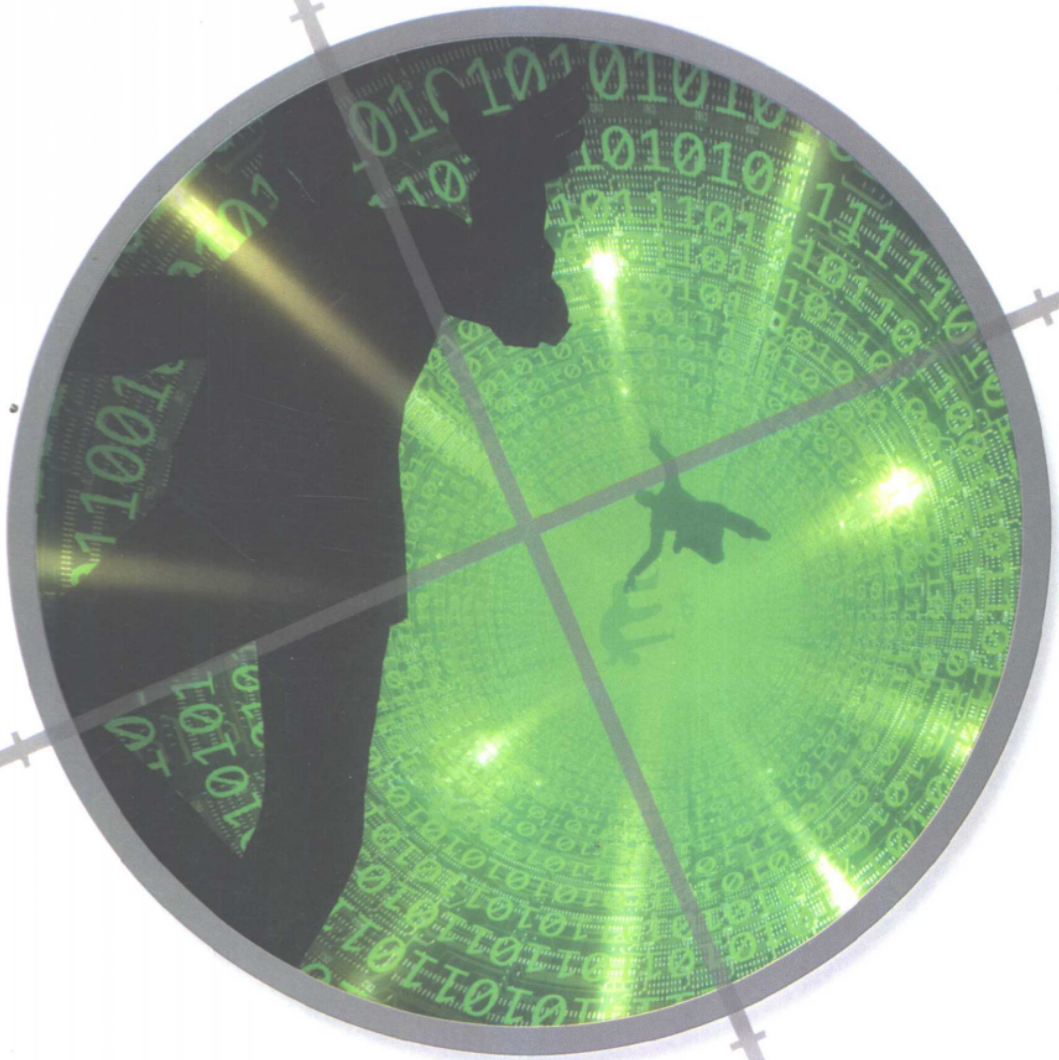
21世纪网络工程丛书——安全防卫系列

附CD



黑客入侵防护系统源代码分析

唐正军 编著

机械工业出版社
China Machine Press

ISBN 7-111-09795-5/TP·2302
选题策划：边　萌
封面设计：樊　俊

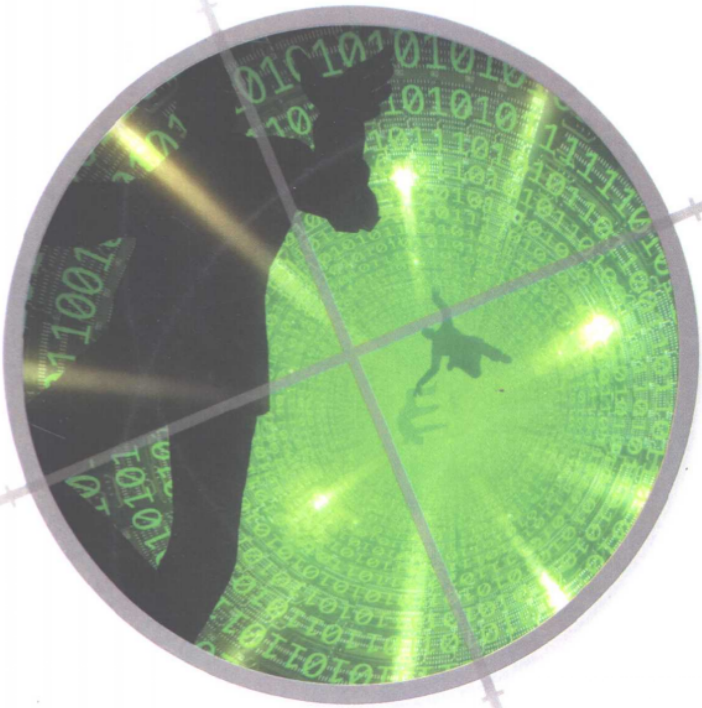
21世纪网络工程丛书——安全防卫系列

黑客攻击技术揭秘

黑客防范技术揭秘

阻击黑客进攻防卫技术

黑客入侵防护系统源代码分析



ISBN 7-111-09795-5
9 787111 097952 >

地址：北京市百万庄大街22号
电话：68326335　邮编：100037
http://www.cmpbook.com
E-mail:online@cmpbook.com

定价：37.00元（附1CD）

21世纪网络工程丛书——安全防卫系列

黑客入侵防护系统源代码分析

唐正军　编著

机械工业出版社

这是一本介绍黑客入侵检测系统的书，全书内容共分为6章。第1章为概述部分，简要回顾了入侵检测系统的发展和主要技术分类。第2、3章对两个具体的入侵检测系统（IDES和NIDES）做了详细的分析和介绍。在第4章中，给出了设计一个网络入侵检测系统所需的基础知识。第5章列出了一个实际入侵检测系统Snort的主体源代码目录。最后一章，对Snort系统的源代码做出了详尽分析。

本书适用于计算机和信息安全专业的高校教师和研究生以及广大网络安全工程技术人员参考之用。

图书在版编目（CIP）数据

