普通高等教育“十一五”国家级规划教材
软件工程专业核心课程系列教材

计算机网络安全

（第二版）

姚永雷 马利 主编

- 教育部高等学校软件工程专业教学指导分委员会推荐教材
- 根据教育部“软件工程课程体系研究”项目成果《中国软件工程学科教程》及专业规范组织编写
- 与最新ACM和IEEE-CCSE同步
- 汇集示范性软件工程专业教学成果

清华大学出版社

普通高等教育“十一五”国家级规划教材
软件工程专业核心课程系列教材

计算机网络安全

（第二版）

姚永雷 马利 主编

清华大学出版社
北京

内 容 简 介

本书是《计算机网络安全》(马利主编,清华大学出版社出版)的修订本,在第一版基础上做了大量的修改,既注重介绍网络安全基础理论,又着眼培养读者网络安全技术和实践能力。全书详细讨论了密码学、消息鉴别和数字签名、身份认证技术、Internet 的安全技术、恶意代码及其防杀技术、防火墙、网络攻击与防范技术、虚拟专用网技术等计算机网络安全的相关理论和主流技术。

本书的编写思路是理论与实践相结合,一方面强调基本概念、理论、算法和协议的介绍,另一方面重视技术和实践,力求在实践中深化理论。希望通过本书的介绍,让读者既能掌握完整、系统的计算机网络安全理论,又具备运用主流网络安全技术实现安全网络的设计能力。

本书是一本理想的计算机专业本科生、大专生的计算机网络安全教材,对从事计算机网络安全工作的工程技术人员,也是一本非常好的参考书。

图书在版编目(CIP)数据

计算机网络安全/姚永雷,马利主编. --2 版. --北京:清华大学出版社,2011.12
(软件工程专业核心课程系列教材)
ISBN 978-7-302-27068-3

Ⅰ. ①计… Ⅱ. ①姚… ②马… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 205352 号

责任编辑:魏江江 李玮琪
责任校对:时翠兰
责任印制:杨 艳
出版发行:清华大学出版社 **地 址**:北京清华大学学研大厦 A 座
http://www.tup.com.cn **邮 编**:100084
社 总 机:010-62770175 **邮 购**:010-62786544
投稿与读者服务:010-62776969,c-service@tup.tsinghua.edu.cn
质 量 反 馈:010-62772015,zhiliang@tup.tsinghua.edu.cn
印 装 者:北京国马印刷厂
经 销:全国新华书店
开 本:185×260 **印 张**:15 **字 数**:365 千字
版 次:2011 年 12 月第 2 版 **印 次**:2011 年 12 月第1 次印刷
印 数:1～3000
定 价:25.00 元

产品编号:043534-01

前　言

随着 Internet 在全球的普及和发展，计算机网络成为信息的主要载体之一。计算机网络的全球互联趋势愈来愈明显，其应用范围愈加普及和广泛，应用层次逐步深入。国家发展和社会运转，以及人类的各项活动对计算机网络的依赖性越来越强。计算机网络已经成为人类社会生活不可缺少的组成部分。

与此同时，随着网络规模的不断扩大，网络应用的逐步普及，网络安全问题也愈发突出，受到越来越广泛的关注。计算机和网络系统不断受到侵害，侵害形式日益多样化，侵害手段和技术日趋先进和复杂化，已经严重威胁到网络和信息的安全。一方面，计算机网络提供了丰富的资源以便用户共享；另一方面，资源共享度的提高也增加了网络受威胁和攻击的可能性。事实上，资源共享和网络安全是一对矛盾，随着资源共享的加强，网络安全问题也日益突出。计算机网络的安全已成为当今信息化建设的核心问题之一。

