网络安全与网络行为研究

朱超军 ◎ 著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

网络安全与网络行为研究

朱超军 ◎ 著

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

内 容 提 要

本书是作者结合多年来对网络安全与网络行为的研究成果撰写而成的。从计算机网络、网络体系结构及计算机网络安全入手，深入探讨了网络的攻击行为和防范、网络犯罪态势、网络犯罪分析和网络行为的立法规范，重点对网络时代下我国高校文化建设面临的挑战和对策进行了研究。

图书在版编目（CIP）数据

网络安全与网络行为研究 / 朱超军著. —北京：北京理工大学出版社，2019.3

ISBN 978-7-5682-6838-7

Ⅰ.①网…　Ⅱ.①朱…　Ⅲ.①计算机网络－网络安全－研究　Ⅳ.①TP393.08

中国版本图书馆CIP数据核字(2019)第044351号

出版发行/北京理工大学出版社有限责任公司

社　　址/北京市海淀区中关村南大街5号

邮　　编/100081

电　　话/(010)68914775(总编室)

(010)82562903(教材售后服务热线)

(010)68948351(其他图书服务热线)

网　　址/http://www.bitpress.com.cn

经　　销/全国各地新华书店

印　　刷/河北鸿祥信彩印刷有限公司

开　　本/710毫米×1000毫米　1/16

印　　张/11

字　　数/196千字

版　　次/2019年3月第1版　2019年3月第1次印刷

定　　价/55.00元

责任编辑/王美丽

文案编辑/孟祥雪

责任校对/周瑞红

责任印制/边心超

前　言　Preface

从世界上第一台计算机诞生到今天互联网的日益普及，计算机的发展速度可谓突飞猛进，从而也把人类文明带入信息时代。计算机网络的出现，使人们在获取和传递信息时又多了一种选择，而且是一种能够提供空前“自由化”的选择。它使信息的传播速度、质量与范围在时间和空间上有了质的飞跃。

随着计算机在社会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，网络尤其是Internet网络的开放性加上系统的缺陷与漏洞、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。

随着网络时代的到来，虚拟空间出现“道德真空”，对传统的社会生活秩序造成很大冲击。大学生是网络用户的重要组成部分。调查获悉，随着高校信息化进程的加快和校园内网络接入条件的改善，大学生的网络行为越来越普遍，上网成为大学生学习、交往、娱乐等生活的重要内容。同时，由于网络上的犯罪现象越来越多，网络犯罪已成为发达国家和发展中国家不得不关注的社会公共安全问题。规范网络行为，防治网络犯罪，已成为整个社会必须面对的课题之一。

本书涉及内容较多，参考了大量的书籍、论文和网络资源，书后列出了较为详尽的参考文献，但涉及面太广，难免挂一漏万，如有遗漏，敬请谅解。

由于作者水平有限，书中难免有疏漏和错误之处，恳请读者批评指正。

著　者

目 录 Contents

第一章　计算机网络

目前，人类社会正从工业经济时代转向知识经济时代，知识经济时代的重要特征就是数字化、信息化和全球化，而信息化和全球化的实现离不开计算机网络。计算机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。

第一节　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、从局部应用到广泛应用的发展过程。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信息的远程传递和共享要求，而通信技术为信息的远程传递和共享提供了可能，将计算机技术与通信技术相互结合，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、增强信息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，是计算机网络产生的技术基础；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。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，通常被认为是计算机技术与通信技术相结合的先驱，该系统能够将分布在 17 个防区内的雷达观测站、机场、防空导弹和高射炮阵地通过通信线路连接，形成一个联机计算机系统，由计算机程序辅助指挥员做决策，自动引导飞机和导弹进行拦截。

现代计算机网络(Internet)的前身——ARPANET(阿帕网络)诞生于 20 世纪 60 年代末。

ARPANET 是由美国国防部高级研究计划管理局(Advanced Research Projects Agency，ARPA)于 1969 年创建的。当时研究的目的是应对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。其目标是在军事上建立一个分散的指挥系统，一旦战争爆发，即使部分指挥点被摧毁，仍然能够通过网络使信息自动转接到正常工作的指挥点上，指挥系统仍然能够保持正常运转。

ARPANET 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 的规模不断扩大，1972 年接入 ARPANET 的计算机达到了 40 台，1983 年达到了 300 台。ARPANET 扩散至整个美洲大陆，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 建设基本完成。

