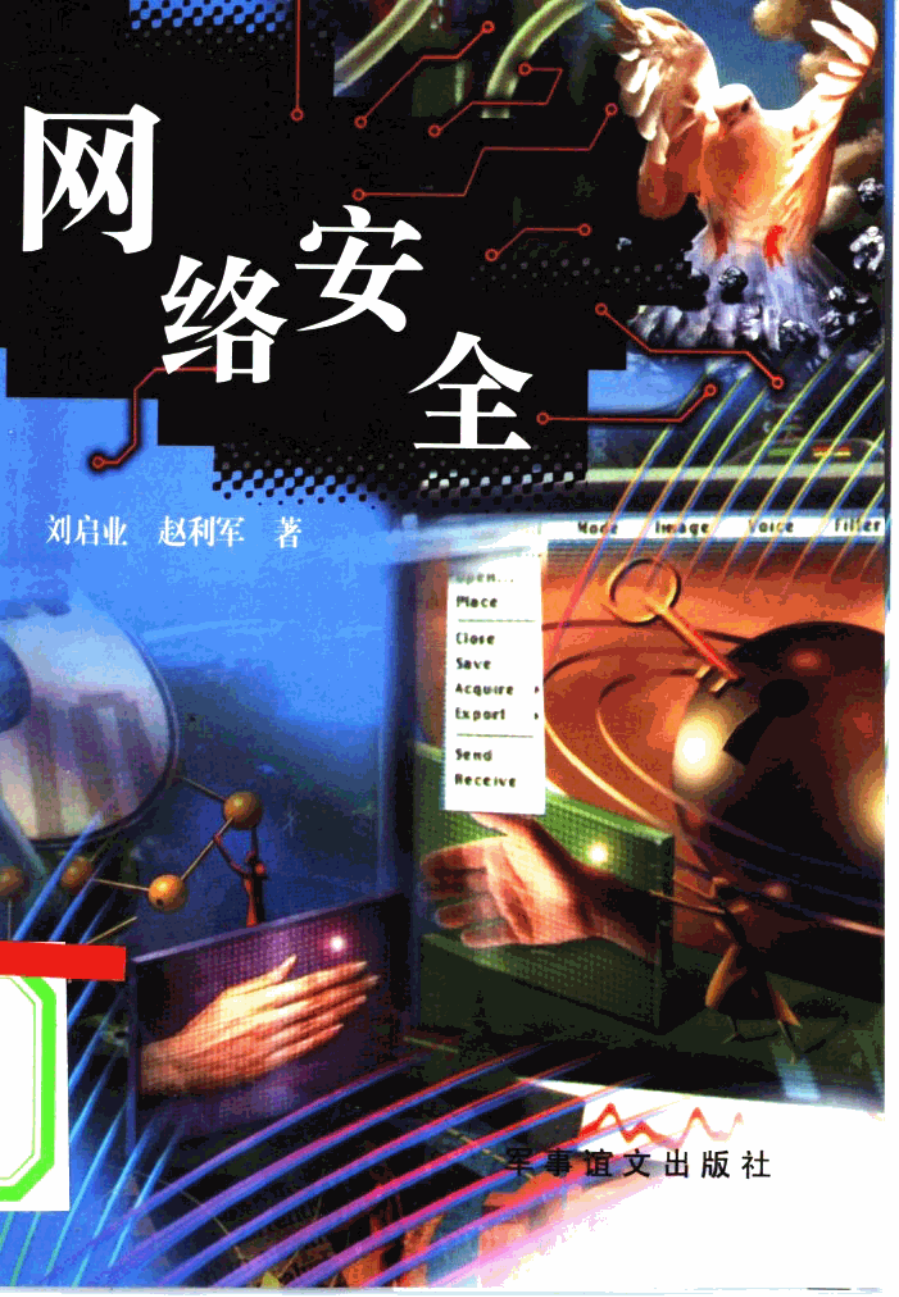
# 网络安全

刘启业　赵利军　著




军事谊文出版社


人类文明已经进入了21世纪，社会发展在经历了农业时代，工业时代之后，现在开始走入信息时代。在农业时代，人们以土地为生存的根本，靠简陋的或单一的生产工具维系生命的繁衍。那时，人们虽然也使用信息，但是并没有意识到信息的深层含义和潜在的力量。在不同地区生活的人们可能一辈子也互不了解，更谈不上进行信息的交流。到了工业时代，产生了以蒸气机为代表的机器制造业，再加上电的发明和应用，使人类向前跨进了一大步。机器扩大了人的认知和活动范围，信息的作用也随着这种扩大而开始被人们重视，工业时代人们开始关心自身周围的社区、国家乃至世界上的事物，这代表了人们对信息作用的认同。即便是这样，在工业时代信息的重要也没有达到今天这样的程度，信息还不能作为一种独立的财富在社会上进行经济活动。对于社会而言，信息似乎没有表现出其独立存在的价值。信息被利用完之后大部分被搁置了，甚至被遗忘了，至于