网络安全指网络系统的软件、硬件以及系统中存储和传输的数据受到保护，不因偶然的或者恶意的原因而遭到破坏、更改、泄露，网络系统连续可靠正常地运行，网络服务不中断。从其本质上讲，网络安全就是网络上的信息的安全。为了保证网络上信息的安全，首先需要自主计算机系统的安全；其次需要互联的安全，即连接自主计算机的通信设备、通信链路、网络软件和通信协议的安全；最后需要各种网络服务和应用的安全。从广义来说，凡是涉及网络上信息的机密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全领域的相关理论和技术发展很快。为使读者全面、及时地了解和应用最新的网络安全技术，掌握网络安全的最新实践技能，编者在本书第一版的基础上进行了修订和补充。本次修订的主要思路是：理论与实践相结合，一方面，强调基本概念、理论、算法和协议的介绍，在不影响读者系统建立网络安全理念的基础上，压缩密码学及应用相关内容，删除过时的和不实用的内容；另一方面，重视技术和实践，力求在实践中深化理论，重点增加网络安全攻击技术和网络安全防护实用技术的介绍。重点修订和补充的内容包括：将密码学相关内容合并，消息鉴别和数字签名合并，并压缩相关内容，删除部分过时的技术介绍；将 Internet 安全的相关技术合并，删除 PEM 的介绍；增加网络安全攻击技术的介绍，尤其是目前网络上常见的如分布式拒绝服务攻击等内容；增加入侵检测相关内容，详细讲解入侵检测原理和技术；扩充恶意软件原理和查杀技术的介绍；增加直观的图例，描述复杂的工作原理和操作流程；对课后习题进行了重新编排，等等。

本书以网络面临的常见安全问题以及相应的检测、防护和恢复为主线，系统地介绍了网络安全的基本概念、理论基础、安全技术及其应用。修订后全书共有 9 章，内容包括计算机网络安全概述、密码学、消息鉴别和数字签名、身份认证技术、Internet 的安全技术、恶意代码及其防杀技术、防火墙、网络攻击与防范技术、虚拟专用网技术。希望通过本次修订，能够反映网络安全理论和技术的最新研究和教学进展，用通俗易懂的语言，向读者全面而系统地介绍网络安全相关理论和技术，帮助读者建立完整的网络安全知识体系，掌握网络安全保护

的实际技能。

本书内容完整,安排合理,难度适中;理论联系实际,原理和技术有机结合;逻辑性强,重点突出;文字简明,通俗易懂。本书可作为高等院校计算机及其相关专业的本科生、大专生的教材,也可作为网络管理人员、网络工程技术人员的参考书。

在本书的修订编写和申报"十一五"国家级规划教材的过程中得到了清华大学出版社的大力帮助和支持,在此表示由衷的感谢。

鉴于编者水平有限,书中难免出现错误和不当之处,殷切希望各位读者提出宝贵意见,并恳请各位专家、学者给予批评指正。作者的 E-Mail 为 ylyao@nusit.edu.cn。

本书配套课件可从清华大学出版社网站 http://www.tup.tsinghua.edu.cn 下载。

编 者

2011 年 9 月

目　录

第1章 概 述

在全球信息化的背景下，信息已成为一种重要的战略资源。信息的应用涵盖国防、政治、经济、科技、文化等各个领域，在社会生产和生活中的作用越来越显著。随着 Internet 在全球的发展和普及，计算机网络成为信息的主要载体之一。计算机网络的全球互联趋势愈来愈明显，信息网络技术的应用愈加普及和广泛，应用层次逐步深入，应用范围不断扩展。基于网络的应用层出不穷，国家发展和社会运转，以及人类的各项活动对计算机网络的依赖性越来越强。

但与此同时，网络安全问题也愈发突出，受到越来越广泛的关注。计算机和网络系统不断受到侵害，侵害形式日益多样化，侵害手段和技术日趋先进化和复杂化，令人防不胜防。一方面，计算机网络提供了丰富的资源以便用户共享；另一方面，资源共享度的提高也增加了网络受到威胁和攻击的可能性。事实上，资源共享和网络安全是一对矛盾，随着资源共享的加强，网络安全问题也日益突出。计算机网络的安全已成为当今信息化建设的核心问题之一。

