揭开网络安全的面纱，探讨网络安全的本质

增强网络安全的意识，提升网络安全的能力

网络安全

陈 震 编著

Network Security

清华大学出版社

网络安全

陈 震 编著

Network Security

清华大学出版社
北京

内 容 简 介

无论是哪一门学科，只有研究其中的本质问题，才能在已有的基础上发展，才能在巨人的肩膀上看得更远。技术来源于生活和社会实践，对很多看似高深的理论，如果能发现它的本质、了解其产生的根源，才会对其理解得更加透彻和深入。本书编写的目的是揭开计算机网络安全的表相，探讨网络安全本质，增进网络安全意识，了解网络攻击的原理，把握攻击防范的技术，化解网络安全风险。

每个国家、组织、机构和个人都有秘密，人们都希望自己的秘密不被他人发现。而出于各种各样的原因，人们又会渴望知道别人的秘密。如果这些秘密被人获知，代价有时是无比巨大的。密码学代表了人类对机密的重视，也体现了人类高超的智慧。本书阐述了密码学在网络通信安全中的应用，同时介绍了同态加密、加密数据库、密文检索以及比特币等密码货币的应用。

本书适合作为高等院校本科生的网络安全类教材，也适合作为网络安全爱好者的参考书。

图书在版编目(CIP)数据

网络安全/陈震编著．—北京：清华大学出版社，2015

ISBN 978-7-302-39335-1

Ⅰ．①网…　Ⅱ．①陈…　Ⅲ．①计算机网络－安全技术－高等学校－教材　Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 024960 号

责任编辑：白立军

封面设计：傅瑞学

责任校对：白　蕾

责任印制：李红英

出版发行：清华大学出版社

网　　址：http://www.tup.com.cn，http://www.wqbook.com

地　　址：北京清华大学学研大厦 A 座　　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

课 件 下 载：http://www.tup.com.cn，010-62795954

印 装 者：清华大学印刷厂

经　　销：全国新华书店

开　　本：185mm×260mm　　**印　　张**：6.5　　**字　　数**：140 千字

版　　次：2015 年 5 月第 1 版　　**印　　次**：2015 年 5 月第 1 次印刷

印　　数：1～2000

定　　价：19.00 元

产品编号：063147-01

前　言

人们享受互联网带来的便利的同时，也面临着种种安全危机。然而，或许是互联网知识欠缺，或许是过于信任开发厂家，大多数人只是将互联网作为了一种娱乐、办公、社交的便捷方式，而忽略了与联网如影随形的网络安全风险，使个人隐私与利益面临种种威胁。

当前互联网逐渐暴露出越来越多的安全问题、各种网络安全现象日益突出情况，很多研究机构都在针对互联网安全问题展开研究。然而，目前国内很少有详细介绍网络安全本质的书籍。对于热心网络安全，希望了解网络安全本质的读者，本书是很好的入门和指导书籍。

在计算机和互联网这个平台之上，许许多多的革新正在不知不觉中层出不穷地上演，人们需要及时更新自己的思维与视角，才能跟上时代的步伐。网络安全是一门交叉学科，和众多学科一样，在解决问题时有两个经典思路（学院派和产业界的区别）：

① 碰到一个问题，解决一个问题——自下而上一点一点拼成系统；

② 构想系统应该是什么样子的——自上而下宏观思考构建系统。

本书有针对性地介绍了网络安全问题的产生、互联网的基本原理和设计的具体协议，以及网络安全威胁的攻击与防范等读者关心的具体问题，并针对这些问题提出了具体的解决方案。本书剖析了网络安全与密码学的关系，介绍了未来网络可能的发展方向、密码货币的诞生与发展，以及网流归档与取证在互联网安全中的重要性。

全书共分 9 章。第 1 章主要介绍安全的本质和网络的本质。第 2 章主要介绍计算机系统与计算机网络。第 3 章介绍一些网络技术和原理。第 4 章介绍网络安全涉及的内容。第 5 章介绍网络攻击的类型。第 6 章介绍网络安全防范技术。第 7 章介绍通信安全与密码学原理。第 8 章介绍未来网络技术。第 9 章介绍最近的网络安全研究的新兴领域。