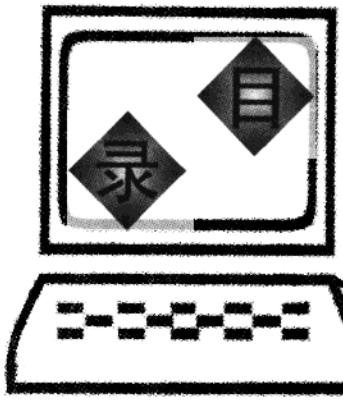
这些信息之间具有什么样的联系？怎样进行二次利用，则较少有人问津。

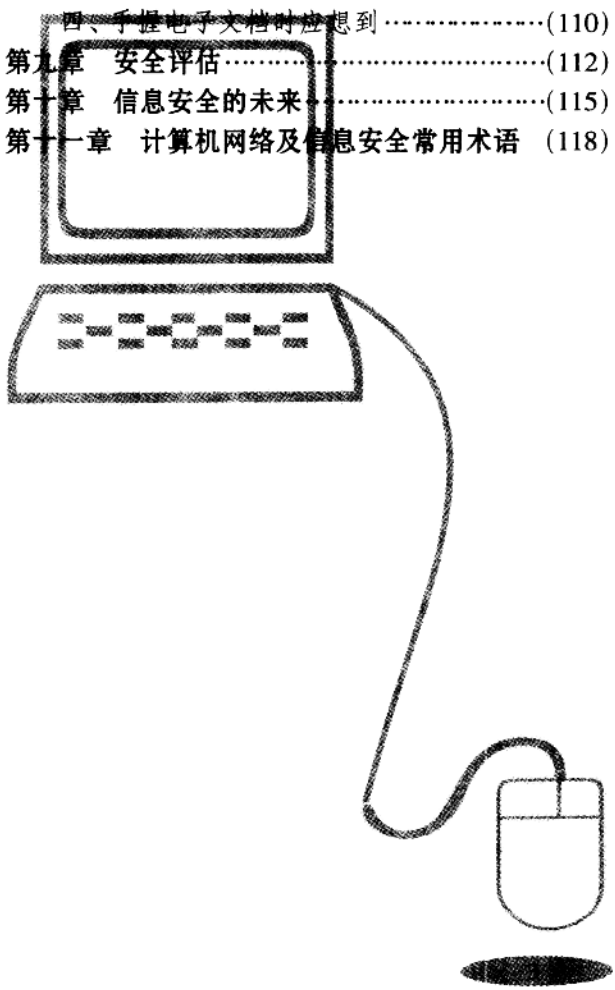
当社会发展到20世纪末，人们突然从某个时刻发现我们周围的一切都变了，传统的行业不再引人注目，自己身边的一切都被计算机包围着，仿佛人们庆祝节日，在一夜之间都换了新装。传统的东西逐渐不时髦了，人们更关注信息行业和产业的发展，特别是以计算机网络为主流的信息行业出尽了风头，电报电话、商业购物、家庭办公、电子邮件、影视娱乐、甚至电视等，各种预测都表明：一个以信息为资源的信息产业正在兴起，信息逐渐成为一种社会财富、其产生价值被全体社会所共识。

信息时代为人们带来了前所未有的好处，他使你坐在家中就可以知道和看到天下事，不需要到邮局就可以通过电脑将你要说的话直接发送给你的朋友，家庭办公在一些行业已经成为可能，从网上每个人都可以获得大量的信息为自己的生活和工作服务。在发达国家网上购物已经开始普及，网上看电视在不远的将来便可以实现。在网上上大学，学习各种知识，爱好游戏的朋友还可以在网络上玩各种游戏等等，等等。网络时代为人们带来的利益太多了，面对这样的世界我们似乎感觉有些手忙脚乱。各种新的技术不断诞生，各种新的，不论是生产的还是管理

