第1章 绪 论

20世纪末，一场以计算机技术、网络技术为代表的技术风暴席卷整个世界，这场技术风暴一直持续到21世纪，推动了整个世界的社会信息化进程。电子商务、电子政务先后出现并得到普及，人类正在打造一个数字化的信息世界，而计算机网络的建设是这个世界的核心。可以说计算机网络是信息时代的重要标志，网络的基本功能包括资源共享、通信和控制，它满足了人们长久以来对信息资源的渴望，人们对网络的依赖也变得越来越强。

社会信息化极大改善了人们工作及生活的品质，同时也带来了不容忽视的信息安全问题。并且，随着社会信息化程度的深入，信息安全问题愈发严重，各种针对网络的攻击行为层出不穷，严重影响了网络的应用，制约了网络的发展。

本章作为全书的导引部分，将重点介绍信息安全的相关知识和概念，入侵检测技术的发展历史、研究内容以及入侵检测技术的分类。

1.1 信息安全概述

1.1.1 信息安全基本概念

信息安全是一个涉及计算机技术、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。安全工作的目的就是为了在与信息安全相关的法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，维护计算机信息安全。

1. 信息

信息是个很大的概念，它泛指人类社会传播的一切内容[1]。然而，在信

息安全领域，信息主要是指那些在网络中传播、在计算机中处理的数字化的内容，也就是数字媒体。网络中信息的形态一般有五种：数据、文本、声音、图像和视频[2]。这五种形态共同构成了现在网络上丰富多彩的数字媒体（也称新媒体）。

不同形态的信息在本质上都是数字化的内容，以二进制的格式存储在存储介质上（如磁盘、磁带、光盘），但是内容的编码方式不同，要用相应的软件才能打开。软件打开信息的过程其实就是对编码后的信息内容进行解码，然后显示出来的过程。

信息是有生命周期的，信息生命周期是指信息被收集、存储、加工和维护使用的整个过程，贯穿其从产生到消亡的始终，从管理的角度而言，一般包括产生、传播、使用、维护、归宿（存档或删除）五个阶段，这五个阶段的关系如图 1.1 所示：

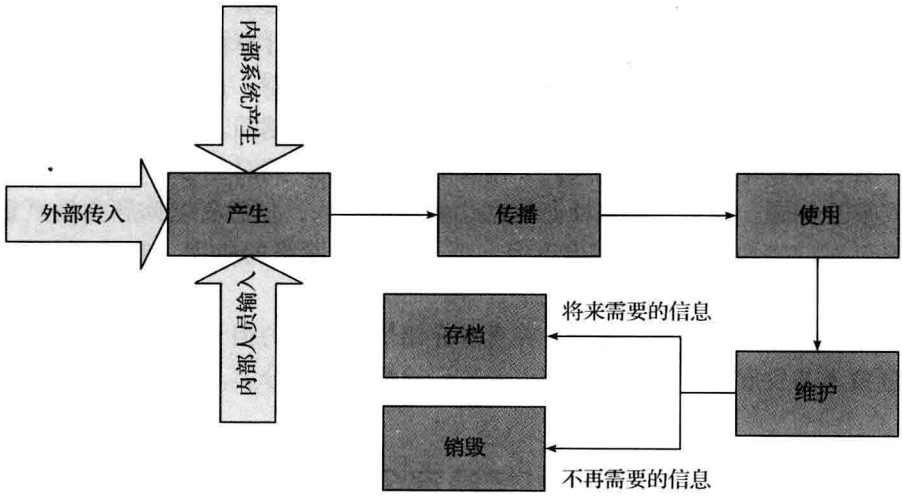

图 1.1　信息生命周期中五个阶段的关系示意图

根据图 1.1，信息产生的来源有三个，分别是外部传入的信息、内部人员输入的信息以及内部系统自动产生的信息。信息一旦产生，就可以进行传播、使用和维护。最后，信息的归宿有两种，有用的信息将被存档，而无用的信息将被销毁。

信息在其生命周期的各个阶段都会遇到安全问题。如，在信息产生阶段，产生信息的源的身份可能存在问题，需要通过身份认证来证实其来源的真实性；在信息传播阶段，信息可能遭受拦截、篡改、伪造和窃听；在信息的使用阶段，信息可能被篡改，遭受非法使用。因此，信息安全需要考虑信息生命周

期的各个阶段。

2. 信息系统

信息系统是由计算机硬件、网络和通讯设备、计算机软件、信息资源、信息用户和规章制度组成的以处理信息流为目的的人机一体化系统[3]。它有五大基本功能：输入、存储、处理、输出和控制[4]。

（1）输入功能：信息系统的输入功能决定于系统所要达到的目的及系统的能力和信息环境的许可。

（2）存储功能：存储功能指的是系统存储各种信息资料和数据的能力。

（3）处理功能：基于数据仓库技术的联机分析处理（OLAP）和数据挖掘（DM）技术。

（4）输出功能：信息系统的各种功能都是为了保证最终实现最佳的输出功能。

（5）控制功能：对构成系统的各种信息处理设备进行控制和管理，对整个信息加工、处理、传输、输出等环节通过各种程序进行控制。

信息系统是一个综合的人机一体化系统，涉及计算机技术、网络技术和数据库技术的应用。根据信息系统的应用特点，目前有数据处理系统（Data Processing System，DPS）、管理信息系统（Management Information System，MIS）、决策支持系统（Decision Sustainment System，DSS）、专家系统（Expert System，ES）和虚拟办公系统（Office Automation，OA）五种类型的信息系统。