书中不当之处恳请广大读者指正。

编　者

2015 年 1 月

目　录

第1章 导 论

1.1 网络安全面面观

1.1.1 不安全的世界与不安全的网络

“网络社会”(Cyber Society)是在计算机网络提供的信息通信、存储和传播的功能的信息基础设施上,由人类社会中的网民(Netizen)虚拟出来的一个社会空间,这个空间活跃的社会角色都映射到使用计算机的现实用户上。

这个虚拟的社会折射了很多现实社会的影子,反映了很多现实社会中不能获得的诉求。因此,社会的行为,如互助、竞争、攻击等;社会的关系,如伙伴、朋友、圈子等;社会的愿望,如正义、公平和稳定等,这些社会特征一样会反映到这个虚拟空间上,最后落实到提供信息基础框架的计算机软件和网络设备上。

现实社会有如下很多典型的安全事件。

(1) 2001 年的 9·11 事件,恐怖分子劫持了 2 架客机撞击美国世贸中心双子大楼,导致世贸中心夷为平地,美国社会陷入了对国家安全的担忧之中。

(2) 2008 年次贷危机,雷曼兄弟公司倒闭,美林公司破产,花旗银行大幅贬值几近崩溃,导致全球陷入经济危机,数百万人失业,经济衰退。

(3) 2009 年金融危机进一步恶化,中国和国际社会一道对美元作为储备货币所引发的经济安全问题表现出担忧。

(4) 2010 年中国北斗系统信号被破解,引发了人们对国家机密的担忧。

(5) 2013 年 6 月,斯诺登曝光了美国“棱镜计划”等网络安全计划,引发了人们对网络安全的军事竞赛担忧。

(6) 2014 年苹果手机追踪用户行踪功能被关注,引发了用户对个人隐私的担忧。

……

世界动荡不安,可以想象网络上也不会风平浪静。

1.1.2 互联网安全风险无处不在

人们平时使用手机或者计算机,主要用来浏览门户网站,收发邮件,使用网银支付,或者下载一些软件等,似乎感觉不到这里有什么安全风险。

殊不知来自网络的安全威胁从计算机连接网络的这一刻开始就已经如影随形。例如,计算机获取的 IP 地址可能是一个私有 DHCP 服务器放出来的,笔记本电脑连接的无线路由器可能是一个钓鱼的无线热点,甚至手机连接的基站也有可能是一个伪基站。

浏览器打开的网站有可能是钓鱼网站，下载的网页中隐藏各种广告和间谍软件，网页中可能嵌入了木马程序，下载的客户端软件中可能被植入了病毒，安装的新应用植入了吸费吸流量的恶意代码，收到的垃圾邮件或许就是“钓鱼”邮件等。互联网安全的风险无处不在。

1.1.3 谁控制着你的手机与计算机

人们买了一部安卓智能手机，用了段时间后发现内存不够用，想卸载一些内置应用，却发现不能卸载。如果要卸载内置应用，往往要采用 Root 方法。这就是用第三方的黑客工具取得管理员权限。但是 Root 完后，其实又把管理权托管给了提供 Root 工具的第三方。人们自始至终都没有真正的控制权。

智能手机是具有计算机功能的手机。智能手机、笔记本电脑和 PC 等这些计算机的控制权，并未完全由用户掌握。这是因为在这个场景下，普通用户是使用软件运行在计算设备的硬件平台。其中，软件开发商生产软件产品，硬件制造商生产硬件产品。

硬件制造商、软件开发商与普通用户之间作为商业产品的销售方与购买方，存在一定的责任权利的关系。用户与软件厂商之间的关系，需要有产品的使用许可证和质量保证，产品需经过测评认证，不违反知识产权。

但是，计算机系统的使用权始终不是风平浪静的，未经授权而获得计算机系统的使用权的情况始终存在。

首先，软件厂商或公司为了追求商业利益可能突破相关约定，控制引导用户的使用行为。用户是不是应该把他们的安全寄托于部分公司上，公司天然是封闭的，对用户是不负责的。无论公司对用户有多少承诺，都无法改变其盈利的最终目的，公司很可能会牺牲普通用户的利益以获得更大的商业利益。