的，或是军事的结构不断形成，适应和变革成了这个时代的特征。然而，就在人们埋头研究和发展信息技术的时候，计算机病毒、计算机黑客、计算机犯罪的出现使人们开始思考一些新的问题：信息时代我们还能安全地生活吗？我们的隐私还能得到有利的保护吗？我们的信息财富是否会轻易地被摧毁呢？安全转眼之间成了信息时代最重要的事情。怎样防止计算机犯罪，怎样防止计算机病毒，怎样防止黑客的攻击，怎样保护我们的隐私，各个方面的人士开始研究和介绍信息安全技术和知识，解决信息安全问题，勾画未来信息时代的安全框架。本书就是在这样的大环境下编写的，针对多数非专业人员关心的计算机网络和安全问题进行了介绍和探讨，书中分别讨论了计算机信息安全、硬件环境安全、软件安全、综合性安全、管理层的安全、安全问题的变革、信息社会中的安全思维等诸多问题，旨在帮助非专业人员了解安全领域中相关各个方面的知识，建立安全意识，把握安全的衡量准则，最终提高信息系统的整体水平。

本书主要由刘启业、赵利军编著，在出版的过程中得到了军事谊文出版社总编王启明同志的大力支持，借此机会表示衷心感谢。由于我们水平有限，书中内容和观点难免有误，希望读者批评指正。





# 第一章　网络简述

这一章主要讲了计算机网络的含义、有关网络的分类以及使用计算机网络所带来的诸多问题。

## 一、什么是计算机网络?

在具体谈到计算机网络的含义之前，我们将分别介绍计算机发展简史;早期使用计算机的模式:从单道程序模式到多道程序的实现，以及多用户的分时终端方式。其中还介绍了计算机体系结构中对这些使用模式起重要作用的虚拟存储器和中断的功能。

### 1. 计算机发展简史

自从 1946 年第一台电子计算机 ENAIC 诞生以来，半个多世纪过去了，计算机技术飞速发展，取得了令人可喜的成果，今后仍将取得新的巨大成就。

计算机发展到今天，其硬件部分所用的器件已经历了四代的发展:

第一代（40～50年代）：采用电子管作为主要元件，用绝缘导线互相连接。寿命短、可靠性差。

第二代（50～60年代）：采用分立的晶体管为主要元件，安装在单面或双面印刷电路版上。内存储器广泛地使用磁芯，整机的寿命和可靠性都比第一代高。

第三代（60～70年代）：采用小规模集成电路（SSI）和中规模集成电路（MSI）作为主要元器件，安装在多层印刷电路版上，开始用半导体存储器代替磁芯存储器，在体系结构上，对高速缓存、主存和外存统一编地址，用硬件来实现各级存储器间的自动调度，这就是虚拟存储器。

第四代（70～80年代）：采用大规模集成电路（LSI）和超大规模集成电路（VLSI）作为主要元器件，这期间由于使用了高密度组装，整机的体积大为缩小，运算速度和存储容量都大为提高。

在计算机硬件发展史上，把晶体管电路集成到硅芯片上的技术，对计算机的发展起到了举足轻重的作用。1965年，摩尔先生观察到一种奇怪而有趣的现象：即集成电路上可容纳的元器件数量，每隔一年半左右就会翻一番，性能也提高了一倍，因而发表了著名的摩尔定律，并大胆预测未来这

种增长仍会延续下去。30 多年来，集成电路的发展就是遵循这条定律进行的。现在已有主频为 1500 兆赫兹的集成电路上市，即最快速度为每秒 15 亿条指令，这就意味着 1992 年我国研制成功的 10 亿次/秒银河Ⅱ计算机，如今只要一个芯片就能实现其计算能力。过去占地上百平方米的计算机，如今已能压缩成笔记本电脑或掌上电脑。也省却了庞大的电源空调系统。在第一代计算机，为了使功耗数百千瓦的机房保持在 25℃（±1℃），湿度为 50%（±10%）的环境条件，必须设置空调系统，而空调系统一开，感觉简直是地动山摇。但如今的笔记本计算机，只需一个微型小风扇就解决了问题。技术的进步，真是令人难以想像。

计算机的软件系统，从程序设计所用的语言方面来看，经历了机器代码语言、汇编语言和高级程序设计语言阶段，现在已发展到更高级的模块化和可视化程序设计语言。

2. **早期使用计算机的模式**

(1)单道程序模式。早期的计算中心，都有一台或数台大型计算机，为了充分利用这些计算机，一般都是 24 小时开机，并设有专门人员，负责分配各个用户的用机时间。调整程序的用户，一般分配 15 分钟左右的上机时间。一旦程序调好后，再根据题

