长江学者论丛

入侵检测理论与技术

杨义先　钮心忻　编著

Theory and Technologies of Intrusion Detection

高等教育出版社
HIGHER EDUCATION PRESS

长江学者论丛

入侵检测理论与技术

■ 杨义先　钮心忻　编著

Theory and Technologies of Intrusion Detection

高等教育出版社
HIGHER EDUCATION PRESS

内容提要

本书从理论和技术两个方面对入侵检测相关知识进行了全面和系统的介绍。全书共分7章，分别对常见入侵与防御、入侵检测基础、大规模分布式入侵检测系统（LDIDS）框架结构、LDIDS的互动协议与接口标准、LDIDS的任务分派机制、LDIDS的数据融合和入侵管理等进行了介绍，内容包括网络安全的主要威胁、常见网络攻击、DDoS攻击与防御、智能型分布式防御、IDS系统模型等入侵检测理论与技术方面的知识。另外，书中介绍的许多算法、协议、方案等都可直接应用于工程实践，书中提出的许多理论问题也有助于激发更多的后继研究。

本书可作为信息安全、密码学、信息与计算科学等专业的研究生和高年级大学生的教学参考书，也可作为上述领域相关科技工作者的实用工具书或技术培训教材。

图书在版编目（CIP）数据

入侵检测理论与技术/杨义先，钮心忻编著. —北京：高等教育出版社，2006.9

ISBN 7-04-020016-3

Ⅰ.入… Ⅱ.①杨…②钮… Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆CIP数据核字（2006）第098103号

出版发行	高等教育出版社	购书热线	010-58581118
社　　址	北京市西城区德外大街4号	免费咨询	800-810-0598
邮政编码	100011	网　　址	http://www.hep.edu.cn
总　　机	010-58581000		http://www.hep.com.cn
		网上订购	http://www.landraco.com
经　　销	蓝色畅想图书发行有限公司		http://www.landraco.com.cn
印　　刷	北京新丰印刷厂	畅想教育	http://www.widedu.com
开　　本	787×1092　1/16	版　　次	2006年9月第1版
印　　张	21.25	印　　次	2006年9月第1次印刷
字　　数	400 000	定　　价	37.30元

本书如有缺页、倒页、脱页等质量问题，请到所购图书销售部门联系调换。

物料号　20016-00

作者简介

杨义先，北京邮电大学教授，博士生导师，首届长江学者特聘教授，首届政府特殊津贴获得者。长期从事信息安全、信号与信息处理、密码学等专业的教学、科研和成果转化工作。已发表论文300余篇、出版著作10余部。本书相关研究成果获邮电部科技进步一等奖、国家教委科技进步二等奖、中国通信学会科学技术二等奖等多项奖励。

钮心忻，北京邮电大学教授，博士生导师，北京邮电大学数字内容研究中心主任。一直从事数字水印与信息隐藏、网络信息安全、软件无线电、信号与信息处理等方面的科研和教学工作。在包括IEEE Trans. On AES等在内的国内外著名学术刊物上发表论文30余篇，完成专著数部，作为项目负责人承担了多项国家级和省部级科研项目，研究成果获中国通信学会科学技术二等奖、信息产业部科技进步三等奖等多项奖励。