黑客则利用系统漏洞，暴力攻击以获取计算机的使用权。恶意代码的制作者受“黑金”利益的驱动，使用木马伪装成免费安全软件，将病毒“伪装”植入某些正常软件，在用户不知情的“默许”下，获得控制权。再加上计算机司法取证的困难，普通用户的知识水平低和安全意识薄弱，使得用户在计算机控制权的博弈中始终处于不利地位。

1.1.4 谁控制着互联网

互联网作为信息发布与获取的网络平台，其控制方包括网络设备商、网络运营商和网络服务商以及其他相关的监管机构。

互联网的控制权应该掌握在谁手中呢？网络运营商、网络服务商、网络设备商、普通网络用户和监管机构之间的责权利应该如何划分？

电信网络是一个高度集中控制的通信网络，电信网络运营商同时也是网络服务商，因此普通用户对电信网络没有控制权，这种控制机制使得普通终端用户在网络应用的创新中也没有主动权。

与之相反，互联网是一个个分散多域管理的网络，通过路由器和配置路由协议，以对等或者购买服务的方式（如 Eyeball ISP），实现不同网络之间互连互通。单个网络运

营商对网络的接入也意味着需要对其他网络承担责任(为其他网络转发流量)。基于端到端的原则,终端用户在网络应用的创新过程中拥有更多的主动权。在绝大多数情况下,网络运营商的工作就是提供一个通道,而即使是普通用户也可以自己创建网络服务提供给其他用户。

网络服务商因为直接提供用户网络服务,从用户使用其服务与产品中获得商业价值。因此,更加关心网络的通信质量,网络的连通性,以及普适的用户接入。大的有实力的网络服务商(如 Google 公司)都在纷纷自建网络,互连自建的数据中心,调优内部网络的性能,以对外提供最佳的服务。

值得指出的是,网络中性化(Network Neutrality)是目前的一个热名词。人们认为网络中性化并不意味着网络去控制化,相反网络的控制功能更需要加强,但是这种加强功能是否需要时时激活,是由网络管理策略来决定的。

1.1.5 系统的安全漏洞

当前随着计算机系统的功能越来越丰富,系统的规模越来越庞大,软硬件系统自身的健壮性由于系统的复杂性而降低,造成系统存在很多安全"漏洞",需要不断安装更新补丁修补。在软件开发过程中,开发的复杂性通过编程语言、编程类库、编译工具和操作系统调用而大大增加了安全漏洞的产生。同时,在商业化的竞争压力下,在系统的功能、性能与安全性之间的平衡中,系统开发对安全功能的重视不够,因为安全往往需要以牺牲性能为代价。

一个典型的案例是微软公司的操作系统——Windows XP 系统,它一度是最流行的桌面系统,因为对易用性的重视而忽视了安全性,导致大量安全问题的产生;而 Windows Vista 系统,由于过于重视安全性而导致性能的下降,大大减少了用户的接受程度,成为昙花一现的短命产品。

1.1.6 网络空间

赛佰空间(Cyberspace)是由互联网连接的信息系统组成的信息空间,与目前现实四维空间对应。这个信息空间包括虚拟的社区、个体与文化,计算机网络系统是该信息空间的支撑。

计算机网络系统本身就是大规模的分布式系统,需要解决可靠性、高效率和低成本的问题。信息以网包为载体,通过网络系统传递。计算机网络产业是一个繁荣的生态系统(Ecosystem),网络系统也是一个基于计算机系统的基础设施,其每个组件都是计算机系统。由组件构造新的组件,最后组成服务产品,符合人类不断建造更大可用系统的内在动力。

1.1.7 网络安全是什么

互联网安全是赛佰空间中互联网连接的信息系统的控制权的博弈。互联网作为信息通信的基础设施,功能类似一个国家的"神经系统"。控制了互联网上的信息导向,就

可以做到舆论导引等。

什么是网络安全？从技术层面来看，网络安全是一种博弈。计算机系统和计算机网络范围内，研究基于网络的系统攻击原理及技术，研究基于网络的保护方法和抵抗可能的破坏及风险。

从国家层面来看，大国都在角力基于互联网的赛佰空间控制权，进行防御与进攻。平时进行情报收集和信息渗透；战时则进行渗透控制和框架破坏以及摧毁性打击。如美国斯诺登案暴露的网络监控案例。