1.1 网络安全面临的挑战

计算机网络，尤其是 Internet，正面临着严重的安全挑战。Internet 是一个全球性的计算机互联网络，在发展初期规模不大，主要用于高等学校和科研院所，并假定用户之间存在信任关系，用户都是善意的。因此，Internet 在初期设计中几乎没有考虑安全方面的问题。但是，随着 Internet 规模逐渐扩大，用户数量不断增长，这种信任模式已经逐步恶化。而且，以电子商务、电子政务为代表的新应用，对网络安全提出了更高的要求。Internet 初期完全开放的设计特性而没有考虑安全的状况已经不能适应当代的需要。

1988 年莫里斯蠕虫病毒的发作使得 Internet 上超过 10%的计算机受害，之后每年重大网络安全事件不断发生。表 1-1 列出了历年的重大网络安全事件。

表 1-1 重大网络安全事件

病毒名称	时 间	影 响
莫里斯(Morris)蠕虫	1988 年	Internet 上超过 10%的计算机受害
梅丽莎(Melissa)	1999 年 5 月	一周内感染超过 100 000 台计算机，造成损失约 15 亿美元
爱虫(I Love You)病毒	2000 年 5 月	造成约 87 亿美元的经济损失
红色代码(Red Code)蠕虫	2001 年 7 月	14 小时内感染了超过 359 000 台计算机
尼姆达(Nimda)蠕虫	2001 年 9 月	高峰时 160 000 台计算机被感染，造成超过 15 亿美元的经济损失
求职信(Klez)	2002 年	造成 7.5 亿美元的经济损失

续表

病毒名称	时间	影响
冲击波(Blaster)	2003 年	造成约 8 亿美元的经济损失
震荡波(Sasser)	2004 年 5 月	破坏能力和造成的影响超过冲击波
极速波(Zobot)蠕虫	2005 年 8 月	具有像"冲击波"和"震荡波"一样的传播能力,而且对反病毒厂商提出了公开挑战
熊猫烧香	2006 年	造成约 80 亿人民币的经济损失
灰鸽子 2007	2005—2007 年	国内后门的集大成者,连续三次位列年度十大病毒
俄格网络战争	2008 年	俄罗斯与格鲁吉亚的冲突中,双方通过互联网相互攻击,开启了信息战争的先河
Conficker 蠕虫	2009 年	感染了超过数以千万计的计算机

近几年,安全攻击的复杂性提高了很多,攻击的自动化程度和攻击速度有了提高,杀伤力也逐步提高;攻击工具的特征更难发现,利用特征进行检测更加困难。例如,红色代码和尼姆达这样的混合型威胁,使用组合的攻击方式来更快地进行传播,造成比单一型病毒更大的危害。2003 年 1 月的蠕虫王,被释放后不到 10 分钟,就感染了 75 000 台计算机。从世界范围看,网络入侵活动日益增多,并超过了恶意代码感染的次数。而且,入侵工具的传播范围越来越广,入侵技术不断提高,对攻击者的知识要求反而降低了。当前,防火墙是人们用来防范入侵者的主要保护措施,但是越来越多的攻击技术可以绕过防火墙,不仅对广大用户,而且对 Internet 基础设施也将形成越来越大的威胁。

自 1994 年我国正式接入 Internet 以来,互联网规模和应用迅猛发展。2009 年,中国互联网络信息中心(China Internet Network Information Center,CNNIC)发布的第 23 次中国互联网发展情况统计报告显示,截至 2008 年 12 月 31 日,中国网民规模达到 2.98 亿人,普及率达到 22.6%,年增长率为 41.9%。然而目前中国互联网安全情况不容乐观,各种网络安全事件层出不穷。综合来看,当前网络安全形势严峻的原因主要有以下三点:

(1) 由于近年来中国互联网持续快速发展,网民数量、宽带用户数量、.cn 域名数量都已经跃居全球第一位,而我国网络安全基础设施建设跟不上互联网发展的步伐,民众的网络安全意识薄弱,中小企业大多采用粗放式的安全管理风格,这三方面的原因直接导致中国互联网安全问题的突出。