黑客入侵防护系统源代码分析/唐正军编著. —北京：
机械工业出版社，2002.3
（21世纪网络工程丛书——安全防卫系列）
ISBN 7-111-09795-5

Ⅰ.黑... Ⅱ.唐... 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（2002）第001570号

机械工业出版社（北京市百万庄大街22号 邮政编码100037）
责任编辑：边 萌
责任印制：路 琳
中国建筑工业出版社密云印刷厂印刷·新华书店北京发行所发行
2002年3月第1版第1次印刷
1000mm×1400mm B5·12.875印张·501千字
0 001—5000册
定价：37.00元 （含1CD）
凡购本书，如有缺页、倒页、脱页，由本社发行部调换
本社购书热线电话（010）68993821、68326677-2527

前　言

当前在全球范围内，对计算机及网络基础设施的攻击行为，已经成为一个越来越严重和值得关注的问题，特别是各种政府机构的网站，更是成为黑客攻击的热门目标。从数年前开始直至最近的大量关于网站被侵和机密资料泄漏的报道都证实了这一点。事实上，这些网络上发生的入侵事件数目的不断增长，同时也反映了互联网络的快速发展历程。近年来对电子商务的热切需求，只会更加激化这种入侵事件的增长趋势。与以往的入侵者大多是出于对互联网络本身的探索或者检验自身技能的目的不同，现实世界中越来越多的入侵行为更加明显地是出于经济、政治或者军事利益和目的的驱动。所以，对这类日益猖獗的入侵行为的监察和防护已成为各种机构（无论是商业机构还是政府机构）的一个迫切要求。