从商业层面来看，控制用户的网络行为，就可以获得更多的商业价值。无论是安全软件的行为，还是黑客的背后淘金行为，或者是网络黑社会的敲诈勒索行为，抑或是恶意商业竞争之间的互相攻击和防御，都使得网络安全市场面临军备竞赛的局面。

从人的层面来看，网络安全的根源是人。人性存在“善”与“恶”，人的行为与环境互为影响，人的行为充满了叛逆、对抗、好奇、热心等。

开放的网络接入环境和开放的网络服务，使得做坏事成本降低。再加上审计缺失与隐私功能，使得网络取证难，而较难被追查。在网络环境下，每个人都犹如戴了一副面具，消除了顾虑，带来了更大的自由度，形成了网络环境对于人性的“善恶”的放大效应。同时也造成了网络复杂而难以管理的环境，除了需要国家来立法、采取强制性的管理以外，更需要每个人的自觉，以营造良好的网络环境。

1.1.8 互联网的环境与文化

互联网的技术标准主要由 IETF 制定，这些标准可以公开评阅和发布。IETF 是一个自发的松散组织，它为互联网技术的工程和演变做出了重大贡献。IETF 是参与制定新互联网标准规范的主要机构。IETF 的文化传统之一体现于 David Clark 早期说的有关 IETF 的一句话：“我们拒绝国王、总统和投票。我们信奉‘大致共识’和‘运行的代码’。”IETF 内普遍接受的另一个信念则如 Jon Postel 早期所说：“发送建议时要保守，接受建议时要开放。”

互联网工程技术也是人类的文化结晶。互联网的工程技术体现了人类社会的意识形态，是集中式更有效，还是分布式更合理？云计算代表前者的集中主义形态，P2P 对等网络代表后者的自由主义形态。

互联网架构是分布式更可靠，还是集中式更安全可控？从过去高度控制的电信网络，发展到分布式自治的互联网。未来的发展是回归高度可控，还是走向更加分散管理？根据不同的设计理念，演化出了不同的未来网络形态，如软件定义网络（SDN，由统一的控制器负责网络的资源管理）和信息中心网络（ICN，以信息交换为本质的分布式网络）。

覆盖网络是当前互联网上的一种重叠组织，覆盖网络的发展，是在现有网络的基础上，构建一个又一个的虚拟网络。这些虚拟网络，可以认为是一个个虚拟社区（Vartual Community），也代表着不同的价值取向和思想形态。从内容的共享到比特币挖矿，凝聚每个社区的是动机和激励；从 BitTorrent 网络的帕累托效率（Pareto Efficiency）到比特币网络的交易等，保障了虚拟网络系统的稳定。哪里有动机与激励，哪里就有虚拟社

区的发展空间。

1.1.9 霍布斯哲学的解释

托马斯·霍布斯(Thomas Hobbes)是英国的著名政治哲学家,他创立了机械唯物主义的完整体系。1651年,霍布斯出版的《利维坦》详细描述了人类从"自然状态"如何形成"利维坦"以及国家。

霍布斯描述的"自然状态",是指每个人都需要世界上的每样东西,也就有对每样东西的拥有权力。但由于世界上的东西都是不足的,资源总是受限的,所以这种资源权力的争夺导致"人和人的冲突"便永远不会结束。而在"自然状态"下,有一些人天生或者后天可能比别人更聪明或更有力量,但没有一个人不怕被暴力攻击而丧命。当受到这些威胁时,人必然会尽一切所能来保护自己。因此,霍布斯认为保护自己免于暴力攻击就是人类最高的需要,而权力的产生就是来自于这种需要。

但是,暴力冲突并不是对所有人都是最有利的。霍布斯认为为了考虑自身安全和避免被他人侵犯,只有在社会契约(Social Contract)的约束下,社会才能有和平。因此,霍布斯认为社会是一群人服从于一个威权,而每个个人(Individual)将自然权力交付给这威权,让它来维持内部的和平并抵抗外来的敌人。这个威权就是一个强而有威信的"利维坦",只有它才能令社会契约实行。

1.1.10 互联网的"利维坦"