(2) 随着技术的不断提高,攻击工具日益专业化、易用化,攻击方法也越来越复杂,越来越隐蔽,防护难度较大。

(3) 电子商务领域不断扩展,与现实中的金融体系日渐融合,为网络世界的虚拟要素附加了实际价值,这些信息系统成为黑客攻击牟利的目标。

根据公安部公共信息网络安全监察局 2008 年病毒疫情调查报告统计,62.7%的被调查单位发生过信息网络安全事件,其中感染计算机病毒、蠕虫和木马程序的情况依然最为突出,其次是网络攻击、端口扫描、垃圾邮件和网页篡改。近年来新增电脑病毒、木马的数量如图 1-1 所示。

攻击者的攻击目标十分明确,针对网站和用户使用不同的攻击手段。对政府网站主要采用篡改网页的攻击形式,对企业则采用有组织的分布式拒绝服务(Distributed Denial of

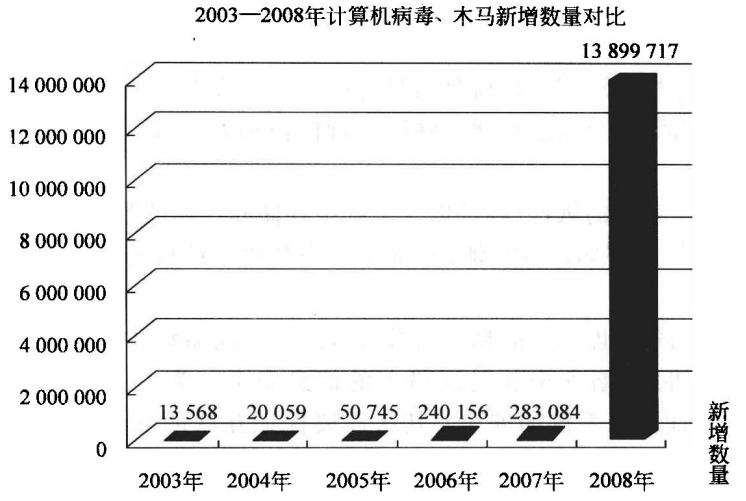

图 1-1　木马、病毒新增数量对比

Service，DDoS）等攻击手段，对个人用户则通过窃取账号、密码等形式盗取用户的个人财产，对金融机构则通过网络钓鱼进行网络仿冒，在线盗取用户身份和密码。

2008 年，病毒木马呈现爆发性增长，制作病毒木马门槛的降低和背后的高利益诱惑都是其主因。2008 年上半年，国家互联网应急中心（National Computer networks Energency Response technical Team/Coordination Center of China，CNCERT//CC）对常见的木马程序活动状况进行了抽样监测，发现我国大陆地区有 302 526 个 IP 地址的主机被植入了木马。包含恶意代码 URL 链接的垃圾邮件数量有所增加，载有恶意软件（不仅仅是恶意代码的链接）的电子邮件数量也在不断增加，针对 DNS 和域名转发服务器的攻击数量有明显增多的趋势。新型网络应用的发展带来了新的安全问题和威胁。

当今社会，互联网已成为重要的国家基础设施，在国民经济建设中发挥着日益重要的作用。随着我国政府信息化基础建设的推进，信息公开程度的提升，网络和信息安全也已成为关系到国家安全、社会稳定的重要因素，社会各界都对网络安全提出了更高的要求。采取有效措施，建设安全、可靠、便捷的网络应用环境，维护国家网络信息安全，成为社会信息化进程中亟待解决的问题。

1.2　网络安全的基本概念

1.2.1　网络安全的定义

计算机网络是利用通信线路把地理位置上分散的计算机和通信设备连接起来，在系统软件和协议的支持下，以实现数据通信和资源共享为目的的复杂计算机系统。网络的基本资源包括硬件资源、软件资源和数据资源等。