郑重声明

策划编辑　刘　英
责任编辑　郭福生
封面设计　于　涛
责任绘图　朱　静
版式设计　范晓红
责任校对　杨凤玲
责任印制　朱学忠

“长江学者”学术著作出版资助项目

“长江学者论丛”编辑出版指导委员会

主 任 委 员：赵沁平　教育部副部长

副主任委员：金国藩　清华大学教授，中国工程院院士

闵乃本　南京大学教授，中国科学院院士

吴树青　北京大学教授，教育部社科委主任

饶子和　清华大学教授，中国科学院院士，长江学者特聘教授

舒德干　西北大学教授，长江学者特聘教授，长江学者成就奖获得者

“长江学者论丛”编辑出版指导委员会办公室

主　　任：吴德刚　教育部人事司司长

副 主 任：刘志鹏　高等教育出版社社长

吕玉刚　教育部人事司副司长，教育部人才发展办公室主任

吴　向　高等教育出版社副总编辑

序

当今世界，科学技术日新月异，知识经济方兴未艾，综合国力竞争日趋激烈。面对日益激烈的国际竞争，立足国情，我国只能走建设创新型国家的发展道路，把提高自主创新能力作为调整经济结构、转变增长方式、提高国家竞争力的中心环节。而科技和人才，特别是创新人才是建设创新型国家和提高自主创新能力的关键。实施科教兴国、人才强国战略，建设创新型国家，构建社会主义和谐社会，高等学校肩负着重大历史使命。教育大计，人才为本。人才问题，始终是高等学校改革与发展的核心问题和头等大事。加快建设高等学校高层次人才队伍，努力培养和造就一批在国际上有重要影响的学术大师、战略科学家和学科带头人，是发展我国高等教育事业的必然要求，也是关系社会主义现代化建设全局的重要任务。

为贯彻落实科教兴国和人才强国战略，推进我国高等学校高层次人才队伍建设，教育部与香港李嘉诚基金会于1998年共同启动了“长江学者奖励计划”。该计划自实施以来，在党和国家领导人的高度重视和关心下，在国家财政等有关部门、高等学校和社会各界的大力支持下，取得了显著成效，在海内外引起了强烈反响。诺贝尔物理学奖获得者杨振宁评价“长江学者奖励计划”是“一个非常了不起的壮举”，“是20世纪末21世纪初中国实施科教兴国战略的一个非常重要的环节。”

长江学者群英荟萃、硕果累累。“长江学者奖励计划”的实施吸引、汇聚和造就了一大批优秀拔尖人才。目前全国88所高等学校聘任727位长江学者，先后有6位优秀学者获得“长江学者成就奖”，31位长江学者被聘为“973”首席科学家，24位长江学者当选为中国科学院、中国工程院院士。在“长江学者奖

励计划”的激励和支持下，长江学者们取得了一批重大科研成果，近年来共有20余篇论文发表在《Nature》、《Science》上，近百项科研成果获得国家自然科学奖、技术发明奖、科技进步奖，其中3项成果获得一等奖，20余项重要成果入选“中国十大科技进展新闻”、“中国基础研究十大新闻”、“中国高校十大科技进展”，有力地支持了国家重大战略的实施，促进了学科建设和科技发展，为培养和造就优秀拔尖创新人才做出了贡献。

编辑出版长江学者学术著作，得到了广大长江学者的积极响应和高等教育出版社的大力支持。希望《长江学者论丛》的出版，进一步提高长江学者在学术领域的影响力，并激励广大学者弘扬长江学者的创新精神，勇攀科学高峰，更好地为促进高校在提高国家自主创新能力、建设创新型国家的伟大事业中，做出更大的贡献。

2006年1月

前　言

顾名思义，入侵检测就是检测入侵行为。目前的入侵检测系统（IDS）大致可以分为两类：基于主机的 IDS 和基于网络的 IDS。前者是一种集中式的 IDS，相当于直接针对敌方总部，一旦发现敌情马上报告，并采取相应的措施。后者是一种分散式的 IDS，它广泛收集敌方各军事点的情报，加以综合分析，一旦发现敌情，马上采取措施加以应对。

最近，基于网络的 IDS 又进一步发展成为分布式 IDS 和大规模分布式 IDS。形象地说，分布式 IDS 不但要对敌国的各军事点情报进行综合和分析，而且也不放过敌国其他领域的情报，比如，根据敌国大量屯集医药用品的事实来判断敌国可能发动战争等。而大规模分布式 IDS 则将刺探敌情的范围扩大到敌国的伙伴国家，因为，这些国家的异常举动可能泄露某种攻击信息。

本书将对包括基于主机的 IDS 和基于网络的 IDS 进行研究，重点研究分布式 IDS 和大规模分布式 IDS 系统的理论和技术。全书共分为 7 章，各章内容与安排如下。