因为互联网没有一个单一的控制权威,并且是开放接入和获取服务,技术的创新层出不穷,监管往往赶不上创新的步伐。因此,互联网的生态可以认为是一种霍布斯所说的自然状态。

如同"霍布斯主义"(Hobbesian)描述的每个个体是自私而野蛮地进行一种无限制的竞争情况。而少数个体比其他个体了解更多的技术,比如黑客、安全公司等,从而可以获得比其他个体更多的能力,就形成了"利维坦"。这些个体就容易攻击、控制别的机器。其他个体只能依附在某些"利维坦"之下,依托利维坦提供服务和保护,如各种杀毒软件公司等。

用户与"利维坦"之间签订的不仅仅是产品或者服务的合同,或仅仅是托管了自己的网络账户或者文件数据,以获取网络使用的便捷和安全;这种托管和信任更是心理上的合同,以信任互联网公司的其他产品或者服务。

1.2 安全的本质

要想了解网络安全,从身边的社会中可以看到同样的影子。

1.2.1 安全的定义

安全一直和威胁相随相伴。自人有自我意识以来,便能够区别自我和非我,外在的

世界一直有危险和伤害。自然环境并非总是友好的，来自外界的各种攻击不断，威胁着身心。正如老子所言："天地不仁，以万物为刍狗。"

安全(Security)的字面意思是免于风险和伤害。安全就是用来摆脱威胁和伤害。

本质上"安全"是一组物质设施、一种社会精神意识和个体的心里感觉。人的安全感来自什么？衣食无忧，家庭幸福，周围环境受我控制，职业和社会状况可确定可控。社会安全感来自什么？犯罪率低，社会稳定，公民都有好的社会保障体系和福利体系。国家安全感来自什么？民富国强，拥有最先进的武力等。

1.2.2 如何保障安全

为了保障安全，在人类社会中如何做到呢？

(1) 了解威胁和风险。对威胁进行防范，要"未雨绸缪"，时时监控；对攻击进行阻挡，要"防御性进攻"。

(2) 提高自身的对抗能力。通过打疫苗，提高免疫能力，对危机的反应能力，对危机的控制能力。

(3) 隔离是保护安全的直接手段。如防盗门锁、禁闭室、监狱、黑名单、经济封锁和制裁等。

(4) 增强对威胁的控制性(防御走向进攻)。知己知彼，分析自身的脆弱性和黑客攻击方法和手段，主动防御(Proactive)。

(5) 惩罚手段。经济处罚，限制人身自由，以暴制暴等惩罚手段。

1.2.3 "适度"安全

绝对安全状况是不存在的，因此对安全的追求是一种无止境的追求，是一个永无止境的过程。安全的需求，基于人的现实需求，满足现实需求，基于人的心理需求，满足心理需求，才会有相对的安全感。

对于安全，可以引入风险控制模型，如图 1.1 所示。举个例子，某些地区晚上出门是很危险的，要保障安全，晚上就尽量不要出门，以避免被人打劫；实在要出门，带个防身工具，如棒球棍，也可以减缓被人打劫的风险；最好几个人一起出门，可以在被人打劫的时候转移风险；最后依然有风险，但觉得风险可控，就出门吧。

因为安全产品对应的风险并不一定发生，这和买商业保险是一样的。因此，制造不安全气氛，到处发布各种安全事件损失以兜售安全产品的现象也会经常发生，这就是"安全"讹诈问题。安全资源的过度配置可能导致"过度"安全，为了保护 1000 元的资产，却需要花 10 000 元的安全产品投资，这是不合理的。分段对风险的评估是配置安全资源的依据，但也要避免因小失大的问题。但是对涉及国家安全的机密数据和文档，其价值是不能用经济利益来衡量的。另外，人是整个安全保障体系中最重要的环节，因此即使进行了安全投资，也要在管理等其他人为因素上多下工夫，确保排除人为因素带来的安全隐患。