现有的安全机制可通过访问控制（例如口令），来保护计算机和网络不被非法攻击和未经授权者使用。然而，如果这些访问措施被泄漏或着被绕过，则一个滥用权利者将可能获得未经授权的访问，从而导致被攻击系统的巨大损失甚至造成系统崩溃。实际的问题是，不能够在所有情形下都依靠访问控制机制来防范入侵活动或着来自内部的攻击行为。几乎所有的安全系统对内部人员的滥用权力行为都是脆弱的，并且审计记录痕迹几乎是检测授权用户的滥用行为的唯一手段。

入侵检测系统（IDS, Intrusion Detection System）是用来检测对计算机系统和网络系统，或者更广泛意义上的信息系统的非法攻击的安全措施。本书试图对入侵检测技术做一个较为全面的介绍，重点分析几个典型的实际系统，对其中所涉及的基础知识也进行了介绍。特别是对一个实际的入侵检测系统（Snort）的源代码做了较为详尽的分析，力图对广大从事实际安全技术的工程人员有所帮助。

网络以至信息安全技术是一门内容广泛、发展迅速的学科，其发展速度可用日新月异来形容。这就需要工程技术人员不断努力工作去发展和提高它。本书只是在此领域内的一次努力尝试，并且由于篇幅所限，所讨论内容必有不周全之处，希望并欢迎广大读者和技术人员提出批评和建议，可发电子邮件至zj_mkt@263.net。同时，欢迎志同道合者共同研究和探讨。

编　者

目　录

1 入侵检测系统概述

- 入侵检测系统的现状
- 进一步发展的若干方向
- 我国的发展状况

第 1 章 入侵检测系统概述

入侵检测系统（IDS, Intrusion Detection System）是用来检测针对计算机系统和网络系统，或者更广泛意义上的信息系统的非法攻击的系统，因为任何实际的信息系统都不可能是完全安全的，同时，它们也不可能在其整个生命周期或者每次使用中都始终保持在百分之百安全的状态之中。更进一步地说，如果我们加上过多特定的安全限制因素后，这样的系统甚至是不可实现的。因此，需要采用入侵检测系统来监测外界非法入侵者的恶意攻击或试探，以及内部合法用户的超越使用权限的非法行动。

有关入侵检测系统的开创性工作始于 20 世纪 80 年代 Denning 的研究论文，最初是作为常规计算机安全手段的补充措施而提出的一种 IDS 模型。Denning 的模型是建立在主机上（Host-based）的若干审计数据文件的基础上，其实质是一种基于规则（Rule-based）的特征匹配系统，它将系统使用时收集到的审计数据如系统登录、程序运行和文件使用情况等，与事先预设好的目标特征文件进行匹配搜索，从而发现主机可能遭到入侵的痕迹。另一种检测模型是基于非规则检测（Anomaly Detection）的方法，首先根据系统过去长期正常运行中产生的大量审计数据建立一个常规状态的数学模型，之后，将监测过程中收集到的信息计算出若干模型参数，将计算出的模型参数与以前建立的常态模型参数相比较，来判断系统是否偏离了正常的状态，得出是否受到入侵的结论。

随着研究工作的进一步发展，入侵检测系统转向分布式的网络环境下的应用，Heberlein et al 将 Denning 模型扩展到对以太网中的网络流量分析，建立了一个名为网络安全监视器（NSM, Network Security Monitor）的入侵检测系统。更进一步的扩展工作是 DIDS 系统（Distributed Intrusion Detection System, 分布式入侵检测系统），它将基于主机的入侵检测与网络流量的监测功能结合起来，集于一身。目前很多商用的入侵检测系统，都具有分布式体系结构，并且同时将基于规则的检测方法与非规则状态检测结合起来使用。