常见的安全术语有信息安全、网络安全、信息系统安全、网络信息安全、网络信息系统安全、计算机系统安全、计算机信息系统安全等。这些形形色色的说法，归根结底都是两层意

思,即确保计算机网络环境下信息系统的安全运行,以及信息系统存储、处理和传输的信息受到安全保护。这些术语是殊途同归的关系。由于现代的信息系统大都建立在计算机网络的基础上,因此,计算机网络安全也就是信息系统安全。强调网络安全,主要是由于计算机网络的广泛应用使得大部分信息都通过网络进行传输和处理,从而使得安全问题显得尤为突出。

网络安全指网络系统的软件、硬件以及系统中存储和传输的数据受到保护,不因偶然的或者恶意的原因而遭到破坏、更改、泄漏,确保网络系统连续可靠正常地运行,网络服务不中断。

因此,网络安全同样也包括信息系统安全运行,以及系统中的信息受到安全保护两个方面。从本质上讲,网络安全就是网络上的信息安全。为了保证网络上信息的安全,首先需要保证自主计算机系统的安全;其次需要保证互联的安全,即连接自主计算机的通信设备、通信链路、网络软件和通信协议的安全;最后还需要保证各种网络服务和应用的安全。

网络安全的具体含义会随着利益相关方的变化而变化。

从一般用户(个人、企业等)的角度来说,他们希望涉及个人隐私或商业利益的信息在网络上传输时能够保持机密性、完整性和真实性,避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯自身的利益。

从网络运行者和管理者的角度来说,他们希望对网络信息的访问受到保护和控制,避免出现非法使用、拒绝服务和网络资源非法占用和非法控制等威胁,制止和防御网络黑客的攻击。

从安全保密部门角度来说,希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵,避免机要信息泄漏,避免对社会产生危害,对国家造成巨大损失。

从社会教育和意识形态的角度来讲,网络上不健康的内容,会对社会的稳定和人类的发展造成阻碍,必须对其进行控制。

1.2.2 网络安全的属性

根据网络安全的定义可知,网络安全具有以下几个属性。

(1) 机密性。保证信息与信息系统不被非授权的用户、实体或过程所获取与使用。

(2) 完整性。信息在存储或传输时不被修改、破坏,并且不发生信息包丢失、乱序等。

(3) 可用性。信息与信息系统可被授权实体正常访问的特性,即授权实体在需要时能够存取所需信息。

(4) 可控性。对信息的存储与传播具有完全的控制能力,可以控制信息的流向和行为方式。

(5) 真实性。也就是可靠性,指信息的可用度,包括信息的完整性、准确性和发送人的身份证实等方面,它也是信息安全性的基本要素。

其中,机密性、完整性和可用性通常被认为是网络安全的三个基本属性。

因此,从广义来说,凡是涉及网络上信息的机密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。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、信息论等多种学科的综合性学科。

1.2.3 网络安全层次结构

国际标准化组织(International Organization for Standardization,ISO)提出了开放式系统互连(Open System Interconnection,OSI)参考模型,目的是使之成为计算机互连为网络的标准框架。但是,当前事实上的标准是 TCP/IP 参考模型,Internet 网络体系结构就以 TCP/IP 为核心。基于 TCP/IP 的参考模型将计算机网络体系结构分成四个层次,分别是:网络接口层,对应 OSI 参考模型中的物理层和数据链路层;网际互连层,对应 OSI 参考模型的网络层,主要解决主机到主机的通信问题;传输层,对应 OSI 参考模型的传输层,为应用层实体提供端到端的通信功能;应用层,对应 OSI 参考模型的高层,为用户提供所需要的各种服务。

从网络安全角度来看,参考模型的各层都能够采取一定的安全手段和措施,提供不同的安全服务。但是,单独一个层次无法提供全部的网络安全特性,每个层次都必须提供自己的安全服务,共同维护网络系统中信息的安全。