3. 信息安全

信息安全是保护整个信息系统（包括其中的信息）的安全，使其不受偶然的或恶意的原因而遭受破坏、更改、泄露，保证系统连续可靠地运行，信息服务不中断，最终实现业务的连续性。

信息安全的最终目标是通过各种技术与管理手段实现信息系统的保密性、完整性、可用性、可靠性、可控性和不可抵赖性[2,5]。

（1）保密性：是指保护信息的隐秘性，防止信息泄露、信息内容被非法获取。保密性可通过信息加密、身份认证、访问控制、安全通信协议等技术来实现。

（2）完整性：是指保障信息不会在未经授权的情况下被更改，强调的是信息在存储和传输过程中的一致性。完整性可通过散列算法来实现，如 MD5、SHA1 算法等。

（3）可用性：是指用户能够不受影响地使用信息，即信息是可以使用的。

（4）可靠性：是指信息的内容是真实可靠的。

（5）可控性：是指信息在整个生命周期内都可被其合法拥有者进行安全的控制。

（6）不可抵赖性：是保障用户在事后无法否认其对信息所实施的行为，如生成、修改、签发、接收和删除等。

无论入侵行为多么复杂多样，其最终目标都是要破坏以上六个特性中的一个或多个。

4. 网络安全

相对于信息安全，网络安全是一个较小的范畴，它是信息安全范畴中的一部分。如果将信息安全限定在计算机网络范畴，就是网络安全了。网络安全就是防范计算机网络硬件、软件、数据偶然或蓄意被破坏、篡改、窃听、假冒、泄露、非法访问并保护网络系统持续有效工作的措施总和。网络安全的保护范围及其与信息安全的关系如图 1.2 所示：

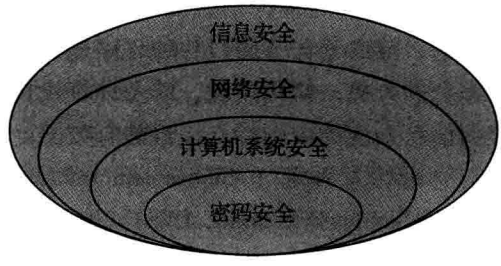

图 1.2　网络安全的保护范围

根据图 1.2，信息安全的范畴最大，其保护的范围包括所有信息资源；网络安全保护的范围是网络信息资源；网络是由计算机构成，所以在网络安全下面还有计算机系统安全，用来保护计算机系统硬件、软件、文件和数据；最后，密码安全是信息安全、网络安全和计算机系统安全的基础和核心，信息的保密性、完整性、可用性、可靠性、可控性和不可抵赖性都可用密码技术来保护。

1.1.2　信息安全体系结构

信息安全的总需求是物理安全、网络安全、信息内容安全、应用系统安全的总和，安全的最终目标是确保信息的保密性、完整性、可用性、可靠性、可控性和不可抵赖性，以及保障信息系统主体（包括用户、团体、社会和国家）对信息资源的控制。

1. 信息安全的保护机制

信息安全的保护机制包括电磁辐射、环境安全、计算机技术、网络技术等技术因素，还包括信息安全管理（含系统安全管理、安全服务管理和安全机制管理）、法律和心理因素等机制。因此，信息安全保护是一个多重的保护机制，如图 1.3 所示：

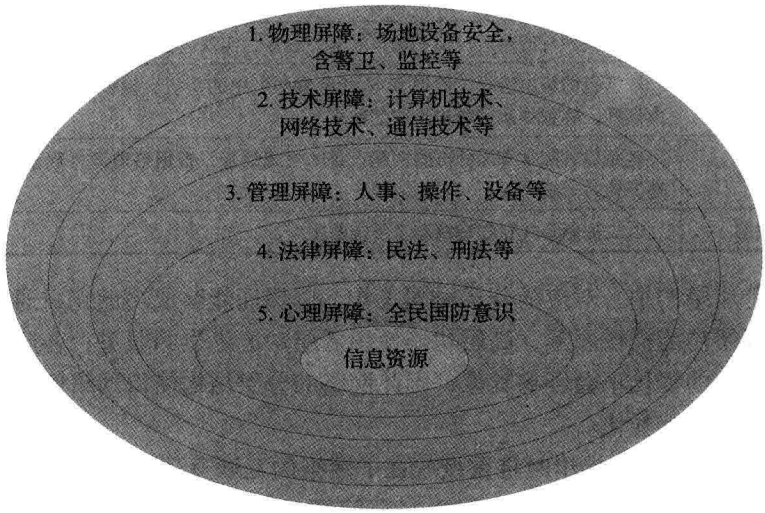

图 1.3 信息安全的保护机制

从图 1.3 可以看到，信息安全的保护是全方位的，涉及五个层次，分别是物理、技术、管理、法律和心理。第一层是物理屏障，包括场地设备安全，含警卫、监控等；第二层是技术屏障，主要是计算机技术、网络技术和通信技术等；第三层是管理屏障，涉及人事、操作和设备的管理；第四层是法律屏障，包括民法、刑法等；第五层是心理屏障，加强全民安全意识，让信息安全的观念深入人心。以上五层共同构成了信息安全的保护机制，而入侵检测技术属于第二层技术屏障的范畴。

2. OSI 安全模型

信息安全涵盖的范围较大，现在是网络时代，作为信息安全的子集，网络安全成为人们关注的重点。计算机网络是在 OSI 参考模型的基础上构建的，OSI 参考模型采用分层的体系结构，将复杂的网络功能分解到各个层来实现，降低了网络系统设计的复杂度。