1.1 入侵检测系统的现状

入侵检测系统的一般系统结构如图 1-1 所示，主要由以下几大部分组成：

- 数据收集装置，收集反映状态信息的审计数据，输入给检测器。
- 检测器，负责分析和检测入侵的任务，并发出警告信号。
- 知识库，提供必要的数据信息支持。
- 控制器，根据警报信号，人工或自动做出反应动作。

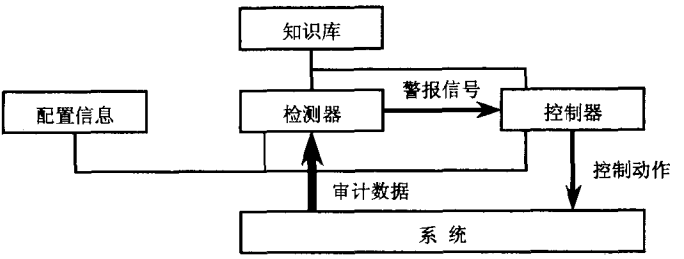


图 1-1 入侵检测系统的结构示意图

从一般意义来说，一个入侵检测系统可以看成一个处理来自所保护系统的各种信息的检测器，所处理的系统信息可分为：长期的信息，如关于攻击的知识库、系统目前的配置信息和描述当前发生事件的审计数据。检测器的作用就是从众多审计数据中剔除无用信息，给出一个用户关心的与安全性相关的分析报告，然后做出决策，发现属于入侵行动的活动。

根据各个部分的实现方法不同，我们可以将入侵检测系统分成很多种类，这里我们把重点放在对检测器类型和获取审计数据来源的讨论上，这是因为考虑到这是一个实用高效入侵检测系统得以实现的两个最关键因素。按照检测器的实现技术，入侵检测系统可分为基于“滥用检测（Misuse Detection）”和“非规则检测(Anomaly Detection)”的两种系统。如果根据系统输入数据的来源，则可分为基于主机审计数据和基于网络流量分析的入侵检测系统。

1.1.1 滥用检测与非规则检测技术

1. 滥用入侵检测

滥用检测系统的应用是建立在对过去各种网络入侵方法和系统缺陷的知识的积累之上，它需要首先建立这样一个数据库，然后在各种收集到的网络活动信息中寻找与数据库项目相关的蛛丝马迹。当符合条件的线索被发现后，它就会触发一个警告，这就是说，任何不符合特定匹配条件的活动将会被认为是合法和可以接受的，尽管其中也许包含着隐蔽的入侵行为。因此，滥用检测系统具备较高的准确性，但是，它的完整性（即检测全部入侵检测行为的能力）则取决于其数据库的及时更新程度。

可以看出，滥用入侵检测系统的优点在于它们具有非常低的虚警率，同时检测的匹配条件可以被很清楚地描述，有利于安全管理人员采取清晰明确的预防保护措施。然而，一个明显的缺陷在于收集所有已知或发现的攻击行为和系统脆弱

性信息的困难性以及及时更新这样一个庞大的数据库需要耗费大量精力和时间。另一个问题是可移植性，因为关于网络攻击的信息决大多数是与主机的操作系统、软件平台和应用类型密切相关，带来的后果是这样的：一个入侵检测系统只能在一个特定的环境下生效。最后，检测内部用户的滥用权限的活动将变得相当困难，因为其中并未利用任何的系统缺陷。

在滥用入侵检测系统中，研究者们提出基于各种类型技术的检测器，如专家系统（Expert System）技术、签名分析（Signature Analysis）技术、Petri 网络分析、状态转移分析（State-transition Analysis）等等。

专家系统技术在各种研究开发模型（Prototypes）中得到广泛应用。通常，专家系统中包含一系列描述攻击行为的规则（Rules），当审计数据事件被转换成为包含能够被专家系统理解的特定警告程度信息的事实（Facts）后，专家系统应用一个推理机（Inference Engine）在事实和规则的基础上推理出最后结论。这里，具体原始的审计数据首先被抽象成为系统能够理解的事实，有利于进一步应用更高层次的各种分析技术。

采用专家系统技术的典型例子有 SRI International 公司开发的入侵检测专家系统（IDES，Intrusion-Detection Expert System）系统，如图 1-2 所示。