图 1-2 形象地描述了网络安全的层次。下面具体说明。

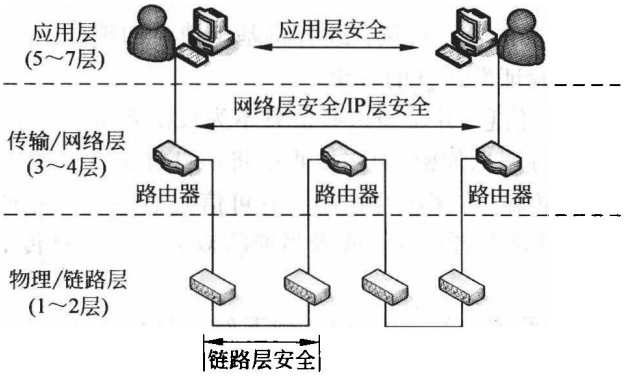

图 1-2 网络安全层次

在物理层,可以在通信线路上采取电磁屏蔽、电磁干扰等技术防止通信系统以电磁(电磁辐射、电磁泄漏)的方式向外界泄漏信息。

在数据链路层,对于点对点的链路,可以采用通信保密机进行加密,信息在离开一台机器进入点对点的链路传输之前可以进行加密,在进入另外一台机器时解密。所有细节全部由底层硬件实现,高层无法察觉。但是这种方案无法适应经过多个路由设备的通信链路,因为在每台路由设备上都要进行加解密的操作,会形成安全隐患。

在网络层,使用防火墙技术处理经过网络边界的信息,确定来自哪些地址的信息可以或者禁止访问哪些目的地址的主机,以保护内部网免受非法用户的访问。

在传输层,可以采用端到端的加密(即进程到进程的加密),以提供信息流动过程的安全性。

在应用层,主要是针对用户身份进行认证,并且可以建立安全的通信信道。

1.2.4 网络安全模型

图 1-3 给出了网络安全模型,消息从通信的一方(发送方)通过 Internet 传送至另一方

(接收方),发送方和接收方是交互的主体,必须共同协调完成消息交换的任务,通过定义Internet上从发送方到接收方的路由以及双方共同使用的通信协议(如TCP/IP)来建立逻辑信息通道。

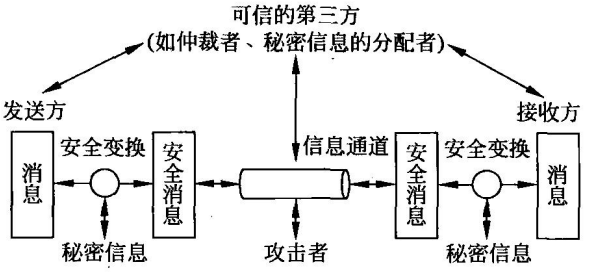

图 1-3 网络安全模型

当需要保护信息传输以保证信息的机密性、完整性、真实性的时候,就会涉及网络安全。一般来说,任何用来保证安全的方法都包含两个因素:

(1) 发送方对信息进行安全相关的转换。例如,对消息进行加密,即对消息进行变换,使得消息在传送过程中对攻击者不可读;或者将基于消息的编码附于消息后共同发送,以使接收方可以基于此编码验证发送方的身份。

(2) 双方共享某些秘密信息,并希望这些信息不为攻击者所知。例如加密密钥,它配合加密算法在消息传输之前将消息加密,而在接收端将消息解密。

为了实现信息的安全传输,许多场合还需要有可信的第三方。例如,第三方负责将秘密信息分配给通信双方,而对攻击者保密;或者当通信双方关于信息传输的真实性发生争执时,由第三方来仲裁。

上述模型说明,设计网络安全系统时,应实现下列4个方面的任务:

(1) 设计一个算法用以实现与安全相关的变换。该算法应是攻击者无法攻破的。

(2) 产生算法所使用的秘密信息。

(3) 设计分发和共享秘密信息的方法,以保证该秘密信息不为攻击者所知。

(4) 设计通信双方使用的协议,该协议利用安全算法和秘密信息提供安全服务。

图1-3所示的网络安全模型虽然是一个通用的模型,但是也有其他与安全有关的情形不完全符合该模型。这些情形下的模型如图1-4所示,该模型可以确保信息系统拒绝非授权的访问。

