高·等·院·校·信·息·安·全·专·业·系·列·教·材

中国计算机学会教育专业委员会与清华大学出版社联合组织编写

名誉主编：何德全　编委会主任：肖国镇

Intrusion Detection

入侵检测技术

唐正军　李建华　编著

http://www.tup.com.cn

清华大学出版社

高·等·院·校·信·息·安·全·专·业·系·列·教·材

Intrusion Detection

入侵检测技术

唐正军 李建华 编著

清华大学出版社
北京

内容简介

本书全面细致地讲述了入侵检测的各项技术，概念清晰，行文流畅，侧重基础，兼顾实用。全书共分为12章。其中，第1章和第2章主要介绍了入侵检测相关的历史和概念；第3章对入侵检测的信息来源、技术分类和若干现有的实际系统做了简要介绍；第4章和第5章分别对基于主机的入侵检测技术和基于网络的入侵检测技术进行了介绍；第6章介绍了混合型入侵检测技术的特点；第7章对若干先进入侵检测算法的应用情况做了简要的介绍；第8章对分布式入侵检测架构的设计问题进行了分析讨论；第9章和第10章分别对入侵检测系统在设计时所要考虑的若干实际问题和入侵检测的响应问题进行了介绍；第11章和第12章对相关的法律问题和未来的技术发展前景做了介绍和展望。

本书适合作为计算机、信息安全、通信等相关专业的高年级本科生和研究生的教学用书，也可供广大网络安全工程技术人员参考。

图书在版编目(CIP)数据

入侵检测技术/唐正军，李建华编著. —北京：清华大学出版社，2004.4

(高等院校信息安全专业系列教材)

ISBN 7-302-08282-0

Ⅰ. 入… Ⅱ. ①唐… ②李… 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(2004)第019140号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦

http://www.tup.com.cn　　**邮　　编**：100084

社 总 机：010-62770175　　**客户服务**：010-62776969

组稿编辑：张　民

文稿编辑：王冰飞

印 装 者：北京鑫海金澳胶印有限公司

发 行 者：新华书店总店北京发行所

开　　本：185×230　**印张**：15　**字数**：299千字

版　　次：2004年4月第1版　2004年4月第1次印刷

书　　号：ISBN 7-302-08282-0/TP·5971

印　　数：1～5000

定　　价：24.00元

高等院校信息安全专业系列教材

编审委员会

序

在社会信息化的进程中，信息已成为社会发展的重要资源，信息安全也成为21世纪国际竞争的重要战场。为了保护国家的政治利益和经济利益，各国政府都非常重视信息和网络安全，信息安全已成为一个世纪性和全球性的研究课题。

我国的信息安全事业正在蓬勃发展，国家领导高度重视，各部门通力合作、统筹规划，大大加快了我国信息安全产业发展的步伐。随着信息安全产业的快速发展，社会对信息安全人才的需求在不断增加，在高等教育领域大力推进信息安全的专业化教育，将是国家在信息安全领域掌握自主权、占领先机的重要举措。

目前，许多大学和科研院所已设立了信息安全专业或是开设了相关课程。很高兴中国计算机学会教育专业委员会和清华大学出版社在近期联合组织了一系列信息安全专业的研讨活动。他们以严谨负责的态度，认真组织全国各高校和科研院所的专家、学者，共同研讨信息安全专业的教育方法和课程体系，并在进行大量前瞻性研究工作的基础上，启动了“高等院校信息安全专业系列教材”的编写工作。这套教材将是我国信息安全专业的第一套完整、权威的教材，相信可以对全国的高等院校信息安全专业的建设起到很好的促进作用。

希望中国计算机学会教育专业委员会和清华大学出版社能够将这个研究课题一直做下去，也希望这套教材能够取得成功并不断完善，以促进各高等院校培养出更多、更好的信息安全专门人才，为我国的信息安全事业做出更大的贡献。

何德全

中国工程院院士

高等院校信息安全专业系列教材编审委员会名誉主编

2003年7月于北京

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，国家对信息安全人才的需求量不断增加，但目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信工程、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家何德全院士担任名誉主编，著名学者肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了编写教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣，又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整，结构合理，内容先进。

② 适应面广，能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套，除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经专家推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足大家的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