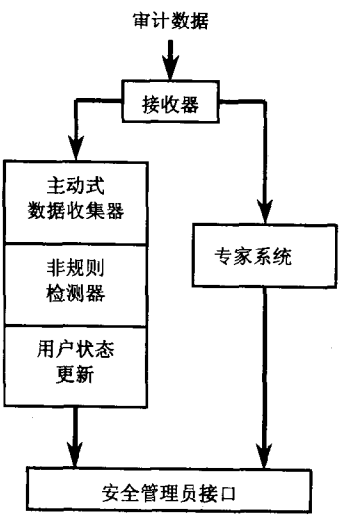


图 1-2 IDES 原型系统的结构

由于处理速度的原因，专家系统技术目前只是在各种研究原型中得到应用，而商业化的软件产品采用了其他效率更高的技术，其中目前应用最广泛的就是签名分析技术。与专家系统比较，相同之处是同样要收集关于网络入侵的各种知识，

不同点是签名分析技术更直接地运用收集到的各种知识，例如入侵行为可以被转化成它们在实施时所产生的一个活动事件的序列或者是某种系统审计文件中的数据样板模型，这一点与反病毒软件的设计思想有类似之处。

2. 非规则入侵检测

非规则入侵检测技术是建立在如下假设基础上的，即任何一种入侵行为都能由于其偏离正常或者所期望的系统和用户的活动规律而被检测出来。描述正常或者合法活动的模型是从通过各种渠道收集到的对过去大量历史活动资料的分析中得到的，入侵检测器就是将它与当前的活动情况进行对比，如果发现状态偏离了正常的模型，则系统发出警戒信号，这就是说，任何不符合以往活动规律的行为都将被视为入侵行为。因此，非规则入侵系统的检测能力中的完整性很高，但是要保证它具备很高的正确性却很困难。

此类检测技术的优点在于它能够发现任何企图发掘、试探系统最新和未被发现漏洞的尝试，同时在某种程度上，它更少依赖于特定的操作系统环境。另外，对于合法用户超越其权限的违法行为的检测能力大大加强。

较高的虚警率是这种方法的主要缺陷，因为所有的信息系统的正常活动并不一定在学习阶段就被全部了解。另外，系统的活动行为是不断变化的，这就需要不断地在线学习，这将带来两个后果。其一是在此学习阶段，入侵检测系统无法正常工作，或者是额外的虚假警告信号；还有一种可能是，在学习阶段，信息系统正遭受着非法的入侵进攻，使得入侵检测系统的学习结果中包含了入侵行为的信息，这样，系统将无法检测到该种入侵行为。

在非规则入侵检测中，最广泛使用的技术是统计分析（Statistics）。系统或者用户的当前行为通过按一定时间间隔采样并计算出的一系列参数变量来描述，如每个会话进程的登录和退出时间，占用资源时间的长短及其在每个进程中占用CPU、内存、硬盘等资源的多少等。采样的时间间隔从几分钟到一个月，时间长短不等。在最初的模型中，系统计算出所有变量的平均值，然后根据平均偏差检测当前行为是否超过了某一阈值，当然，这样的模型是很简单和粗糙的，无法准确检测。即使将单个用户的变量数值与积累起来的群体变量值来比较，检测能力还是提高很小。目前在几种检测系统中使用了一种更加复杂的模型，检测系统同时计算并比较每个用户的长期和短期活动状态，而状态信息随着用户行为的变化而不断更新。

另一种主要的非规则检测技术是神经网络技术。神经网络技术通过学习已有的输入、输出矢量对集合，进而抽象出其内在的联系，然后得到新的输入、输出的关系，这种技术在理论上能够被应用于在审计数据流中检测入侵行为的痕迹。然而，目前尚无可靠的理论能够说明神经网络是如何理解学习范例中的内在关系

的，所以同样也无法清楚地解释它是如何发现并理解入侵行为的。神经网络技术和统计分析技术的某些相似之处已经被若干实验证明，而使用神经网络技术的优势在于它能够以一种更加简洁的方式来表示各种状态变量之间的非线性关系，同时能够自动地进行学习并更新训练的进程。