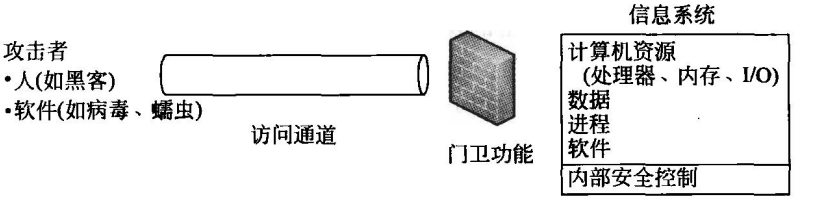

图 1-4 网络访问安全模型

应对非授权访问所需的安全机制分为两大类:第一类称为网闸功能,它包含基于口令的登录过程,该过程只允许授权用户访问;第二类称为内部监控,该程序负责检测和拒绝蠕

虫、病毒以及其他类似的攻击。一旦非法用户或软件获得了访问权，那么由各种内部控制程序组成的第二道防线就监视其活动，分析存储的信息，以便检测非法入侵者。

1.3 OSI安全体系结构

在大规模网络工程建设、管理和网络安全系统的设计与开发过程中，需要从全局的体系结构角度考虑安全问题的整体解决方案，这样才能保证网络安全功能的完备性和一致性，减低安全代价和管理开销。这样一个网络安全体系结构对于网络安全的设计、实现与管理具有重要意义。

为了有效评估一个机构的安全需求，以及对各个安全产品和政策进行评价和选择，负责安全的管理员需要以某种系统的方法来定义对安全的要求，并刻画满足这些要求的措施。国际标准化组织(ISO)于1989年正式公布了ISO 7498-2："信息处理系统-开放系统互连-基本参考模型-第2部分：安全体系结构"，定义了开放系统通信的环境中与安全性有关的通用体系结构元素，作为对OSI基本参考模型的补充。这是一个普遍适用的安全体系结构，对于具体网络的安全体系结构具有指导性意义，其核心内容是保证异构计算机之间远距离交换信息的安全。

OSI安全体系结构主要关注安全攻击、安全机制和安全服务。可以简短地定义如下：

(1) **安全攻击**：任何危及企业信息系统安全的活动。

(2) **安全机制**：用来检测、阻止攻击或从攻击状态恢复到正常状态的过程，或者实现该过程的设备。

(3) **安全服务**：加强数据处理系统和信息传输的安全性的一种处理过程或通信服务。其目的在于利用一种或多种安全机制进行反攻击。

1.3.1 安全攻击

网络攻击是指降级、瓦解、拒绝、摧毁计算机或计算机网络中的信息资源，或者降级、瓦解、拒绝、摧毁计算机或计算机网络本身的行为。在最高层次上，ISO 7498-2将安全攻击分为两类，即被动攻击和主动攻击。被动攻击试图收集、利用系统的信息但不影响系统的正常访问，数据的合法用户对这种活动一般不会觉察到。主动攻击则是攻击者访问他所需信息的故意行为，一般会改变系统资源或影响系统运作。

1. *被动攻击*

被动攻击采取的方法是对传输中的信息进行窃听和监测，主要目标是获得传输的信息。有两种主要的被动攻击方式：信息收集和流量分析。

(1) 信息收集造成传输信息的内容泄漏，如图1-5 (a)所示。电话、电子邮件和传输的文件都可能因含有敏感或秘密的信息而被攻击者所窃取。

(2) 采用流量分析的方法可以判断通信的性质，如图1-5(b)所示。为了防范信息的泄漏，消息在发送之前一般要进行加密，攻击者即使捕获了消息也不能从消息里获得有用的信息。但是，即使用户进行了加密保护，攻击者仍可能获得这些消息模式。攻击者可以决定通信主机的身份和位置，可以观察传输的消息的频率和长度。而这些信息可以用于判断通信