OSI 参考模型将网络功能分解到七个层，从底层硬件提供的服务开始，每一层都建立在其下一层的基础上并负责完成被明确定义的该层功能，同时向它

的上一层提供特定的服务。OSI 参考模型每层功能如表 1.1 所示[6,7]：

表 1.1　OSI 参考模型

OSI 参考模型	功　能
应用层	面向实际的网络应用，如文件传输、电子邮件、文件服务、虚拟终端
表示层	数据的表示，如数据格式化、代码转换、数据加密
会话层	解除或建立与别的节点的联系
传输层	提供端到端的接口，使用端口号标识进程，实现进程之间信息的可达
网络层	数据包的路由选择，使用 IP 地址定位网络中的主机，根据目的 IP 地址进行路由选择，将数据从信源机发往信宿机
数据链路层	链路层首部含有通信链路两端设备的物理地址，根据该地址将数据从链路的一端发往另一端
物理层	以二进制形式在物理链路上传输数据

在分层结构中，对应的分层协同工作，以保证能够成功地完成通信；低层功能为高层功能提供服务，高层功能使用低层功能提供的服务；各层间相互独立，某一层的变化不会影响其他，因此网络的分层结构使得网络便于实现和维护，容易实现标准化。

OSI 参考模型在提出时将重点放在了网络的互联互通上，没有考虑网络的安全问题，随着网络的发展，网络安全问题日益凸显，严重影响了网络的使用，为打造安全健康的网络环境，研究人员针对 OSI 参考模型各层的功能不同，提出了 OSI 安全模型，如图 1.4 所示：

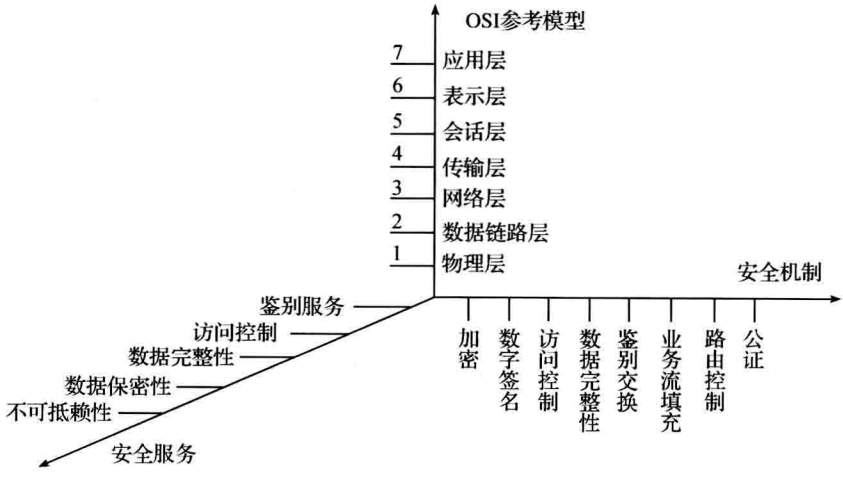

图 1.4　OSI 安全模型

OSI 安全模型是在 ISO 7498-2 中规定的，它描述了 OSI 参考模型与安全服务、完全机制之间的关系。对于 OSI 参考模型的各个层，有对应的安全机制来提供相应的安全服务。

3. 信息安全服务

图 1.4 的 OSI 安全模型规定了开放系统需要提供的五种安全服务：鉴别服务、访问控制、数据保密性、数据完整性和不可抵赖性。

（1）鉴别服务：鉴别服务提供对通信中的对等实体和数据来源的鉴别，鉴别一般由两个过程组成，第一步是识别对象的内容，也就是弄清楚对象是什么；第二步是验证对象的真实性，包括对象身份的真实性或来源的真实性。鉴别服务用来保障通信双方身份的真实可靠，以及传输的数据来源的真实可靠。

（2）访问控制：访问控制主要是根据主体的身份来控制其对客体的访问，从而防止非授权的访问。一般情况下，系统为主体分配了不同的访问控制权限，限制其对某些信息的访问或对某些功能的使用。

（3）数据保密性：数据保密性是保护数据内容，防止信息泄露，从而被未经授权的用户获取，它使得数据内容对非法用户是不可见的。

（4）数据完整性：数据完整性用于保护信息的内容，防止信息被未经授权地修改，在网络传输中，就是要求发送的信息和接收到的信息一致，保障的是信息内容的真实可信。

（5）不可抵赖性：不可抵赖性是防止用户对其所实施的行为进行否认和抵赖。在电子商务盛行的今天，不可抵赖性可以防止交易过程中的欺诈行为，防止交易发生后参与交易的一方对交易行为进行否认。

4. 信息安全机制

安全机制用来提供相应的安全服务，图 1.4 的 OSI 安全模型提出了八种安全机制，这八种安全机制可在 OSI 参考模型的各个层次中工作，以提供相应的安全服务。

（1）加密机制：加密机制主要用于保护信息的保密性，既可对存储的数据加密，又可对传输中的数据进行加密。加密机制可用于 OSI 参考模型的多个协议层中。

（2）数字签名机制：数字签名机制主要用来提供不可抵赖服务，证明用户确实执行过某个行为。比如可以对文件进行数字签名来证明拥有该文件。数字签名本身必须具有不可伪造和不可抵赖的特点。

（3）访问控制机制：访问控制机制提供访问控制服务，用来限制对信息资源的访问或对某些功能的使用，防止未授权的访问行为。

（4）数据完整性机制：数据完整性机制用来保护数据的完整性，从而保证数据前后的一致性。一般在发送数据的同时，通过散列函数计算数据的散列值，将散列值随着数据一起发送，接收方收到数据后，采用相同的散列函数计算同一数据的散列值，然后比较两个散列值是否相等，从而验证数据的完整性。