第 1 章着重分析了当今主流网络攻击手段，并针对每一种攻击，尽量提出相应的检测、防御方法。当前的入侵方法中，有的是寻找并利用操作系统的漏洞，有的是利用应用程序的实现上的漏洞，有的是针对网络协议漏洞而进行攻击，有的是寻找加密算法的弱点进行密码破解，有的是利用网络协议在特定的操作系统上的实现的漏洞进行入侵，等等。本章重点分析了目前常见的拒绝服务攻击和分布式拒绝服务攻击的原理和手段，包括 TCP 标志位攻击、通用洪流攻击、反射式攻击等；介绍了常用的分布式拒绝服务攻击工具，包括 Trinoo、TFN、TFN2K、Stacheldraht、shaft 和 mstream 等；总结了目前分布式攻击的类型和特点。在对目前分布式攻击的类型和特点分析的基础上，提出了分布式攻击的发展趋势，主要包括体系结构及特点。其中主要特点包括可控性强、隐蔽性强、可更新性、智能性和通信安全保密性等。本章将目前针对分布式拒绝服务攻击的防御划分为三个层次并进行比较，然后提出了源端防御的概念；介绍了源端防御程序设计并给出其体系结构及各模块结构图。本章在对分布式拒绝服务攻击的防御手段进行深入分析后，提出了未来分布式防御的发展趋势及智能型分布式防御模型，给出了模型的体系结构和特点，并分析了实现需要解决的一些关键问题。

第 2 章对现有入侵检测领域的各种检测模型和技术进行综述和归类分析，详细地讨论了各种技术的优缺点。提出了基于系统行为分类的检测模型和基于数据流的入侵检测系统设计模型。讨论了评测检测系统与检测算法的

性能和重要测度。给出了采用多检测器结果进行数据融合，来提高系统检测率、减小虚警率的解决方案。研究了通过监控系统关键程序来检测入侵的技术，设计了实用的神经网络分类器或贝叶斯分类器，提出了一个基于系统行为分类检测模型的入侵检测系统设计原型及其详细设计和系统框图。首次解决了同时对系统中的多个系统关键程序的执行进行监控的问题。在分析网络数据多维属性特征模型的基础上，讨论并给出了网络入侵检测可利用的网络数据特征以及相应的知识获取和数据分析技术。在对网络入侵检测所面临的问题进行分析和研究的基础上，提出了一个网络入侵检测系统的分布式体系架构。并且针对检测子系统间的协作，提出了一个基于贝叶斯分类器的多探测器结果融合决策的解决方案，然后从网络安全纵深防御体系的角度分析了入侵检测在网络安全中的地位。

第3章根据大规模分布式环境的特点，提出了一种具有分层式框架结构的大规模分布式入侵检测系统。这种大规模分布式入侵检测系统可以根据网络规模的变化灵活地进行配置，而框架结构中的任何一个独立的结点都可以视为一个完整的入侵检测系统。通过对入侵检测系统特点的归纳，本章提出了可加入入侵检测系统框架的入侵检测系统的标准。组成该标准的模块具有4层结构。符合该4层结构标准的入侵检测系统不仅是大规模分布式入侵检测系统的一部分，而且也是一个独立的入侵检测系统。整个入侵检测系统由多个功能模块构成，分层结构更明确地说明了功能模块之间如何协同完成检测工作。尽管各个入侵检测系统不尽相同，但运作机制符合该4层结构标准的系统都可以很好地完成大规模分布式入侵检测的任务。

第4章设计了一套可以实现安全部件之间交换数据、告警和命令的协议和接口标准。本章重点介绍的SCXP协议建立在BEEP协议的基础上，保证了通信的安全性和实时性，实现了安全部件之间的双向通信。而SCIMF消息格式定义了安全部件之间传送的消息，实现了对安全事件进行报警、响应、控制、广播等操作。