1.1.2 基于主机与基于网络的入侵检测

基于主机的入侵检测技术是入侵检测中最早应用的领域，最早的入侵检测工具的应用目标就是一台大型计算机，在其周围连接着若干用户终端。在这种环境中，入侵检测的任务被大大简化，因为外来的影响几乎没有。入侵检测工具分析主机提供的审计信息（进程在主机本地或者另外的机器上运行），然后给出关于怀疑为不安全行为的报告。

随着计算技术的重点由大型机环境向分布式网络计算环境的转移，出现了若干适应网络环境的入侵检测系统的研究模型。最初的应用是使各个基于主机的入侵检测系统能够通过网络相互通信，因为在一个分布式的网络中，用户能够从一台主机跳到另一台，在运动中能够改变自己的身份，并在若干台机器上发起进攻。为了适应这些情况，各主机上的入侵检测系统必须能够与其他同类系统交换信息。这种信息的交换可以发生在不同的层面上，如通过网络交换原始的审计记录数据文件，或者发送经过本地分析得出的警戒信号等等。无论哪种方式，都要付出不同的代价。传送原始审计记录将加重网络的带宽负担，而本地处理这些记录将影响本地工作站的运行效率。

特别是随着因特网的广泛使用，入侵检测系统越来越把重点放在对网络本身的入侵行为上。大量的网络攻击行为（DNS 欺骗、TCP 劫持、端口扫描、拒绝服务攻击等）通过分析主机审计数据是很难被发现的。因此，人们发展了特定的工具软件（如嗅探器 Sniffer）来实时截获网络数据包，并在其中寻找入侵的痕迹。另外，许多针对服务器的传统攻击手段也能够通过解析数据包的载荷，找出可疑的命令来防御。对于许多系统管理员来说，这些工具软件能够在若干关键的网络节点上进行安装，基本上能够覆盖全部网络来对大部分的攻击手段进行防御。

大量混合的入侵检测方法在近年出现，它们同时采用基于主机和基于网络的入侵检测工具。一个较有名的例子是 DIDS（Distributed Intrusion Detection System, 分布式入侵检测系统），它在主机节点上运行 Haystack 软件来检测本地的攻击行为，用 NSM（Network Security Monitor,网络安全监视器）来监视网络入侵行为。而 Haystack 和 NSM 同时向系统控制器（Director）汇报情况，然后进行最后的分析处理。

基于主机和基于网络的入侵检测各有其不同的信息来源。前者的信息来源包

括：

- System Sources（系统信息）。几乎所有的操作系统都提供一组命令，显示关于本机当前激活的进程的状态信息。在 UNIX 环境下，类似的命令有 ps、pstat、vmstat 等。这些命令能够提供关于进程的非常详细的信息，因为它们直接检查的是内核程序（Kernel）的内存信息。
- Accounting（记账），通常指由计算机操作系统以及(或)操作员所执行的特定操作,它记录用户对计算机资源的使用，如处理器占用时间，内存、硬盘或者网络的使用情况等，以便向用户收费。它的优势在于广泛的存在性，如从大型机到工作站以及网络设备等。
- Syslog（系统日志），它是一种由操作系统提供给应用程序的服务，该项服务接收由应用程序发来的一行文本字符串，加上时间戳和运行平台系统的名称信息，然后将它们存档起来。
- C2 Security Audit（C2 级安全审计），它记录所有可能与安全性有关的发生在系统上的事件。它的起源在于美国政府要求其未来采购的计算机系统必须具有 C2 级以上的安全证书（该证书由美国国防部的可信计算机评估标准 TCSEC 来确定）。各个厂商为适应这一要求，在其系统内加入了该项审计特征，如 Sun 公司的 BSM、Shield Packages 以及 AIX。

所有的安全审计都具有相同的基本原理，它们记录在用户空间和可信计算空间（通常指的是操作系统的内核）之间交互执行指令的情况，这是基于这样一个假设即用户的活动不能危害系统本身，而只有在用户在申请使用系统内核服务时，可能危害安全的行为才有可能发生。由于 C2 级安全审计具备许多优点，它已经成为绝大多数基于主机的入侵检测工具的主要审计信息来源，并且它也是目前惟一可靠的收集当前用户活动信息的途径。

