网络与电子商务安全

贾伟 著

国防工业出版社
National Defense Industry Press

网络与电子商务安全

贾伟 著

国防工业出版社
·北京·

内容简介

本书围绕网络与电子商务安全，从基础理论出发，循序渐进地论述了网络与电子商务安全的基本原理、技术应用、评估标准与安全策略。主要内容包括：网络体系结构、网络安全体系结构与安全模型、网络安全技术、电子商务安全技术、电子商务安全协议、安全评估标准与安全策略等。本书可供学习或研究网络与电子商务安全人员参考。

图书在版编目(CIP)数据

网络与电子商务安全/贾伟著.—北京：国防工业出版社，2006.4

ISBN 7-118-04495-4

Ⅰ.网… Ⅱ.贾… Ⅲ.①计算机网络－安全技术 ②电子商务－安全技术 Ⅳ.①TP393.08②F713.36

中国版本图书馆 CIP 数据核字(2006)第 029047 号

※

国防工业出版社出版发行

(北京市海淀区紫竹院南路 23 号 邮政编码 100044)

天利华印刷装订有限公司印刷

新华书店经售

*

开本 710×960 1/16 印张 9¾ 字数 160 千字

2006 年 4 月第 1 版第 1 次印刷 印数 1—4000 册 定价 18.00 元

(本书如有印装错误，我社负责调换)

国防书店：(010)68428422 发行邮购：(010)68414474

发行传真：(010)68411535 发行业务：(010)68472764

前　言

随着计算机在各个领域中的广泛应用和快速发展，网络的普及速度超出了人们的想象，通过网络传输、存储和处理的信息呈几何级数增长，网络已经成为信息社会必不可或缺的基础设施。但是网络安全以及网络应用安全一直以来都是人们密切关注的焦点，由于网络的开放性（尤其是 Internet 网络）、系统的缺陷与漏洞、恶意攻击、计算机病毒、工作人员的误操作以及安全意识淡薄等安全威胁的存在，使得基于网络的各种应用（如电子商务、电子政务等）的安全性受到了严重挑战。因此，加强网络安全管理，提高网络安全性和可用性已经成为关系国家安全、经济发展和社会稳定的一个重大课题，具有重要的战略意义。

本书是笔者结合多年来对网络安全的研究进行编写的。全书共 8 章。第 1 章计算机网络概述，阐述了计算机网络相关的概念、网络分类与功能、网络与电子商务安全等基本内容；第 2 章网络体系结构，在阐述了网络体系结构、OSI 模型及 TCP/IP 模型的基础上，重点对 OSI 参考模型与 TCP/IP 参考模型进行了分析与比较；第 3 章计算机网络安全，重点探讨了网络面临的安全威胁、网络安全内容及安全要素、OSI 网络安全体系结构、TCP/IP 网络安全体系结构及网络安全模型等内容；第 4 章网络安全技术概述，就网络安全技术所涉及的内容进行了较为详细的讨论，主要包括：信息加密技术、密钥管理、网络加密方式、访问控制技术、防火墙技术、安全扫描技术、入侵检测技术及病毒防范技术等；第 5 章电子商务概述，就电子商务相关的概念、功能、类型及方法进行了概述；第 6 章电子商务安全，探讨了电子商务面临的安全威胁、电子商务安全的基本要求及电子商务安全架构，重点对加密、报文鉴别、数字签名、数字时间戳、认证及公钥基础设施 PKI 等电子商务安全技术进行了较为详细的分析阐述；第 7 章电子商务安全协议，主要对电子商务安全所涉及的两个协议——SSL 协议和 SET 协议进行了探讨；第 8 章安全评估标准与安全策略，对国内外典型的安全评估标准进行了阐述，重点对网络安全策略及电子商务的安全策略进行了分析和阐述。

目　录

第 1 章　计算机网络概述

目前人类社会正在从工业经济时代转向知识经济时代，知识经济时代的一个重要特征就是数字化、信息化和全球化，而信息化和全球化实现的核心基础离不开计算机网络。网络已经成为衡量一个国家综合实力的重要标志，它的产生与发展已经对人类社会的政治、经济、文化、科学技术和社会生活产生了深刻影响。