（5）鉴别交换机制：可通过密码技术来实现，由发送方提供，而由接收方验证来实现鉴别。在此过程中可通过特定的握手协议来防止鉴别重放攻击。

（6）通信业务填充机制：为防止信息遭受攻击而人为添加到信息中的干扰信息，这能够为防止通信业务分析提供有限的保护。

（7）路由选择控制机制：针对信息传输过程的安全，路由选择控制机制可为信息的传输选择安全的路由通道，或保证敏感数据只在具有适当保护级别的路由上传输。

（8）公证机制：公证机制是一种第三方认证技术，通过第三方机构实现对通信数据的完整性、保密性、真实性的公证。公证服务主要是加密技术和数字签名技术的应用。

5. 信息安全体系框架

信息安全的体系框架如图 1.5 所示，可以看出，完整的信息安全体系框架主要由技术体系、组织机构体系和管理体系共同构成。技术体系又分为技术机制和技术管理两大部分，将物理安全放在了技术机制下运行环境及系统安全技术的范畴；组织机构体系包括机构的建立、岗位的培训及人事制度；管理体系包括法律、制度及培训。

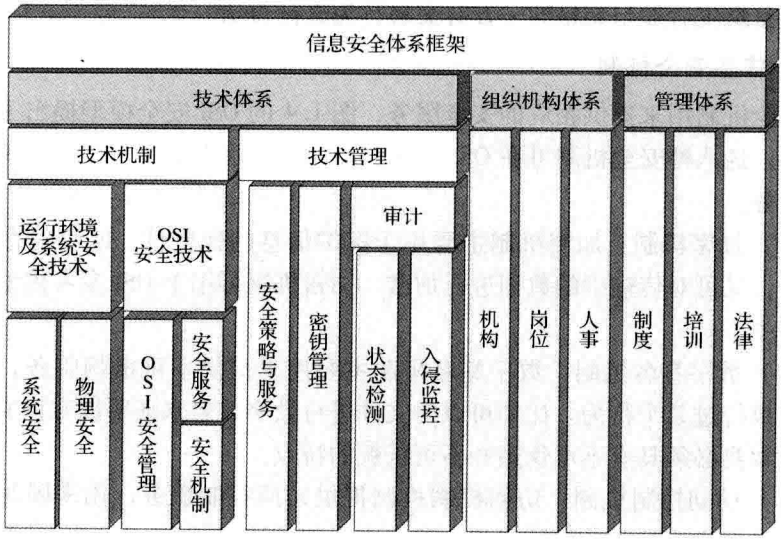

图 1.5　信息安全体系框架

信息安全的体系框架其实反映了信息安全多重保护机制，含有 OSI 安全模型中安全服务和安全机制的内容。

1.2 入侵检测概述

1.2.1 入侵检测发展史

早在 20 世纪 70 年代，计算机及网络的安全问题就摆在了研究者的面前，那时候主要采用审计跟踪技术来检测入侵行为。直到 1980 年 4 月，James P. Anderson 在为美国空军做的一份题为 *Computer Security Threat Monitoring and Surveillance*（《计算机安全威胁监控与监视》）的技术报告中才首次提出了入侵检测的概念。在这份报告中，James P. Anderson 提出了一种对计算机系统风险和威胁的分类方法，将威胁分为外部渗透、内部渗透和不法行为三种，还提出了利用审计跟踪数据监视入侵行为的思想[8]。从此人们开始了入侵检测技术的研究。

1984 年到 1986 年，乔治敦大学的 Dorothy Denning 和 SRI/CSL 的 Peter Neumann 研究出了第一个入侵检测系统模型 IDES[9]，如图 1.6 所示：

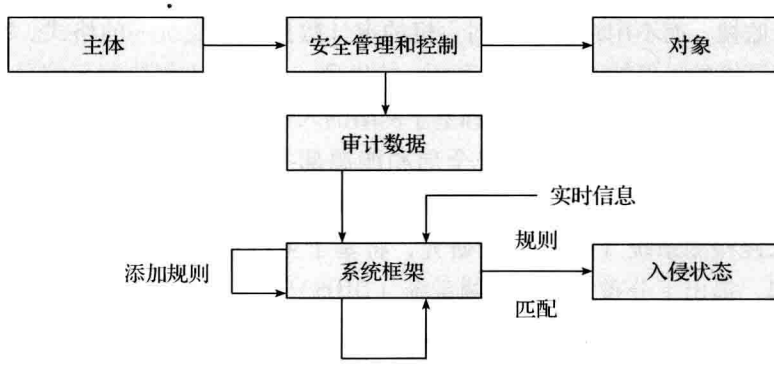

图 1.6 IDES 模型

IDES 模型由六个部分组成：主体、对象、审计记录、轮廓特征、异常记录、活动规则，作为一种通用的入侵检测系统模型，成为入侵检测系统研究的基础模型。此外，IDES 是基于规则的模式匹配系统，采用了两大入侵检测技术之一的误用入侵检测技术。

1988 年，SRI/CSL 的 Teresa Lunt 等人对 IDES 进行了改进[10]，改进的 IDES 增加了异常检测功能和专家系统，被用来构造异常行为的模型并且检测