目运算量的大小，向计算机时间分配人员申请数个小时的上机时间，经同意后按约定的时间到机房上机。当分配的时间用完后，必须立即把机器的使用权交给等待上机的下一个用户。总之，这种使用计算机模式的主要特点是单个用户、单道程序独占全部资源：即运算器、主存储器和所有的外围设备均为单个用户占用。

(2) 虚拟存储器。众所周知，计算机内存的存取速度快，容量相对于外存较小，而外存容量一般要大于内存几个数量级，但存取的速度慢。用户程序只能直接从内存储器取数进行运算，一旦用到外存储器中的数据，编程人员必需编出把数据从外存调到内存中的指令，操作非常麻烦且容易出错。因而在1959年，英国人在其研制的Atlas计算机中引入并实现了一级存储器的概念——物理上虽有内外存之分，但由于将内外存统一编址，且由硬件来自动实现外存和内存间数据的调度，因而用户从逻辑上看就认为整个外存都可当内存使用来编程了。大概在60年代中期，美国的IBM公司把英国人提出的一级存储器思想用到IBM360和370系统中，并在技术上有所改进，取名为虚拟存储器。至今，“虚拟”一词已被广泛使用。如“虚拟现实”在中国科学技术馆就有演示：观众站在距离约2米的布幕前，可以看到由计算

机控制的排球正向你飞来，当你举手击球时，在听到击球声的同时，你还将在布幕上看到球正按照你手击的方向、击力的大小而运动着，使你感到就像真的在训练场地击球一样。这是因为人手的整个动作过程，已由安装在人背后的摄像机拍下，这些运动的图像转换为数据，并经计算机处理后再控制球受击后的运动速度及轨迹。

(3) 中断的引入。为了提高整个计算机系统的利用率，计算机研制人员提出了中断的概念，并用硬件来实现它。在中断系统控制的基础上，再配合相应的管理程序，从而实现了多道程序。计算机的所谓中断，是指当程序运行中，出现某些事件时（例如要求输入或者输出），则必须中止正在运行的程序，转到指定的处理程序去处理该事件，然后再恢复原运行的程序。为此，必须在内存中分配一些缓冲区，以保留中断时的现场数据。如被中断时的指令计数器和运算器各寄存器的内容等。一般的中断系统都分有若干级，即允许高一级的中断要求可中断低一级的中断运行程序。计算机的中断功能，犹如一个棋盘（相当于运算器），只能供两人对棋。若甲乙两人对棋 15 分钟后，仍未分胜负，此时丙丁两人要求使用棋盘，则甲乙必须让给丙丁。即甲乙被丙丁的要求所中断。但甲乙的残局（即现场）必须记录下来，以便丙丁下完后（或超过

15 分钟仍未分胜负），再把棋盘让给甲乙两人恢复残局，继续未下完的一盘棋。

(4) 多道程序的实现。有了中断系统，就具有实现多道程序的功能。例如当一道程序要求输出一些中间结果的数据，需要花 20 秒的打印时间，这个时间的绝大部分都可以用来调入另一道程序进行运算。早期的机械打印机速度缓慢，打印一行数据至少在毫秒级，而运算器的速度为微秒级（当前已达到毫微秒级），两者相差 3 个数量级。因此一道题目在打印输出的同时，另一道题目已经可以完成很多运算了。

有了中断系统，实时控制才能实现。当用计算机引导地面多部观测设备对飞行中的航天器进行跟踪测控时，对每一部设备的引导就相当于一道程序，它们要求的响应时间一般都是毫秒级（个别人工手动控制的秒级），因而只要计算机的运算速度在 20 万次/秒以上，并有足够的内存容量和接口设备，就能满足这些实时控制的要求的。当然，如果对整个测控精度要求提高时，对计算机的运算速度和容量都会有进一步的要求的。