ARPANET 之所以能有如此大的规模与影响力，主要是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 之后，从 20 世纪 70 年代开始，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的 CYCLADES 分布式数据处理网等。这些网络主要是为了实现数据的远程传输、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。

20 世纪 70 年代中期，在分组交换式网络大力发展并积累了很多经验的同时，出现了局域网。20 世纪 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。

20 世纪 80 年代初，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。ARPANET 是一个成功的计算机网络系统，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，ARPANET 也将 TCP/IP 协议作为网络互联的标准协议，这极大地促进了 Internet 的发展。这一阶段是属于 Internet 的实验研究阶段，Internet 以 ARPANET 作为主干网络。

20 世纪 80 年代中期至 90 年代中期，Internet 进入了实用发展阶段。在这一时期，NSFNET 取代了 ARPANET 成为 Internet 的主干网络。NSFNET 是由美国国家科学基金会(National Science Foundation，NSF)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 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国 5 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联网络。由于在这一时期 Internet 主要应用于科研和教育领域，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 真正发展成为一个国际性的涉及多领域的互联网络。一些有远见的企业在意识到 Internet 的商业价值后，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。

纵观计算机网络的发展历史，可以看出，虽然它的发展历史并不长，但是它的发展同样经历了从简单到复杂、从低级到高级的过程。计算机网络的发展与演变过程大致可以概括为三个基本阶段，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联(Open System Interconnection，OSI)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计算机网络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。

第二节　计算机网络的定义

在计算机网络发展的不同阶段，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。

强调资源共享为主要目的的计算机网络定义是目前最常用的定义，能够比较准确地反映计算机网络基本特征。

强调资源共享为主要目的的计算机网络定义是：以能够相互共享资源的方式互联起来的自治计算机系统的集合。其中，“共享资源”中的“资源”包括硬件、软件和数据等；“互联”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”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的，是一个计算机系统的集合体。

通过上述定义可以看出，计算机网络，首先，是以实现“资源共享”为主要目的；其次，“互联”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。

第三节　计算机网络的分类

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。例如，按照网络拓扑结构来划分，网络可以分为星形网、树形网、环形网、总线形网、全连通形网和不规则形网；按照信息交换方式来划分，网络可以分为线路交换网、报文交换网、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。目前最常用的网络分类方法主要有两种，即按照网络传输技术分类和按照网络覆盖范围分类。

一、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被其他计算机接收到的一种计算机网络。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节点的转发，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。

二、按照网络覆盖范围分类

按照网络覆盖范围来划分，计算机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(Local Area Network，LAN)，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联起来的通信网络。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。

在计算机网络技术中，局域网应用最广泛，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，网络归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，网络的覆盖范围在 1 km 左右；而使用光纤时，网络的覆盖范围可以达到 30 km。

(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形、环形和星形三种。起初采用最多的是总线形网络拓扑结构的局域网，随着交换型局域网网络技术的飞速发展，到 20 世纪 90 年代后期，采用星形网络拓扑结构的局域网已经取代了采用总线形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 10～100 Mb/s，在高速局域网中速率可以达到 1 000～10 240 Mb/s，误码率在 10^{-8}～10^{-11} 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(载波侦听多路访问/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(Metropolitan Area Network，MAN)，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类似，只是网络的覆盖范围比局域网大一些，可以说是局域网的延伸，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 100 km。城域网的建设、使用和管理可以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 IEEE802.6 标准，网络拓扑结构通常采用的是标准中推荐使用的分布式队列双总线(Distributed Queue Dual Bus，DQDB)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，城市中的每个节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节点之间的信息发送和接收形成了一个环流，从而形成一个环形信道。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：局域网的互联、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(Wide Area Network，WAN)，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 9.6 Kb/s～45 Mb/s。

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联、城域网互联及提供宽带综合业务服务等。

第四节　计算机网络的功能

计算机网络功能强大、内容丰富，其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，提高了工作效率和资源的利用率。