基于网络的信息来源有：

- SNMP Information（简单网管信息），简单网管协议的管理信息库（MIB，Management Information Base）是专门存放用于网络管理目的信息的地方，它包含了网络的配置信息（如路由表、地址、名称等）以及大量的性能和记账信息（如用来记录在各个网络接口和各协议层上的网络流量的计数器信息）。SNMP 协议目前有 v1、v2、和 v3 版本，前两个版本由于缺乏内在同一的安全特征，越来越多的入侵检测系统开始利用 v3 版本的 SNMP 的新安全特征作为审计数据来源。
- Network Packets（网络数据包）。网络嗅探器软件 Sniffer 作为入侵者收集和分析信息的工具已经被广泛使用了很久，现在它也被认为是一种分

析网络事件的有效途径。随着集中式计算方式向分布式计算方式的转移，越来越多的计算活动发生在网络上。试想在数据包进入敏感服务器之前，就将其捕获和分析，这可能是监视和保护该服务器的最有效方法。

采用数据包作为信息来源的一个好处体现在对拒绝服务攻击（DoS）的检测上。这种攻击行为绝大部分都是从网上发起，而且必须在网络层次上进行检测，因为基于主机的入侵检测系统无法得到关于此类攻击的主机审计数据。这种方法的另一个优点在于信息来源格式的标准化，信息的获取、格式都同在TCP/IP 协议机制上，有利于跨平台的分析。

网络数据包已经成为近来若干商业化工具和许多研究项目的信息来源方式。但是有关的测试同样显示，采用截获网络包这种方法（至少在目前的实现方法下）同样有其缺点，即一个有经验的入侵者有可能逃脱软件工具的检测。在此领域的研究工作仍在继续进行。

1.1.3 其他的若干问题

其他一些问题还涉及入侵检测系统的性能评测标准、可重用性问题等等，可参考有关文献。

1.2 进一步发展的若干方向

1.2.1 宽带高速网络的实时入侵检测技术

大量高速网络技术如 ATM、千兆以太网、G 比特光纤网等在近年内不断出现，在此背景下的各种宽带接入手段层出不穷，其中很多已经得到了广泛的应用。如何实现高速网络下的实时入侵检测成为一个现实的问题。

这需要考虑两个方面的问题。首先，入侵检测系统的软件结构和算法需要重新设计，以适应高速网络的新环境，重点是提高运行速度和效率。开发设计相应的专用硬件结构，加上配合设计的专用软件是解决这方面问题的一个途径。另一个问题是，随着高速网络技术的不断进步和成熟，新的高速网络协议的设计也成为未来的一个发展趋势，如对 TCP/IP 协议的重新设计等，所以，现有的入侵检测系统如何适应和利用未来新的网络协议结构是一个全新的问题。

1.2.2 大规模分布式入侵检测

传统的集中式入侵检测的基本模型，是在网络的不同网址放置多个传感器用来收集当前网络状态信息，然后这些信息被传送到中央控制台进行处理和分析。

更进一步的是，这些传感器具有某种主动性，能够接收中央控制台的某些命令和下载某些识别模板等。

这样的集中式模型具有几个明显的缺陷。首先，面对在大规模、异质网络基础上发起的复杂攻击行为，中央控制台的业务负荷将会达到不可承受的地步，以至于无法具有足够能力来处理来自四面八方的消息事件。这种情况会造成对许多重大消息事件的遗漏，大大增加漏警概率。其次，由于网络传输的延时问题（这在大规模异质网络中尤其如此），到达中央控制台的数据包中的事件消息只是反映了它刚被生成时的环境状态，不能反映随着时间的推移可能已经改变的当前状态。这将使得基于过时信息做出的判断的可信度大大降低，同时也使得返回去确认相关信息来源的行为变得非常困难。异质网络环境所带来的平台差异性也将给集中式模型带来困难。因为每一种攻击行为在不同的平台操作环境中都出现不同类型的模式特征，而且已知的攻击方法数目非常多，这样，在集中式模式的系统中，想要进行较为完全的攻击模式的匹配就已经非常困难，更何况要面对不断出现的新的攻击手段所带来的更多新的攻击模式的匹配问题。