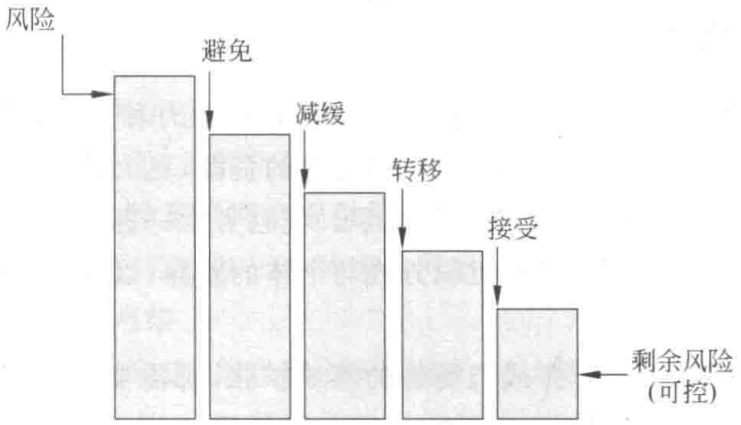

图 1.1　风险控制模型

1.3　网络的本质

1.3.1　网络的定义

任何多个相关的个体都可连成网络，网络(Network)是被联网(Networking)的结果。哲学讲万事万物都是有联系的，是因为任何事物都不会无缘无故产生、发展和消亡，总是处于联系之中。这个联系就是网络。

个体可以小到原子，大到社会组织、宇宙天体。每个网络都有其特定的功能。基因调节网、神经网络、大脑网络、新陈代谢网络、知识表述语义网、电网、交通网、物流运输网、经济网络、社会网络等，这些网络可以处理、存储、传递和接收能量、物质等广义的信息。网络是群体结构，其实，任何事情的发展都是网络的或者说是社会的。几乎没有单独的不受任何影响，也不影响任何其他个体的独立事件，所有事件必是某网络中的一个事件。

大规模的网络系统一直是大自然的奇迹，更是人类的伟大发明。

宽广的长江流域，在重力与地貌影响下，小河汇聚成支流，支流汇聚成主干，最后形成大江，奔向大海大洋，蔚为壮观。

纵横交错的灌溉网络，是劳动人民的智慧，将水资源运输、供给、调配到不同的地方，浇灌了农作物，生产了所需的农产品，养育了各族人民。

雄伟的长城，最初是秦朝将战国时代各国分散的、各自修建的城墙连接起来，形成的统一的连通的工程，借以统一部署，快速调动防御力量，抵御外族入侵。

庞大的高速铁路与高速公路，四通八达，纵贯东西南北，穿隧道，过大江，形成快捷的国家交通网络。

便利的地铁网络，在地下修建，穿沟走壑，可以从一地，转乘到达另外地点，形成快捷的城市交通网络。

1.3.2 网络的意义

大自然的网络化系统和人造的网络化系统，其推动力和目标是不同的。人造网络系统扩张的原动力更在于人的欲求，能获得更多的资源，更大的能力。

网络系统扩张的外在推动力来自于竞争。优胜劣汰一直是大自然和人类社会的基本法则。社会是由人组织而成的，组织方式与个体的差异，以及组织的目标与使命有很大的关系。

资源总是有限的，系统扩张或抗衡别的系统扩张，都需要竞争资源，增强能力。将所占领的资源并入其中，吸纳新的能力。

单个组织及个人的资源和能力也是有限的，往往在竞争中处于劣势。需要互相之间共享资源，互相之间补充能力。

联网，将分散资源或者系统连接起来，达到系统资源聚集，增强能力，是系统扩张、竞争资源的基本方式。

1.3.3 通信网络

通信网络是传递信息内容的网络。作为人类语音通信的电话网络早就存在（自 Alexandra Graham Bell 发明电话始，有 100 多年的历史），其他如电报网络也有很长的历史。3G 和 4G 无线网络的兴起，将无线数据通信进一步发展到普适的地步，传统通信网络运营商为互联网接入提供丰富带宽以后，这些运营商在提供通道的同时，目前也在大力开发内容，以提高网络的“黏性”。

1.4 计算机网络的本质

1.4.1 网络的本质与功能

传统的通信网络负责信息传输和交换，通信网络运营商主要是作为信息的通道商，收取交通费用，并不提供内容，如电信网络、X.25 数据网络等。从 1946 年电子计算机的出现，将计算机系统连接起来的共享计算/存储等资源的需求，是计算机网络产生的直接原因。另外，通信网络也转为全数字化并计算机自动控制。

计算机通过计算机网络来完成信息的交换。计算机网络由路由器和通信链路组成。计算机网络通过网络设备将独立异构的计算机系统连接起来，完成计算机系统之间的资源共享。计算机网络要解决的一个核心问题是需要定义一套原语（Primitive），即通信协议（如当前互联网采用的 TCP/IP），让不同的异构计算机之间能够交换数据。此外，计算机网络要研究如何有效地连接计算机系统，因此需要光通信等通信技术作为基础。通信技术的革命为计算机网络的普及打下了基础。