3. 均衡负荷及分布式处理

计算机系统中的一些作业传送给网络中的其他计算机系统去处理，实现了均衡负荷，提高了工作效率。

分布式处理功能使得计算机网络能够将一个大型的科学计算任务或信息处理任务分散到不同的计算机上，进行分布式处理。这种分布式处理对用户来讲是透明的。

4. 综合信息服务

随着 Internet 网络应用的飞速发展，综合信息服务已成为计算机网络提供的基本服务功能。计算机网络不再只提供文字和数字信息的传输，它同时能够提供图形、图像、音频和视频等多媒体信息的传输、存储、加工和处理功能，以实现综合信息服务。

第二章　网络体系结构

第一节　网络协议

建立计算机网络的主要目的是实现资源共享和数据传输，进一步实现分布式处理。数据传输是基础，实现资源共享和分布式处理都需要有数据传输的支持。因此，计算机网络的特点就是多计算机之间的协同配合与信息的相互交换。要在多计算机之间有条不紊地进行信息交换，必须制定一系列的规则、标准或约定，参与通信的各方共同遵守、执行，从而保证网络通信的正常进行。这些说明信息交换格式、信息交换方法和信息交换过程的规则、标准或约定的集合，通称为协议(Protocol)。协议是网络特有的产物，是网络赖以生存的保证手段。有网络，就有通信；有通信，就离不开协议。因此，协议在网络中占有非常重要的位置。

网络协议是由语义、语法和时序三要素组成的。

1. 语义(Semantics)

语义规定了通信双方如何进行数据交换，包括需要发出何种控制信息，完成何种动作以及做出何种应答等。因此，语义部分由发出的命令请求、完成的动作和回送的响应集合组成，同时定义了用于协调同步和差错处理的控制信息等。

2. 语法(Syntax)

语法规定了通信双方进行信息交换时所采用的信息结构与格式，包括数据与控制的信息格式、编码及信号电平等。

3. 时序(Timing)

时序规定了通信过程中事件发生的顺序以及速度匹配和排序等。

计算机网络是一个庞大而复杂的系统，要保证网络通信能够有条不紊地进行，就需要制定一系列的协议。每种协议都是针对某个特定的目标和问题来设计的。例如，文件传输协议(File Transfer Protocol，FTP)是为了实现文件传输而设计的

协议；超文本传输协议(Hyper Text Transfer Protocol，HTTP)是为了浏览器与Web服务器之间进行网页浏览而设计的协议；等等。因此，在计算机网络中存在大量的各种各样的协议。这些协议在网络的灵活性、差错控制、流量控制、同步机构、路由选择、安全保密、格式转换以及系统兼容性等方面做出了定性规定。

第二节　计算机网络的体系结构

计算机网络通信是一个非常复杂的过程，不可能用一个协议规定了所有的通信细节。因此，为了减少网络协议设计的复杂性，提高其可靠性、可用性和可维护性，网络设计采用了在工程设计中常用的结构化设计方法，即将复杂的通信问题划分为若干易于处理的子问题，然后为每一个子问题设计一个单独的协议。每个单独协议的设计、编码和测试都能够相对独立地去完成。这种“分而治之”的设计方法，大大降低了计算机网络系统设计和实现的复杂性。

分层模型(Layering Model)就是一种用于开发网络协议的设计方法。在分层模型中，整个网络通信过程是按照层次方式来组织的，每层协议完成该层的一些特定功能。层与层之间是上下连接的关系，下层为上层提供服务，每一层在接受下一层提供服务的基础上实现本层的功能，再向上一层提供服务。服务是通过层间接口提供的，上层不必关心下层的内部结构与实现细节，只关心能够为上层提供什么样的服务，以及如何使用下层提供的服务来实现本层的功能等。

采用分层模型的好处有以下几个方面：

1. 降低了网络通信设计的复杂性，易于实现

计算机网络是一个庞大而复杂的系统，将其通信过程划分为若干功能层次，使得整个系统的结构功能完整，层内功能具体、明确且相对独立，层间接口清晰，从而方便了设计、简化了系统实现。

2. 灵活性好，便于更新，易于维护

当某一层的内部结构发生了变化，或者是实现技术和方法有新的突破时(如算法更新、新技术或产品的出现等)，只要上下层之间的服务与接口关系保持不变，其上层与下层就不会受影响，系统具有良好的灵活性，便于更新，易于维护。

3. 有利于交流和理解，促进了网络协议的标准化

由于每层的功能及所提供的服务都已有了明确定义和说明，因此有利于不同系统之间的交流和理解，满足了网络协议的标准化的要求，进一步促进了网络协