面对诸多难题，很多新的思路已经出现。其中一种就是攻击策略分析（Attack Strategy Analysis）的方法。它采用了分布式智能代理的结构方式，由几个中央智能代理和大量分布的本地代理组成，其中本地代理负责处理本地事件，而中央代理负责整体的分析工作。与集中式模型不同的是，它强调的是通过全体智能代理的协同工作来分析入侵者的攻击策略，中央代理扮演的是协调者和全局分析员的角色，但绝不是惟一的事件处理者，其地位有点类似于战场上的元帅，根据对全局形势的判断，指挥部下开展行动。这种方法有其明显的优点，但同时又带来了其他的一些问题，如大量代理的组织和协作问题、它们之间的通信以及处理能力和分析任务的分配等等。

1.2.3 入侵检测的数据融合技术

目前的入侵检测系统还存在若干缺陷。首先，现有的实时 IDS 系统在技术上还不具备足以检测到由受到良好训练的黑客发起的复杂、隐蔽的攻击行为的能力。其次，检测的虚假警告问题也是一个令许多网络管理员头疼的事情。最后，来自各种来源的大量泛滥的数据、系统消息等常常没有及时得到很好的处理，非但无助于解决问题，反而浪费和降低了 IDS 系统的处理能力和检测性能。

为解决上述问题，多传感器数据融合技术提供了一条重要的技术途径。它能够把从多个异质分布式传感器处得到的各种数据和信息综合成为一个统一的处理进程，来评估整个网络环境的安全性能。数据融合入侵检测系统的输入可以是从网络嗅探器处得到的各种网络数据包、系统日志文件、SNMP 信息、用户资料信息、系统消息和操作命令等，系统输出是入侵者的身份估计和位置确定、入侵

者的活动信息、危险性信息、攻击的等级和对整个入侵行为危险程度的评估等。

入侵检测数据融合推理的层次结构如图 1-3 所示。

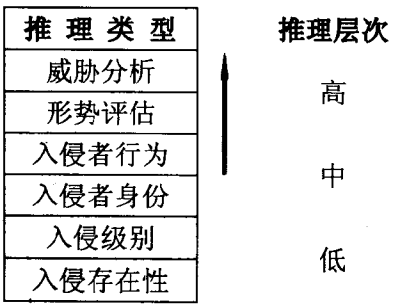


图 1-3 IDS 数据融合推理层次

入侵检测数据融合技术同样面临着若干挑战，例如开发一种通用的结构化“元语言”来描述入侵检测和网络管理的对象，以及对动态网络攻击行为的检测技术，还有将具有强烈数学背景的多传感器数据融合理论应用到实际的 IDS 系统所面临的若干复杂问题等。

1.3 我国的发展状况

我国计算机系统及网络是以国外产品为主，其操作系统的安全性基本上是最低层次的，即使最高的也只是美国标准的 C 级。同时，软硬件系统中也难免存在各种潜在威胁和安全“陷阱”（迄今已经发现的 PIII 芯片、WIN98 的安全问题及 Windows 操作系统的安全“后门”就证明了这一事实）。因此，利用这些设备建立的网络系统，即使采用了加密、防火墙等安全技术措施，其安全水平也不可能有根本性的提高。

在我国计算机网络的安全现状下，基于防火墙、加密技术的安全防护固然重要，但是，要根本改善网络的安全现状，必须发展网络入侵检测技术。如果说加密和防火墙技术是静态的防御措施的话，那么入侵检测技术就是一种随着当前网络状态变化而动态响应的安全防御手段，所以入侵检测技术已经成为当前网络安全技术领域内的一个研究热点。其本身的快速发展和极具潜力的发展前景需要有更多的研究和工程技术人员投身其中，在基础技术原理的研究和项目应用技术开发等多个层面同时开展工作，才有可能做出具有领先水平的高质量入侵检测系统。