基于规则的属性，如图 1.7 所示：

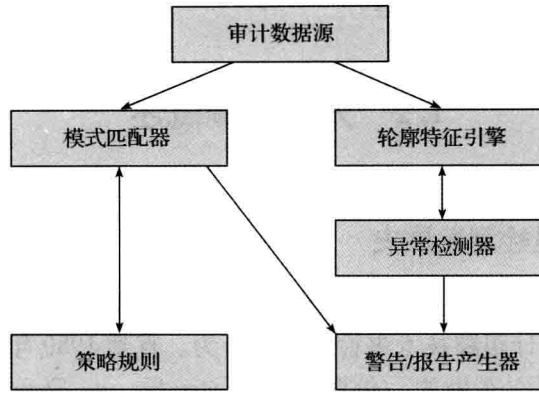

图 1.7　改进的 IDES 模型

改进后的 IDES 模型采用了异常入侵检测技术，至此，入侵检测技术两大阵营都登上了历史的舞台，分别是：误用入侵检测技术和异常入侵检测技术。

同年，著名的 Morris 蠕虫事件使人们认识到网络安全的重要性，对网络的入侵检测成为研究的重点。

1990 年是入侵检测系统发展史上的一个分水岭，加州大学戴维斯分校的 Heberlein 等人开发了 NSM[11]，第一次将网络数据流作为审计数据。NSM 能够对异构主机进行监视，而不用将来自不同主机的审计数据转换成统一的格式。NSM 标志着基于网络的入侵检测系统（NIDS）的出现。从此，入侵检测系统分为了基于主机的入侵检测系统（HIDS）和基于网络的入侵检测系统两类（NIDS）。

1991 年，美国空军、国家安全局和能源部共同资助空军密码支持中心、劳伦斯利弗摩尔国家实验室、加州大学戴维斯分校、Haystack 实验室，开展对分布式入侵检测系统（DIDS）的研究，将基于主机和基于网络的检测方法集成到一起，提出了分布式入侵检测系统（DIDS）[12, 13]，如图 1.8 所示：

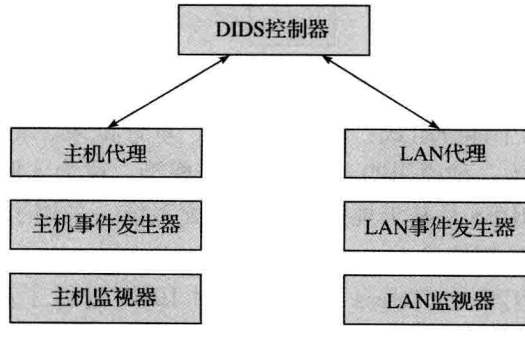

图 1.8　DIDS 模型

DIDS是一个十分重要的产品，主要应用于网络环境。1994年，Mark Crosbie和Gene Spafford提出了自动代理的概念。自动代理大大增强了入侵检测系统的可量测性、可维护性、有效性和容错性。自动代理在体系结构上对大规模的分布式的网络环境下的入侵检测系统的设计给出了好的方案。AAFID是第一个采用自动代理结构的入侵检测系统[14, 15]。

1996年，基于图形的入侵检测系统（GrIDS）的设计与实现解决了入侵检测系统可量测性的问题[16]。这使得检测大规模的自动和协同攻击更加便利。

在体系架构上，入侵检测系统经历了四个阶段：基于主机的入侵检测系统，基于网络的入侵检测系统，分布式入侵检测系统和自动多代理的入侵检测系统。随着网络的发展，入侵检测系统的规模也变得越来越庞大。

除了体系结构上的不断完善，入侵检测系统的核心单元——分类器的构造也得到了很大的发展。分类器的构造与学习科学的发展密切相关。这些学习方法有：统计方法，贝叶斯方法，数据挖掘，遗传算法，人工神经网络（ANN）[17]，神经模糊计算[18]，人类免疫系统[19]，支持向量机（SVM）[20]等。评价分类器性能的标准是准确性，即能够对新的行为进行正确的判断，区分其为正常行为或是入侵行为，这是由分类器的推广能力决定的。推广能力强的分类器能够根据已知的样本对未知的样本进行正确的判断。目前，支持向量机在推广能力方面具有明显的优势，得到了广泛的应用。

从20世纪90年代到现在，入侵检测系统的研发呈现出百家争鸣的繁荣局面，并在智能化和分布式两个方向取得了长足的进展。目前，SRI/CSL、普渡大学、加州大学戴维斯分校、洛斯阿拉莫斯国家实验室、哥伦比亚大学、新墨西哥大学等机构在这些方面的研究代表了当前的最高水平[21-33]。

1.2.2 国内外研究现状

目前国内外关于信息安全的国际会议已有上百个，比较有影响的有IFIP/SEC，ACM CCS，IEEE S&P，ISC，ICICS，CIS，CNCC，NDSS等。ACM，Springer，Elsevier，IEEE等国际知名组织和出版商每年都会刊登大量的相关文章，出版相应的论文集。其中，国际信息处理联合会IFIP召开的世界计算机大会（IFIP/WCC）下面的安全会议（IFIP/SEC）是信息安全领域的国际顶级学术会议，因其引领技术潮流而备受各国信息安全界的关注，而入侵检测一直是IFIP/SEC会的主要议题之一。IFIP/SEC主要由IFIP信息安全专委会TC11负责，第一届IFIP/SEC信息安全国际会议于1983年5月在瑞典斯德哥尔摩召开，每年召开一次，到2009年已召开24届。需要特别提到的是2000年世界计算机大会IFIP/WCC2000在北京举行，江泽民主席在会议开幕式上致词，国

内著名信息安全专家卿斯汉为 IFIP/SEC2000 程序委员会主席，充分说明信息安全问题在中国已经受到了足够的关注和重视，相关的研究已经与国际社会接轨，并得到国际社会的认可。国际信息与通信安全会议 ICICS 是国内信息安全领域的顶级会议，也是国际公认的第一流国际会议，由中科院软件研究所主办。ICICS 为国内外信息安全学者与专家齐聚一堂，探讨国际信息安全前沿技术提供了难得的机会，对促进国内外的学术交流，促进我国信息安全学科的发展做出了重要的贡献。