1.1　计算机网络的产生与发展

计算机网络是计算机技术与通信技术相互渗透、密切结合的产物，是人类社会进步和发展的一个显著标志。计算机网络经历了从简单到复杂，从低速到高速，从局部应用到全球范围的发展过程。众所周知，计算机是信息加工和处理的工具，具有速度快、精度高、存储容量大等显著特点。但是单个计算机的处理能力无法满足远距离的信息加工处理和共享要求，而通信技术为远距离的信息传递和共享提供了可能。将二者相互结合，既能够实现信息的加工处理、远程传递和共享，又能够满足提高计算机系统性能、增强可靠性和可用性的要求。因此，随着计算机技术与通信技术的相互融合渗透，就产生并逐渐形成了计算机网络。

计算机技术与通信技术的发展融合，为计算机网络的产生奠定了技术基础，而强烈的社会需求则是推动计算机网络产生与发展的最重要因素。计算机网络的诞生最早可以追溯到 20 世纪 50 年代初，由美国麻省理工学院为美国空军设计的 SAGE 半自动地面防空系统，该系统能够将分布在 17 个防区内的雷达观测站、机场、防空导弹和高炮阵通过通信线路连接，形成一个联机的计算机系统。联机的计算机系统被用作辅助决策，自动引导飞机和导弹进行拦截等。

SAGE 系统通常被认为是计算机技术与通信技术相结合的先驱，然而名声最响、影响最大的现代计算机网络（Internet）的鼻祖——ARPANET 网络则

诞生于 20 世纪 60 年代末。ARPANET 网络也是美苏冷战时期的产物。ARPANET 网络是由美国国防部高级研究计划管理局(ARPA,Advanced Research Projects Agency)于 1969 年创建的。当时研究的目的是为了对付来自苏联的核攻击威胁,在战争中保障计算机系统工作的不间断性。目标是在军事上建立一个分散的指挥系统,一旦战争爆发,若部分指挥点被摧毁,通过网络使信息仍然能够自动转接到正常工作的指挥点上,使指挥系统仍然能够保持正常运转。

ARPANET 网络采用分组交换技术,以电话网作为主干网络,最初只连接了 4 台计算机,两年后接入的计算机达到了 15 台。随后 ARPANET 网络的规模不断扩大,1972 年接入 ARPANET 网络的计算机达到了 40 多台,1983 年达到了 300 多台,网络跨越了整个美洲大陆,连通了美国东西部的许多高等院校和研究机构,并且利用通信卫星实现了与夏威夷及欧洲等国家和地区的计算机网络系统的连接,同年 ARPANET 网络建设基本完成。

ARPANET 网络之所以能有如此大的规模与影响,主要因为它具有如下一些重要特性,而其中的大部分特性通常被认为是现代计算机网络应当具备的基本特性。

(1) 采用分组交换技术。

(2) 采用专用的通信控制处理机。

(3) 采用分层协议。

(4) 采用分散控制。

(5) 实现了资源共享。

继 ARPANET 网络之后,从 20 世纪 70 年代开始,西方许多发达国家也纷纷开始建立和发展各自的分组交换式网络。例如,英国邮政局的 EPSS 公用分组交换网、加拿大的 DATAPAC 公用分组交换网、法国信息与自动化研究所(IRIA)的 CYCLADES 分布式数据处理网等。这些网络的连网目的主要是为了实现远程的数据传输、处理和资源共享,网络的覆盖范围广,接入网络的多数为大型计算机或中小型计算机,这些网络通常被称为广域网。

在分组交换式网络大力发展,并积累了很多经验的同时,20 世纪 70 年中期出现了局域网。特别是到了 80 年代,随着微型计算机的普及应用,局域网技术得到了空前快速发展。局域网不同于广域网,它以实现共享数据、软件和昂贵的外部设备为主要目的。局域网是将一个单位内部或一个相对独立的局部区域内的各种微型计算机和通信设备连接起来的通信网络。局域网的主要特点是范围小、速度快、可靠性高,被广泛应用于办公自动化、工厂自动化、过

程控制、企业管理、辅助教学、军事指挥、医疗管理、银行业务处理和商业信息处理等领域。

从20世纪80年代初开始，Internet的发展引起了世人的瞩目。Internet是一个覆盖全球范围的互联网，它的前身就是ARPANET网络。ARPANET网络是一个成功计算机网络系统，它在概念、功能、结构和系统设计等方面为Internet的产生和发展奠定了基础。特别是随着TCP/IP协议的标准化和公开化，在ARPANET网络中也将TCP/IP协议作为网络互连的标准协议，极大地促进了Internet的发展。这一阶段是属于Internet的实验研究阶段，Internet以ARPANET网络作为主干网络。

