊性问题。
- 要告诉人们怎样保护网络系统的各种资源，避免或减少自然或人为的破坏。
- 要开发和实施卓有成效的安全策略，尽可能减小网络系统所面临的各种风险。
- 要准备适当的应急计划，使网络系统中的设备、设施、软件和数据在受到破坏和攻击时，能够尽快恢复工作。
- 要制订完备的安全管理措施，定期检查这些安全措施的实施情况和有效性。

- 确保信息的安全，就是要保障信息完整、可用和保密的特性。

总之，信息社会的迅速发展离不开网络技术和网络产品的发展，网络的广域化和实用化都对网络系统的安全性提出越来越高的要求。从广义上考虑的网络系统所包含的内容非常丰富，几乎囊括了现代计算机科学和技术的全部成果。为了提高网络安全性，需要从多个层次和环节入手，分别分析应用系统、宿主机、操作系统、数据库管理系统、网络管理系统、子网、分布式计算机系统和全网中的弱点，采取措施加以防范。

1.1.2 网络系统的安全对策与入侵检测

近年来，尽管对计算机安全的研究取得了很大进展，但安全计算机系统的实现和维护仍然非常困难，因为我们无法确保系统的安全性达到某一确定的安全级别。入侵者可以通过利用系统中的安全漏洞侵入系统，而这些安全漏洞主要来源于系统软件、应用软件设计上的缺陷或系统中安全策略规范设计与实现上的缺陷和不足。即使我们能够设计和实现一种极其安全的系统，但由于现有系统中大量的应用程序和数据处理对现有系统的依赖性以及配置新系统所需要的附加投资等多方面的限制，用新系统替代现有系统需付出极大的系统迁移代价，所以这种采用新的安全系统替代现有系统的方案事实上很难得到实施。另一方面，通过增加新功能模块对现有系统进行升级的方案却又不断地引入新的系统安全缺陷。

入侵检测是最近 10 余年发展起来的一种动态的监控、预防或抵御系统入侵行为的安全机制。主要通过监控网络、系统的状态、行为以及系统的使用情况，来检测系统用户的越权使用以及系统外部的入侵者利用系统的安全缺陷对系统进行入侵的企图。和传统的预防性安全机制相比，入侵检测具有智能监控、实时探测、动态响应、易于配置等特点。由于入侵检测所需要的分析数据源仅是记录系统活动轨迹的审计数据，使其几乎适用于所有的计算机系统。入侵检测技术的引入，使得网络、系统的安全性得到进一步的提高（例如，可检测出内部人员偶然或故意提高他们的用户权限的行为，避免系统内部人员对系统的越权使用）。显然，入侵检测是对传统计算机安全机制的一种补充，它的开发应用增大了网络与系统安全的纵深保护，成为目前动态安全工具的主要研究和开发的方向。许多研发机构和主要的安全厂商都在进行这方面的研究和开发，有的已推出了相应的产品。

实践经验使人们认识到：由于现有的各种安全防御机制都有自己的局限性。例如，防火墙能够通过过滤和访问控制阻止多数对系统的非法访问，但是不能抵御某些入侵攻击，尤其是在防火墙系统存在配置错误、没有定义或没有明确定义系统安全策略时，都会危及到整个系统的安全。另外，由于其主要是部署在网络数据流的关键路径上，通过访问控制来实现系统内部与外部的隔离，从而对于针对恶意的移动代码（病毒、木马、缓冲区溢出等）攻击、来自内部的攻击等，防火墙将无能为力。因此，针对网络的安全不能只依靠单一的安全防御技术和防御机制。只有通过在对网络安全防御体系和各种网络安全技术和工具的研究的基础上，制订具体的系统安全策略，通过设立多道安全防线、集成各种可靠的安全机制（诸如：防火墙、存取控制和认证机制、安全监控工具、漏洞扫描工具、入侵检测系统以及进行有效的安全管理、培训等）、建立完善的多层安全防御体系，才能够有效地抵御来自系统内、外的入侵攻击，达到维护网络系统安全的目的。