第5章首先简要介绍了入侵检测技术和移动代理技术，然后研究了移动代理技术在入侵检测中的应用和任务分派机制。本章根据分布式大规模入侵检测系统的特征，研究了引入移动代理技术的可行性和优势，同时研究了任务分派机制的整个过程，包括功能层代理的设计、代理向协调模块的注册、代理的命名、代理之间通信的消息格式、代理的通信模型以及协调模块对代理的复制、分派、终止等过程。使用任务分派机制，就是根据需要由协调模块派出移动代理，到需要的地方去执行任务。这样一方面加强了那里的处理能力，使某一结点的处理能力和实际的需求相适应，使得某一结点的负载不会过大；另一方面派出移动代理可以执行特殊的任务，也就是说，下层的静态代理只具备常规的处理能力，完成一般的处理任务，但它们具备一定的怀疑能力。而协调模块派出的移动代理是

专门用于处理复杂情况的，比如检测未知攻击等。

第6章重点介绍了大规模分布式入侵检测系统中的数据融合算法。算法主要通过聚类、合并和关联3个步骤实现。从各个安全部件送上来的低级告警首先通过聚类模块进行预处理，并按照相似度形成告警簇，各个告警簇再通过合并模块生成一个或多个中级告警，最后关联模块利用单个攻击的前、后件之间的因果关系将多个中级告警关联合并成高级告警并输出。其中聚类、关联是关键模块。聚类模块只需要分析告警之间的简单的冗余关系，但处理对象是数目比较多的低级告警，因此本章采用基于概率的方法，通过计算告警之间的相异度来实现聚类；而关联模块需要分析告警之间的复杂的因果关系，但处理对象是数量已经精简的中级告警，因此本章采用基于专家系统的方法，通过对攻击建模，产生关联规则，然后利用关联规则进行关联。

第7章在入侵防御、入侵容忍和入侵管理系统的体系结构、检测技术、告警管理以及主动响应及互动协议方面开展了研究。主要包括：对DARPA提出的公共入侵检测框架(CIDF)在分布式方面进行了改进和扩展，增加了分布式入侵检测系统的协调模块和管理模块的任务分派功能，并提出一种“分布采集、动态协调、智能管理”的体系结构参考模型；通过分析分布式入侵的特点，提出了基于静态代理和移动代理技术相结合的入侵管理系统(MADIMS)，它采用“分布采集、动态协调、区域管理”概念模型，用一个类似树状的结构来构造分布式入侵管理系统；在分析了产生大量无用告警的原因的基础上，提出一种基于“过滤→关联→聚类→合并”告警融合处理机制的入侵管理技术。

本书的各章(甚至各节)都尽量相对独立，以适应各种需求之读者自由组合并阅读相关章节。希望本书所列的详细章节目录有助于读者迅速了解每一章节的主题，并据此迅速找到自己关心的内容。如果我们的这些努力能够提高读者的阅读效率，那么我们就心满意足了。

本书是北京邮电大学信息安全中心和北京邮电大学数字内容研究中心全体成员多年来集体智慧的结晶。在本书写作过程中李中献博士、夏光升博士、张振涛博士、李新博士、曾志峰博士、李鸿培博士、徐国爱博士、张茹博士、崔宝江博士、谷利泽博士、辛阳博士、郑康锋博士、李晖博士、李剑博士、杨榆博士、李丽香博士、周亚建博士后、吕慧勤博士、褚永刚博士、王自亮硕士、张宏硕士、陈亚娟硕士、宋传恒硕士、王伟硕士、吕明硕士、陶明硕士、张小芬硕士、张洁硕士、杨亚飞硕士、安宁硕士、魏战松硕士等为本书提供了丰富的资料。特别感谢胡正名教授、温巧燕教授、罗守山教授、牛少彰教授、罗群教授，他们同心协力，率领北京邮电大学信息安全中心和北京邮电大学数字内容研究中心两百余位研究人员在网络信息安全研究的丰硕成果是本书的营养源泉。本书也是国家“863”项目“分布式大规模入侵检测的互动协议和接口标准研究”(编号：2002AA143041)和国家“863”项目“IPS、IMS相关技术研究”(编号：2005AA143040)的成果总结。本

书还获得了国家自然科学基金项目“入侵检测理论与技术”(批准号:60424006)的资助,特此致谢。

由于作者水平有限,书中难免出现各种失误和不当之处,欢迎大家批评指正。

作者

2006 年 5 月

目　录