从20世纪80年代中期至90年代中期，Interne进入了实用发展阶段。在这一时期，NSFnet取代了ARPANET网络成为Internet的主干网络。NSFnet是由美国国家科学基金会(NFS，National Science Foundation)于1984年开始组建的广域网络。NSFnet所采用的网络硬件技术与ARPANET网络基本相同，但是它在软件技术和体系结构等方面都有了新的发展与突破。NSFnet也采用基于TCP/IP的网络通信协议，它利用层次型结构方法把全美五个超级计算中心的计算机与分布于全国范围内的大学和研究所的大量的计算机彼此连接起来，构成了一个范围广泛、功能强大的计算机网络系统，并且NSFnet对全社会开放，资源可以为全社会所共享。各大学和研究院所的积极参与，极大地丰富了Internet的信息资源，于是各种Internet信息服务项目(如Gopher、FTP、WWW等)被相继开发出来，使得Internet真正发展成为以信息服务为主要目的的计算机互连网络。由于在这一时期Internet主要用于教育和科研院所的非商业应用，因此网络安全没有引起足够重视，这也给后来基于Internet的商业应用留下了安全隐患。

自20世纪90年代中期开始，Internet呈现出爆炸性增长的发展势头，不仅网络的规模在迅速扩大，而且网络的应用领域也从最初的科研和教育领域扩展到了文化、产业、政治、经济、体育、娱乐、商业及服务业等领域，使得Internet真正发展成为了一个国际性的涉及多领域的互连网络。尤其是一些有远见的企业和公司在意识到Internet商业价值后，纷纷加入Internet，并通过Internet开展产品宣传、技术支持、用户培训、产品销售和服务等工作，进一步推动了Internet的快速发展，使Internet进入了一个商业化阶段。在这一时期，Internet主干网络也由原来的政府资助转变为公司的经营与管理。

综观计算机网络的发展历史，可以看出虽然它的历史并不长，但是它的发展同样经历了从简单到复杂，从低级到高级的发展过程。计算机网络的发展

与演变过程大致可以概括地分为三个基本阶段，即具有通信功能的单一计算机系统阶段、以通信子网为中心的计算机网络阶段和以开放系统互连(OSI，Open System Interconnection)参考模型为代表的采用分层体系结构的计算机网络阶段。

目前计算机网络进入了一个高速发展的时期，随着计算机技术、通信技术、微电子技术和光电子技术等高新技术的不断创新和迅猛发展，计算机网络正朝着高速化、集成化、多媒体化和智能化等多个方向发展，网格计算、移动网络、网络存储及网络分布式对象计算等已经成为网络新的研究与应用的热点问题，新一代的网络正在酝酿和发展之中。

1.2 计算机网络定义

在计算机网络发展不同的阶段，人们对计算机网络有不同的需求和认识，因此就产生了不同的定义。一般计算机网络的定义可以分为三类：一是强调信息传输为主要目的，二是强调资源共享为主要目的，三是强调用户透明性为主要目的。而强调资源共享为主要目的计算机网络定义是目前最常用的定义，也是能够比较准确反映计算机网络基本特征的网络定义。

强调资源共享为主要目的计算机网络定义是“以能够相互共享资源的方式互连起来的自治计算机系统的集合”。其中，“资源共享”中的资源包括：硬件、软件和数据等。“互连”是指各计算机之间能够通过某种介质相互连接起来，并且相互之间能够交换信息；“自治”功能是指每台联网的计算机都是一个完整的计算机系统，它能够独立地进行工作。所有的计算机都是平等独立的，任何一台计算机都不能干预其他计算机的工作；“计算机系统的集合”是指计算机网络是由多台计算机组成，是一个计算机系统的集合体。

通过此定义可以看出，计算机网络首先是以实现“资源共享”为主要目的。其次，“互连”的计算机可以是分布在不同地理位置的多台具有“自治”功能的“计算机系统的集合”。最后，网络中计算机在信息交换时必须遵循相同的协议。

1.3 计算机网络分类

计算机网络种类繁杂，划分标准也很多，依据不同的分类标准，同一个计

算机网络可以划归到不同类型的网络中，如按照网络拓扑结构来划分，网络可以分为星型网、树型网、环型网、总线型网、全连通型网和不规则型网；按照信息交换方式来划分，网络可以分为线路交换网、报文交换、分组交换网和信元交换网；按照网络的带宽来划分，网络可以分为窄带网和宽带网；按照网络传输介质来划分，网络可以分为有线网和无线网等。以上给出的这些分类标准，大多数只是按照网络的某一方面的特征来划分网络，并不能比较全面地反映计算机网络技术的本质特性。而目前最为常用网络类型的划分标准主要有两大类，即按照网络传输技术分类和按照网络覆盖范围分类。