中国计算机学会教育专业委员会

清华大学出版社

2003 年 7 月

前言

计算机和互联网技术正在改变着人类社会的面貌，与之伴随而来的是信息和网络安全的问题。作为整体安全保护机制的重要环节，入侵检测技术本身也在不断发展和进步。国内各个高校陆续开设了信息安全方面的课程，但是还存在着若干实际的问题，如缺乏用作教学用途的教材。此次，借着清华大学出版社组织出版信息安全教材丛书之际，作者在过去研究和写作的基础之上，按照教材体例的要求编著出版了本书。在编写过程中，作者一直强调概念的清晰性和知识的基础性。希望本书的内容组织和写作方式，能够满足读者对入侵检测技术的教学需求。

本书的内容组织共分为三大部分。

第一部分包括第 1 章和第 2 章，介绍了入侵检测技术的发展历史、入侵检测的基本概念、对应的基本检测模型，以及相关的安全模型等问题。这部分包括了入侵检测技术的基础、背景知识和总体框架。

第二部分是本书的主要部分，包括第 3 章至第 8 章，共 6 章内容，主要介绍各种具体类型的入侵检测技术。其中，第 3 章介绍了入侵检测常用的各种信息来源，包括操作系统的审计记录、系统日志、应用程序的日志信息、基于网络数据的信息源等，并对不同信息来源的特点和信息源的选择问题分别进行了介绍；第 4 章主要介绍了基于主机的入侵检测技术，其中包括如何获取审计数据、应用于入侵检测的统计模型和专家系统规则检测技术、状态转移分析技术以及其他主机检测技术；第 5 章介绍了基于网络的入侵检测技术，首先对网络协议基本知识进行了回顾，然后介绍了数据包截获技术，最后对主要的网络入侵检测引擎的设计机制进行了介绍；第 6 章分别对采用多种信息源和多种检测技术的混合型入侵检测技术进行了实例分析；第 7 章简要回顾了若干先进检测算法在入侵检测中的应用情况；第 8 章对分布式的入侵检测架构设计问题进行了较为深入的讨论，其中包括需要解决的关键问题、基础设计的实例分析以及进一步的发展等。

第三部分包括第 9 章至第 12 章，主要讨论与入侵检测技术相关的其他

问题。第 9 章介绍在入侵检测系统设计时需要考虑的若干实际问题；第 10 章关注入侵检测的响应问题，对响应策略的确定以及响应组件的设计进行了介绍；第 11 章介绍了与入侵检测相关的法律问题，包括网络空间中的法律运用和入侵证据的处理等；第 12 章对入侵检测技术的未来发展进行了展望。

本书在编写过程中得到了作者所在的上海交通大学入侵检测研究小组（SJTU-IDRG）成员伍星、陈杰、刘志辉、马思佳、罗自立、丁海波等人的大力帮助，这里对他们表示衷心的感谢。本书在材料组织过程中参考了大量的技术文献和资料，在此对相关的作者表示敬意，并请广大读者对本书提出宝贵意见与建议。本书的责任编委张玉清博士认真审阅了书稿，并提出了许多宝贵的意见与建议，这里一并表示衷心的感谢。最后，希望本书的出版能够为入侵检测技术的普及起到积极作用。

作　者

2004 年 3 月

目 录

第1章 入侵检测技术的历史

1.1 主机审计——入侵检测的起点

主机审计出现在入侵检测技术之前，其定义为：产生、记录并检查按照时间顺序排列的系统事件记录的过程。在早期的中央主机集中计算的环境之下，主机审计的主要目的是统计用户的上机时间，便于进行计费管理。不久，随着计算机的普及，审计的用途扩展到了跟踪记录计算机系统的资源使用情况，经过进一步的发展，主机审计开始应用于追踪调查计算机系统中用户的不正当使用行为的目的。此时的主机审计，已经逐步开始引入了安全审计的概念。安全审计的主要需求来自于商业领域和军事、行政领域，其中后者的强大需求和支持迅速推动了安全审计的发展。

美国军方在20世纪70年代支持了一项内容广泛的关于计算机系统安全的研究计划，最终的研究成果包括了一项重要的计算机安全评估标准，即TCSEC(可信计算机系统评估准则)。TCSEC准则首次定义了计算机系统的安全等级评估标准，并且给出了满足各个安全等级的计算机系统所应满足的各方面的条件。TCSEC准则规定，作为C2和C2等级以上的计算机系统必须包括审计机制，并给出满足要求的审计机制所应达到的诸多安全目标。在此之后，计算机安全问题得到了更多的注意和重视，其中美国军方特别设立了一个针对计算机审计机制的研究项目，该项目由James-Anderson负责主持。