国外从事信息安全入侵检测研究的主要机构有：乔治敦大学、普渡大学 COAST 实验室、SRI 公司计算机科学实验室（SRI/CLS）、Haystack 实验室、加州大学戴维斯分校、加州大学圣塔芭芭拉分校、洛斯阿拉莫斯国家实验室、哥伦比亚大学、新墨西哥大学等。其中，SRI/CSL、普渡大学、加州大学戴维斯分校、洛斯阿拉莫斯国家实验室、哥伦比亚大学、新墨西哥大学等机构在这些方面的研究代表了当前的最高水平。国内从事信息安全入侵检测研究的主要机构有：中科院、国防科技大学、哈尔滨工业大学、上海交通大学、北京邮电大学等。近年来，以信息安全专家卿斯汉、方滨兴、冯登国、李建华、周仲义、陈恭亮、唐正军为代表的众多国内信息安全研究人员在入侵检测领域取得了丰硕的研究成果，发表了大量的文献和专著[34-71]。卿斯汉等人定期撰写介绍入侵检测研究现状的文章[72,73]，发表在国内权威期刊上，这对于国内信息安全研究人员了解相关领域的研究动态起了很好的帮助作用。

近几年，随着人们对信息安全的认识不断提升，信息安全问题越来越引起人们的重视，入侵检测系统的市场更是飞速发展，许多公司投入到这一领域，推出了自己的产品。国外的企业及其产品有：Sourcefire 公司（现被 Barracuda Networks INC 收购）的 Snort、ISS（Internet Security System）公司的 RealSecure、Cisco 公司的 Secure IDS（前身为 NetRanger）、Axent Technologies 公司（现被 Symantec 收购）的 Netprowler/Intruder Alert、CA 公司的 SessionWall-3/eTrust Intrusion Detection、NFR 公司的 NID，NAI 公司的 CyberCop Monitor 等。国内在入侵检测研究方面虽然起步较晚，但发展很快，目前在公安部取得销售许可证的安全厂商已有 30 余家，主要的企业及其产品有：启明星辰（VenusTech）的天阗、北方计算中心的 NIDS detector、远东科技的黑客煞星、金诺网安的 KIDS、绿盟的冰之眼 IDS 等。

1.2.3 入侵检测的研究内容

经过二十多年的研究与发展，入侵检测已经从最初简单的基于审计信息的单机检测模式，发展到以网络为平台，研究内容丰富，涉及领域广泛的一门综

合性学科。入侵检测各领域研究内容和现状如下：

1. 体系结构研究

入侵检测系统体系结构研究的是系统各功能部件以及部件之间联系的内容。

1984 年至 1986 年，乔治敦大学的 Dorothy Denning 与 SRI/CLS 实验室的 Peter Neumann 合作研究出了一种实时入侵检测系统模型——入侵检测专家系统（Intrusion Detection Expert System，IDES）[9]，该模型为构建入侵检测系统提供了一种通用的框架。1988 年，SRI/CLS 的 Teresa Lunt 等人对 IDES 进行了改进[10]，改进的 IDES 增加了异常检测功能和专家系统，被用来构造异常行为的模型并且检测基于规则的属性。1990 年，加州大学戴维斯分校的 Heberlein 等人开发了 NSM[11]，第一次将网络数据流作为审计数据。NSM 能够对异构主机进行监视，而不用将来自不同主机的审计数据转换成统一的格式。NSM 标志着基于网络的入侵检测系统的出现。1991 年，Haystack 实验室和加州大学戴维斯分校的 Heberlein 等人又合作开发了分布式入侵检测系统 DIDS（Distributed Intrusion Detection System）[12,13]，该系统结合了基于主机和基于网络的检测方法，由多个功能构件组成，各功能构件分散在网络中，分工协作，共同实现入侵检测，能够适用于大型的网络。1994 年，普渡大学 COAST 实验室的 Spafford 等人提出了自治代理（Agent）的概念，设计并实现了采用自治代理结构的入侵检测系统 AAFID[14,15]，又称为主体型入侵检测系统（Agent-Based IDS）。自治代理大大增强了入侵检测系统的可量测性、可维护性、有效性和容错性，在体系结构上对大规模分布式的网络环境下的入侵检测系统的设计给出了好的方案。

总体上，随着网络系统的复杂化、大型化，以及入侵行为的协作性加强，入侵检测系统的体系结构由集中式向分布式发展，经历了三个发展阶段：基于主机的入侵检测系统、基于网络的入侵检测系统和分布式入侵检测系统。其中主机型（Host-Based）和网络型（Network-Based）是集中式的入侵检测系统。分布式入侵检测系统中的主体型入侵检测系统，在体系结构上具有很好的可扩展性、可维护性、可靠性和稳定性，更适合于时下大规模、高速且复杂的网络环境，是当前研究的重点[14,15,21,34,49,74-80]。

2. 攻击模型研究

攻击模型的建立对于了解网络攻击原理，分析网络入侵过程，评估网络安全程度有着重要的意义，对于入侵检测系统的部署有着重要的指导作用。

攻击模型的建模方法主要有四种，分别是攻击树[81-87]、攻击网[88-91]、状

态转移图[92-93]和攻击图[94-103]。其中攻击图的建模方法最为有效，也是目前研究的重点。早期，攻击图由 Red Teams 通过对系统的脆弱性分析，手动生成，当网络规模较大时，这种方式效率很低。目前，网络攻击图自动生成的研究主要有两种方法：基于模型检测技术的方法[94,95,104,106]和基于图论的方法[98,107-110]。