这种网络的节点是计算机，边是传输层或应用层的各种连接。从信息的角度看，计算机网络完成信息的各种传递。计算机和人的最大不同是计算机没有自我意识，因此

信息对计算机的影响并不改变计算机的行为目的，虽然计算机可以协作和分工完成一些事情，也可以学习，但仍然是机械的，而不是具有自我意识的。

计算机网络的典型例子有 Internet、P2P、CDN 等，它们是全互联的或全连通的。为了完成各种信息处理任务，计算机网络也许把信息传递的任务交给通信网络来完成，也就是说通信网络可以为计算机网络提供信息传递服务。但计算机网络完成的任务和通信网络是没有关系的，它可以基于各种通信网络，比如 IP 网、电话网等。只是在考虑效率时，才考虑下层通信网络。

随着通信技术的突飞猛进，信息通信的通道价值日益降低，而通信内容的价值比较高。互联网最吸引人的是 Web 内容和各种音视频等，互联网提供了丰富的内容，逐渐取代了一些传统的媒体形态，因此互联网已不再单纯是作为网络存在，而是作为一种新的内容发布与获取的场所而存在。

除了狭义的信息网络外，还有广义的信息网络，如计算机网络是用来获取和发表信息的工具。目前互联网是基于端到端原则，计算与通信还是基本分离的，图 1.2 给出了实际的互联网结构图。由互联网运营商将各局域网与终端接入骨干网(Backbone)。

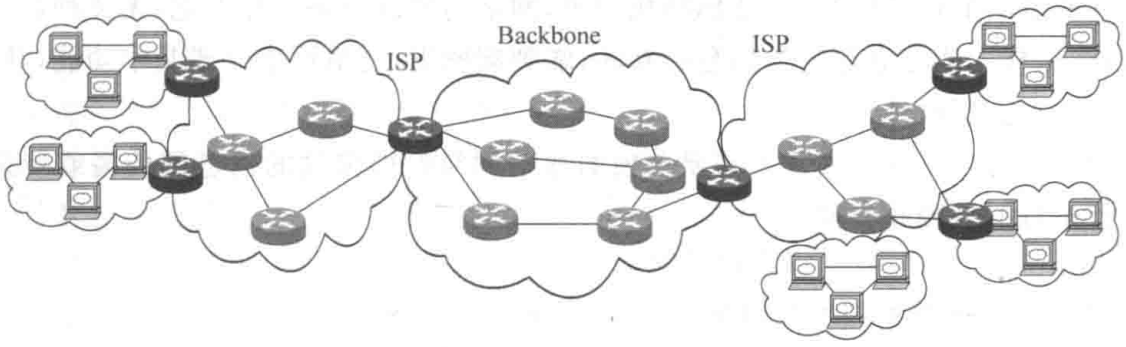

图 1.2　实际的互联网结构图

计算机及其信息网络始终是人的代理、人的工具，开始帮助人处理信息、传递信息、存储信息、发布和获取信息。当前网络中的每一个事件都基于个体目的，比如我要信息(内容获取)，我们要发布信息(内容发布)，我要通信，我要处理(服务)等。包括 CDN 也是为个体服务的。但是，从更高层面看，无数个体在达到自己利益目标的同时，其实也是在帮助别人，回馈社会，这一点非常类似经济学知识，因此有网络经济学这门学科。

1.4.2　网络设计

设计 P2P 网络系统的人，并不想让计算机网络控制在某些人手中，转发权的垄断意味着没有竞争。P2P 思想，人人皆有转发权是网络创新的根本。

现有的 Internet、电话网以及正在兴起的信息中心网络，都是为满足人们的某些需求而设计的，而不是根据网络本身的自然原理设计的。目前尚没有网络应该是什么样的理论。因此网络的设计取决于基本需求的确定和设计原则的确定。

观察历史上的通信网络，其演化的动力始终是人们的需求。比如会话的需求、抗核打击的需求、内容发布与检索和存取的需求(如 HTTP、Search Engine、Web、P2P、