James-Anderson在1980年完成的技术报告《计算机安全威胁的监控》("Computer Security Threat Monitoring and Surveillance")中，首次明确提出安全审计的目标，并强调应该对计算机审计机制做出若干修改，以便计算机安全人员能够方便地检查和分析审计数据。Anderson在报告中定义了3种类型的恶意用户。

① 伪装者(Masquerader)：此类用户试图绕过系统安全访问控制机制，从而利用合法用户的系统账户。例如，使用盗窃而来的口令和密码访问系统的入侵者。

② 违法者(Misfeasor)：在计算机系统上执行非法活动的合法用户。

③ 秘密活动者(Clandestined User)：此类用户在获取系统最高权限后，利用此种权限以一种审计机制难以发现的方式进行秘密活动，或者干脆关闭审计记录过程。

Anderson 关注如何发现伪装者的问题，并在其报告中指出，可以通过观察在审计数据记录中的偏离历史正常行为模式的用户活动来检查和发现伪装者和一定程度上的违法者。Anderson 对此问题的建议，实质上就是入侵检测中异常检测技术的基本假设和检测思路，为后来的入侵检测技术发展奠定了早期的思想基础。

Anderson 的技术报告被视为在入侵检测领域内一篇最早的技术文献，起到了重要的思想启蒙作用。

1.2 入侵检测基本模型的建立

1987 年 Dorothy Denning 发表了入侵检测领域内的经典论文《入侵检测模型》("An Intrusion Detection Model")，文中对入侵检测问题进行了深入的讨论，建立了入侵检测的基本模型，并提出了几种可能的检测方法。这篇文献正式启动了入侵检测领域内的研究工作，被认为是入侵检测领域内的开创性成果。

Denning 提出的统计分析模型在早期研发的入侵检测专家系统(Intrusion Detection Expert System，IDES)中得到较好的实现。IDES 系统中的统计分析组件，采取了一组特征量度值(例如文件访问、CPU 使用等)来建立系统活动的正常行为模式，之后计算出当前用户行为与先前正常活动模式的偏离程度，并根据偏离程度的大小来判断是否发生了入侵活动。可以看出，IDES 系统主要采纳了 Anderson 的技术报告中所给出的检测建议，但是，Denning 的论文中还包括了其他检测模型，详细内容在 4.2 节中介绍。

Denning 对入侵检测的基本模型给出了建议，如图 1-1 所示。

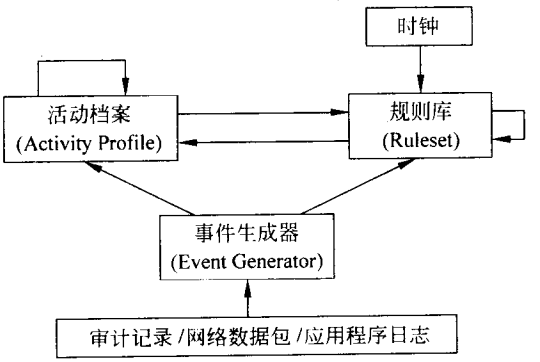

图 1-1 通用入侵检测模型

在图 1-1 所示的通用入侵检测模型中，事件生成器从给定的数据来源中(包括主机审

计数据、网络数据包和应用程序的日志信息等),生成入侵检测事件,并分别送入到活动档案计算模块和规则库检测模块中。活动档案模块根据新生成的事件,自动更新系统行为的活动档案;规则库根据当前系统活动档案和当前事件的情况,发现异常活动情况,并可以按照一定的时间规则自动地删减规则库中的规则集合。

Denning 所提出的入侵检测基本模型,其意义在于一般化的模型定义,并不强调具体的实现技术。基本模型中的各个部件都可根据实际系统的设计要求,加以具体实现,同时可以加以细化和进一步扩展。

1.3 技术发展的历程

入侵检测技术自 20 世纪 80 年代早期提出以来,经过 20 多年的不断发展,从最初的一种有价值的研究想法和单纯的理论模型,迅速发展出种类繁多的各种实际原型系统,并且在近 10 年内涌现出许多商用入侵检测系统产品,成为计算机安全防护领域内不可缺少的一种重要的安全防护技术。本节将带领读者回顾入侵检测技术在过去历史时期内的发展历程,帮助加深对入侵检测的理解。