2001 年，乔治梅森大学（GMU）的 Ramakrishnan 和 Ritchey 采用了模型检测方法来自动地寻找攻击路径[94,105]，但是由于当时采用的模型检测工具 SMV 在目标状态不满足指定的属性时，只能产生一条攻击路径，无法生成完整的攻击图，因此这种方法效率仍然较低。2002～2004 年，卡耐基梅隆大学（CMU）的 Sheyner、Haines 等人对 SMV 做了改进，开发了新的模型检测工具 NuSMV[111]，该工具弥补了 SMV 的不足，当属性不满足时，可以给出所有的反例，形成一个完整的网络攻击图[95,106]。模型检测方法存在的主要问题是系统状态空间过大，需要占用大量的存储空间，并且无法对个别行为进行优化执行，严重影响了攻击图生成及分析的效率。因此人们对模型检测做了改进，提出了符号模型检测技术[112]，在模型检测的基础上用二分决策图（Binary Decision Diagram，BDD）来隐含表示状态空间和转换关系，有效压缩了状态空间的大小，节省了存储空间，提高了效率。

图论的方法也被广泛应用于攻击图的自动生成过程中，较早提出从图论角度对网络安全进行量化分析的是 Ortalo、Deswarte 和 Dacier 等人[113,114]，但其模型对网络安全的分析过于理想化，研究力度不够深入。2003 年，Noel、Jajodia 和 O'Berry 等人提出了渗透依赖图（Exploit Dependency Graphs）的概念[115]，较好地表示了攻击者利用多个脆弱性的多阶段入侵过程。2005 年，Li 对其做了归纳和改进，提出了渗透图的概念[116]，提高了对多阶段入侵过程的表述能力。国内，中国科学技术大学的汪渊等人对基于图论的网络安全分析方法做了研究，提出了对网络安全脆弱性的威胁程度进行定量分析的层次分析模型和指标体系，采用图论的方法对各种安全脆弱性信息进行关联分析，取得了好的成果[110]。国防科技大学的张维明等人提出了一种基于渗透图模型的网络安全分析方法 NEG-NSAM，通过对网络系统参数进行抽象以及对系统脆弱性进行关联分析，构造了网络渗透图模型，从而分析可能入侵安全目标的渗透路径[117]。

模型检测方法和图论方法都能自动地生成网络攻击图，但是对于大规模的网络系统，都存在“状态爆炸”的可能，目前攻击图建模研究的重点是对这两种方法进行改进，从而降低状态空间的大小，提高攻击图的生成效率。

3. 特征提取方法研究

数据源是入侵检测系统的重要模块，为入侵检测提供原始数据，面对网络系统中大量的数据信息，有效的特征提取对于入侵检测的检测率、可靠性及实时性都有着重要的影响。

网络系统中的数据源有两种：一种是主机系统中的审计数据、安全日志、行为记录等信息，一种是网络协议数据包。特征提取的目的就是对这些原始数据进行分析，提取攻击特征，通过适当的编码将其加入入侵模式库。一个特征应该是一个数据独有的特性，提取出来的特征应该能够准确、完整地描述该数据或行为，从而为判断入侵提供依据。

提取入侵行为的特征，就是对入侵行为进行形式化的描述，对其进行准确的分类。目前，网络攻击分类方法主要有四种[118]：基于经验术语的分类方法[119-121]，基于单一属性的分类方法[122-127]，基于多属性的分类方法[128-130]，基于应用的分类方法[131-137]。其中基于多属性的攻击分类方法将攻击看成是一个动态的过程，并将其分解成相互关联的多个独立的阶段，再对每个阶段的属性进行独立的描述，具有很好的扩展性，能够全面地、准确地表述攻击过程，得到了广泛的研究和应用。

近几年，基于主成分分析（Principal Component Analysis，PCA）和独立成分分析（Independent Component Analysis，ICA）的特征提取方法成为研究的热点[138-146]。PCA 技术可以将数据从高维数据空间变换到低维特征空间，能够保留属性中那些最重要的属性，从而更精确地描述入侵行为。ICA 也是一种用于数据特征提取的线性变换技术，与 PCA 的主要区别是：PCA 分析仅利用数据的二阶统计信息，所得的数据特征彼此正交；而 ICA 分析利用了数据的高阶统计信息，强调的是数据特征之间的独立性。

4. 模式匹配算法研究

模式匹配主要指字符串的模式匹配，就是在文本中搜索给定的字符串，被广泛地应用于病毒扫描、入侵检测及信息搜索中。模式匹配算法分为单模式匹配算法和多模式匹配算法。单模式匹配算法一次只能在文本中对一个模式串进行匹配；多模式匹配算法一次可以同时对多个模式串进行匹配，在效率上远远大于单模式匹配算法。

单模式匹配算法主要有 BF 算法[147,148]、KMP 算法[149-151]、BM 算法[152-154]、RK 算法[155]、BMH 算法[156,157]、QS 算法[158-160]等。其中 KMP 算法、BM 算法以及 RK 算法比较有创新性，而 BMH 算法和 QS 算法则是对 BM 算法的一种改进。KMP 算法提出一种对模式串中已匹配的子字符串的复用方法，通过对模式串

的预处理，在进行模式匹配之前确定下模式串不同位置可以向后移位的距离，从而提高了模式串在文本中滑动的距离，并且字符串中的每个字符只匹配一次，实现了无回溯匹配。BM 算法开创性地采用了从右向左的匹配方法，同时提出了坏字符原则（Bad Character）和好后缀原则（Good Suffix），进一步提高了模式串匹配时的移动距离。RK 算法则结合哈希（Hash）方法和素数理论来进行模式匹配，取得了较好的匹配效果，并且哈希方法的应用也为多模式匹配算法所借鉴，如著名的 Wu-Manber 算法。