1.3.1 按照网络传输技术分类

计算机网络所采用的传输技术决定了网络的主要技术性能和特点。按照网络传输技术来划分，计算机网络可以分为广播式网络和点对点式网络两类。

1. 广播式网络

广播式网络是用一个共享通信信道把所有的计算机连接起来，网络中任何一台计算机发出的信息都能够被所有其他计算机接收到的计算机网络。目前，大多数的局域网和城域网都采用这种技术，并且以微波、卫星通信方式传播的广域网也采用这种技术。

2. 点对点式网络

在点对点式网络中，一条通信线路只连接两台计算机，直接的数据交换仅仅发生在直接连接的两台计算机之间。在计算机网络中，通常是源计算机与目的计算机之间并没有直接通路，于是源计算机发出的信息一般要经过中间若干结点的转发，才能够到达目的计算机。由于从源计算机到目的计算机的信息传输的路径可能不止一条，并且比较大的报文还需要分解为若干小分组才能够在网络中正常传输，因此路径选择和分组存储转发是点对点式网络中必须解决的主要问题。目前，大多数的广域网都采用这种技术。

1.3.2 按照网络覆盖范围分类

按照网络覆盖范围来划分，网络可以分为局域网、城域网和广域网三大类。

1. 局域网

局域网(LAN，Local Area Network)顾名思义就是局部区域内的网络，它是指在一个有限范围内的各种计算机设备和通信设备互连起来的通信网络。局域网以实现共享数据、软件和昂贵的外部设备为主要目的。

局域网是计算机网络技术中应用最为广泛的技术之一，也是计算机网络技术成功应用的一个范例。局域网常用于政府机关、企事业单位和校园网的组建，接入局域网络的设备主要包括个人计算机、工作站、打印机、扫描仪、绘图仪及各种网络通信设备（如集线器、交换机、路由器）等。目前许多单位都有自己的局域网，甚至有的家庭中也都有自己的小型局域网。

局域网具有速度快、可靠性高、区域有限、组网方便、使用灵活、投资少等特点，可以归纳为以下几个方面。

（1）网络的覆盖范围有限

局域网的覆盖范围小，一般在数千米以内，网络属于一个部门或一个单位所有。网络的覆盖范围与使用的传输介质密切相关，目前局域网常用的传输介质主要有双绞线、同轴电缆和光纤等。使用双绞线和同轴电缆作为网络的传输介质时，网络的覆盖范围一般在 1km 左右。而使用光纤时，其网络的跨度可以达到 30km 左右。

（2）网络拓扑结构灵活多样

局域网的网络拓扑结构主要采用总线型、环型和星型三种，如图 1.1 所示。以往采用最多的是总线型网络拓扑结构的局域网，但是20 世纪 90 年代后

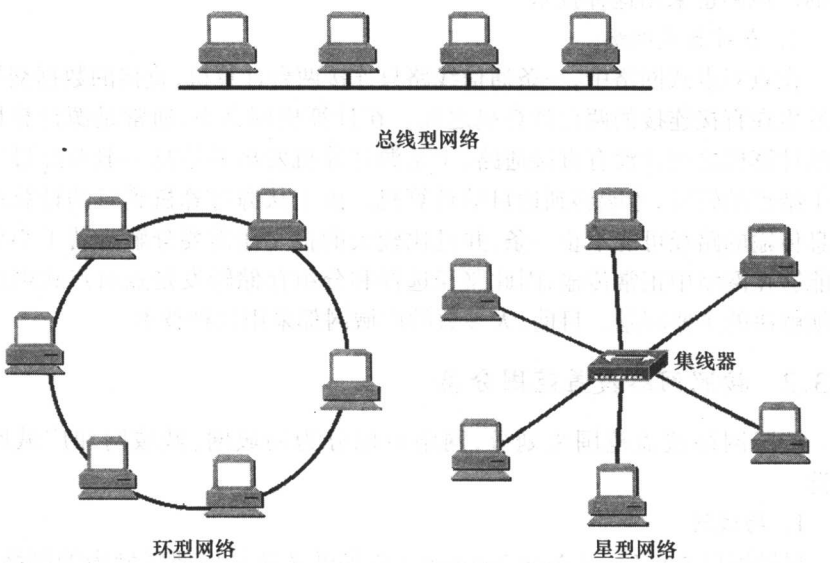

图 1.1　总线型、环型和星型网络拓扑结构

期随着交换型局域网网络技术的飞速发展，采用星型拓扑结构的局域网已经取代了采用总线型网络拓扑结构局域网的统治地位，成为局域网的主流形式。

(3) 传输速率高且误码率低

局域网的传输速率一般为 10Mb/s～100Mb/s，在高速局域网中速率可以达到 1000Mb/s～10Gb/s。误码率一般在 10^{-8}～10^{-11}范围内。它的低延时和高可靠性，能够很好地支持计算机间的高速通信。