1980 年,Anderson 在其完成的一份技术报告中提出了改进安全审计系统的建议,以便用于检测计算机用户的非授权活动,同时,提出了基本的检测思路。

1984—1986 年,Denning 和 Neumann 在 SRI 公司内设计和实现了著名的 IDES,该系统是早期入侵检测系统中最有影响力的一个。IDES 系统采纳了 Anderson 提出的若干建议。IDES 系统包括了统计分析组件和专家系统组件,同时实现了基于统计分析的异常检测技术和基于规则的滥用检测技术。IDES 系统的设计思路给后来的很多类似系统提供了启发。

1987 年,Dorothy Denning 发表的经典论文"An Intrusion Detection Modal"中提出入侵检测的基本模型,并提出了几种可用于入侵检测的统计分析模型。Denning 的论文正式启动了入侵检测领域内的研究工作。

同年,在 SRI 召开了首次入侵检测方面的专题研讨会。

1989—1991 年,Stephen Smaha 设计开发了 Haystack 入侵检测系统,该系统用于美国空军内部网络的安全检测目的。Haystack 同时采用了两种不同的统计分析检测技术,来发现异常的用户活动。早期的原型系统采用批处理的离线处理方式。

1990 年,加州大学 Davis 分校的 Todd Heberlien 发表在 IEEE 上的论文"A Network Security Monitor",标志着入侵检测第一次将网络数据包作为实际输入的信息源。NSM 系统截获 TCP/IP 分组数据,可用于监控异构网络环境下的异常活动。

1991 年，在多个部门的赞助支持下，在 NSM 系统和 Haystack 系统的基础上，Stephen Smaha 主持设计开发了 DIDS(分布式入侵检测系统)。DIDS 是首次将主机入侵检测和网络入侵检测技术进行集成的一次努力，它具备在目标网络环境下跟踪特定用户异常活动的能力。

1992 年，加州大学圣巴巴拉分校的 Porras 和 Ilgun 提出了状态转移分析的入侵检测技术，并实现了原型系统 USTAT，之后发展出 NSTAT、NetSTAT 等系统。

差不多同一时期，Kathleen Jackson 在 Los Alamos 国家实验室设计开发了 NADIR 入侵检测系统，该系统用于监控 Los Alamos 的内部计算网络环境，采用了以每周计算活动档案的统计技术来描述用户的活动情况，并使用专家系统规则来检测异常的用户行为。

而 SAIC 和 Haystack Labs 分别开发出了 CMDS 系统和 Stalker 系统，这两个系统是首批投入商用的主机入侵检测系统。

1994 年，Porras 在 SRI 开发出 IDES 系统的后继版本 NIDES 系统，后者在系统整体结构设计和统计分析算法上有了较大改进。进一步，SRI 开发了用于分布式环境的 EMERALD 系统，该系统设计在大型分布式网络环境下工作，具备在不同功能层次上进行检测分析的能力，体现了不同检测部件之间的协作性能。EMERALD 采纳了 IDES 和 NIDES 的检测技术，具备统计分析和规则分析的能力。

1995 年，普渡大学的 S. Kumar 在 STAT 的思路基础上，提出了基于有色 Petri 网的模式匹配计算模型，并实现了 IDIOT 原型系统。

1996 年，新墨西哥大学的 Forrest 提出了基于计算机免疫学的入侵检测技术。

1997 年，Cisco 公司开始将入侵检测技术嵌入到路由器，同时，ISS 公司发布了基于 Windows 平台的 RealSecure 入侵检测系统，自此拉开商用网络入侵检测系统的发展序幕。

1998 年，MIT 的 Richard Lippmann 等人为 DARPA 进行了一次入侵检测系统的离线评估活动，该评估活动使用的是人工合成的模拟数据，最后的测试结果对于后来的入侵检测系统开发和评估工作都产生了较大影响。

1999 年，Los Alamos 的 V. Paxson 开发了 Bro 系统，用于高速网络环境下的入侵检测。Bro 系统在设计上考虑了鲁棒性、安全性，并且处理了许多反规避的技术问题。

同年，加州大学的 Davis 分校发布了 GrIDS 系统，该系统试图为入侵检测技术扩展到大型网络环境提供一个实际的解决方案。

Wenke Lee 提出了用于入侵检测的数据挖掘技术框架。

2000 年，普渡大学的 Diego Zamboni 和 E. Spafford 提出了入侵检测的自治代理结构，并实现了原型系统 AAFID 系统。

值得指出的是，在发展的早期阶段(1984—1992 年)，入侵检测还仅仅是个有趣的研