多模式匹配算法能够同时匹配多个模式，比单模式匹配算法具有更大的实用性，是当前研究的重点。目前主要的多模式匹配算法有 AC 算法[161]、AC-BM 算法[162,163]、Wu-Manber 算法[164]。AC 算法是基于有限状态自动机（Finite State Automation，FSA）的，在进行模式匹配之前，首先对模式串进行预处理，生成 FSA 树，即匹配树，然后通过对文本串的一次扫描来完成对所有模式串的匹配。AC 算法支持多模式的匹配，但是必须逐一地查看文本串的每个字符，考虑到 BM 算法能够利用转移表跳过文本中的大段字符的特点，Jason、Staniford 等人提出了 AC-BM 算法，该算法结合了 AC 算法和 BM 算法的特性，利用劣势移动表和优势跳转表来实现跳跃式的并行搜索，从而提高了搜索速度。类似的结合 AC 算法和 BM 算法特性的算法还有 Commentz-Walter 算法[165]、Baeza-Yates 算法[166]等。

Wu-Manber 算法采用了 BM 进行跳跃的思想和 Hash 散列的方法，在实际应用中，是大规模多模式匹配最快的算法之一。Wu-Manber 算法分为两个阶段，预处理阶段和字符串搜索阶段。在预处理阶段，Wu-Manber 算法通过对模式串的分析确定匹配窗口的大小并创建三个数据表：转移表（Shift Table）、前缀表（Prefix Table）、后缀表（Suffix Table）。匹配窗口的大小由最短的模式串的长度决定；转移表根据坏字符原则建立起块字符（一般为两个字符）的转移距离；后缀表通过计算模式串中匹配窗口内后缀块字符的哈希值，将具有相同哈希值的模式串连成单向链表的形式，存储在后缀表中对应哈希值的位置；前缀表与后缀表类似，不过使用的是模式串中的前缀块字符。字符串匹配过程分为三步，首先根据文本串在匹配窗口内的后缀块字符查转移表，确定转移距离，根据转移距离滑动匹配窗口；其次，如果转移距离为“0”，意味着是可能的匹配入口，根据后缀块字符查后缀表，找到所有具有相同后缀块字符的模式串的链表的入口；最后，计算匹配窗口内前缀块字符的哈希值，遍历链表，计算链表中模式串的前缀块字符的哈希值，搜索具有相同前缀哈希值的模式串。

Wu-Manber 算法具有很好的实用性，得到了广泛的研究和应用，目前，针

对 Wu-Manber 算法，人们提出了很多改进方案。有的方法从转移距离的角度出发，通过将 QS 算法中的方法用于 Wu-Manber 算法来提高匹配窗口的转移距离[167-169]；有的方法通过对模式串的分析，利用数学方法通过计算来获得尽可能大的转移距离[168]；有的方法从 Wu-Manber 实现的角度出发，通过简化操作过程来简化 Wu-Manber 算法的实现，提高性能[170,171]；有的方法从 Wu-Manber 算法在实际应用中存在的问题的角度出发，通过特别设计弥补 Wu-Manber 的缺陷，如 Wu-Manber 算法对短模式处理能力很差，需要遍历整个链表等[170,172,173]。这些改进的 Wu-Manber 算法都取得了不错的效果，如著名的网络入侵检测系统 Snort 中就采用了一种改进的 Wu-Manber 算法 MWM（Modified Wu-Manber）[174]，它采用转移表和前缀表来实现模式串的过滤和匹配。

5. 入侵检测方法研究

入侵检测方法可以分为两类：异常入侵检测（Anomaly Detection）和误用入侵检测（Misuse Detection）[72,73,175]。

异常入侵检测利用系统特性的统计信息来构造正常的行为模式，将那些与正常行为模式有差异的行为定性为入侵行为。异常检测依赖于异常模型的建立，模型不同检测方法也不同。异常检测的一个关键在于先验概率的获取，异常检测方法根据现有的样本分析其统计规律，从而对新的入侵行为进行判定，这种方法构造的入侵判定装置也称为分类器，好的分类器能够对行为进行准确的分类，将其划分为入侵行为或正常行为。常用的异常入侵检测方法有：基于特征选择的异常检测方法[176-178]，基于贝叶斯推理的异常检测方法[179]，基于贝叶斯网络的异常检测方法[180]，基于模式预测的异常检测方法[181]，基于贝叶斯聚类的异常检测方法[175]，基于机器学习的异常检测方法[182-184]，基于数据挖掘的异常检测方法[185-189]，基于应用模式的异常检测方法[190]，基于文本分类的异常检测方法[191]，基于神经网络的异常检测方法[192]，基于统计的入侵检测方法[179]。

误用入侵检测则是提取已知的入侵行为的特征，构造入侵行为的规则库，如果某个行为与规则库中的任意规则匹配，则该行为为入侵行为。误用入侵检测的前提是对入侵行为的特征提取与编码，建立规则模式库，其检测过程主要是进行模式匹配。入侵特征描述了网络攻击的特征、条件、排列和关系等，其构造方式很多，相应的误用入侵检测方法也多种多样，常用的误用检测方法有：基于条件概率的误用检测方法[175]，基于状态迁移分析的误用检测方法[193,194]，基于键盘监控的误用检测方法[175]，基于规则的误用检测方法[195]，基于专家系统的误用检测方法[192]，基于模型推理的误用检测方法[192]，基于