(4) 支持多种介质访问控制方式

局域网支持的介质访问控制方式主要有：CSMA/CD(载波侦听道路访问/冲突检测)介质访问控制方式、Token Bus(令牌总线)介质访问控制方式和 Token Ring(令牌环)介质访问控制方式等三种。目前应用最多的是采用广播式的 CSMA/CD 介质访问控制方式的以太网(Ethernet)。

2．城域网

城域网(MAN，Metropolitan Area Network)顾名思义其网络的覆盖范围是一个大的城市区域，一般在几十千米以内。城域网是一种介于局域网和广域网之间的高速网络，它采用的技术与局域网相类似，只是网络的覆盖范围比局域网更大一些，可以说是 LAN 网络的延伸，连接的计算机数量更多，一个城域网通常连接着多个局域网。

城域网的主要特征可以归纳为以下几个方面。

(1) 网络的覆盖范围较大

城域网的网络覆盖范围在一个大的城市区域内，最大范围一般不超过 100km。城域网的建设、使用和管理可以是由一个单位或部门完成，也可以由政府统一规划管理。

(2) 网络拓扑结构简单，且采用无竞争的介质访问控制方式

城域网是一种标准成熟，结构简单的计算机网络。其网络标准采用的是 IEEE 委员会制定的 IEEE 802.6 标准，网络拓扑结构通常采用的是标准中推荐使用的称为分布式队列双总线(DQDB，Distributed Queue Dual Bus)结构。

DQDB 采用双总线的网络拓扑结构，两条总线贯穿整个城市，城市中的每个结点都同时与两条总线相连接。每条总线都是单向的，并且每条总线都有一个端点，它产生一个稳定的 53 字节的信元流。这种双总线的网络拓扑结构使得网络的各结点之间的信息发送和接收形成了一个环流，从而形成一个环型信道。对网络的访问采用的是无竞争的、有序的介质访问控制方式。

(3) 综合服务

城域网的综合服务功能主要体现在：局域网的互连、对多媒体信息传输的

支持及提供宽带综合业务服务等。

3. 广域网

广域网(WAN,Wide Area Network)顾名思义是广阔区域的网络。广域网可以跨城市、跨地区、甚至跨国家地进行信息的交换和资源共享,形成一个远程网络。由于广域网信息传输的距离较远,再加上信号衰减也比较严重,因此广域网一般都采用租用专线方式来建网,通信方式采用分组交换技术。在我国除电信网外,还有广电网、联通网等为用户提供远程通信服务。但是随着经营政策的改革与落实,也出现了其他部分部门单位自行组网的现象。另外,广域网总的出口带宽有限,一般用户的终端连接速率较低,通常在 9.6Kb/s~45Mb/s 之间。

广域网的主要特征可以归纳为以下几点。

(1) 网络的覆盖范围广

广域网的网络覆盖在一个很大的区域范围内,一般可以从几十千米到几千千米。覆盖范围广,接入设备多且复杂。

(2) 通常采用分组交换技术

广域网的通信子网通常采用分组交换技术,可以充分利用公用分组交换网、卫星网和无线分组交换网等网络将分布在不同地点的计算机系统连接起来,实现信息交换和资源共享。

(3) 多功能多用途的综合服务

广域网的多功能多用途的综合服务功能主要表现在:大的区域范围内的局域网互连、城域网互连及提供宽带综合业务服务等。

1.4 计算机网络功能

计算机网络的功能强大,内容丰富,但是最基本的功能主要有以下几点。

(1) 数据传输

数据传输是计算机网络的最基本功能之一,它用于实现计算机之间的信息的传递。

(2) 资源共享

资源共享是计算机网络的主要目的。在计算机网络中,资源主要是指计算机硬件、计算机软件和数据。资源共享能够使用户跨越时空限制,共享网络系统中的资源,避免重复投资,提高了资源的利用率和工作效率。

(3) 均衡负荷及分布式处理