使用多道程序的解题模式，用户不一定自始至终在机房等待运算结果，机器时间的分配也可相对灵活一些。

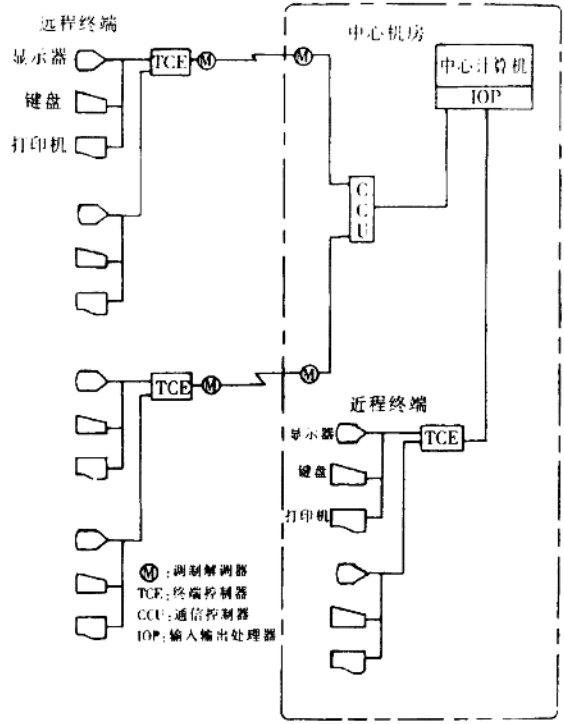



图 1　典型的计算机中心及终端系统图

(5) 从多道程序到多用户分时终端方式。通过

为几十台以至数百台近远程终端机来共享计算机的资源，乃是多道程序的进一步发展。近程终端机（离主机几百米）一般都配有输入键盘、显示器、打印机。而远程终端机（离主机几十以至几千公里）除与近程的配置相同外，必须另加调制解调器和申请专用的通信线路，才能和主机连接。这些用户终端机没有任何计算能力，它仅仅是一个简单的输入输出设备，即用户可以直接从终端键盘上输入要运算题目的程序和数据，而主机将定时轮流询问开机的各台终端，如发现有输入、输出、或运算的请求时，便快速响应，并给出一定的时间片来完成该请求。分时终端方式的引入，使得数百个用户可同时使用一台计算机，用户不必进入机房，就可通过终端调试程序，提交题目，中心计算机的运算结果，可以返回到相应终端的显示器或打印机上。

3. **什么是计算机网络?**

建立计算机网络的目的。上述的各种使用计算机模式，即使是面向多台终端的计算机中心，也并未构成网络。因而人们自然而然地会想到：如果从硬件上把多个计算中心、多台计算机连接起来，并配上相应的软件，使多台计算机组成一个有机的整体，而用户的题目，可以根据其规模，自动地分配到不同的机器上运算，那该有多好。例如，最近美国科学家披露，

在破解人类基因密码的伟大工程中，为了完成基因排序，他们曾用了700台计算机互联进行处理，整个系统达每秒1.3万亿次浮点运算，每台计算机的主处理器是由64位的Alpha芯片组成的。建立计算机网络的目的，就是使得每一台计算机的本地资源都能为连接到该网络上的任一台计算机所利用。

实现网络的难点。可以想到，不同的地理位置，不同型号的计算机联在一起，必然会碰到一系列的计算机硬软件问题和通信问题等。整个20世纪60～70年代，许多计算机的研究人员都在探讨这些课题。1975年底，我们曾就计算机网络的发展趋势及技术难点同一位美籍华人计算机教授进行了座谈，他认为：这是很难实现的事，因为各个计算机的指令系统和编码都不一样，如何能互相理解？就如上海人讲上海话，广东人讲粤语，北京人讲普通话，各人只会本地的语言，大家凑在一起时很难通过语言来沟通的。在当时的硬软件技术发展水平下，教授的话，无疑是有一定道理的。

计算机网络是什么？从硬件方面看，就是依靠通信线路连接起来的一组计算机及相关的设备，这些线路可以通过一般的双绞线、电缆或光纤，建立永久性的连接；也可以通过电话或其他通信线路建立暂时性的连接。除了硬件支持外，还要有软件方面的相

应支持，如数据链路控制、传输控制、数据流控制等，这样才能实现网络的功能。

通信子网的拓扑结构。计算机网络从逻辑功能上看，可以分为两个子网，即计算机资源子网和通信子网。资源子网前面介绍了许多，它的主要任务是提供资源共享所需的计算机硬软件及数据处理的能力。而通信子网主要功能是完成数据的传输、交换及通信控制，为计算机网络的通信功能提供服务。它由网络节点、通信链路和信号变换器（如 Modem）等组成。

通信子网的拓扑结构，按相互连接结构分为星形网、树形网、环形网、星环网等。

①星形网：在这种结构中，中央站点——即中心服务器与每一个终端节点（最终用户）之间都只有一条通路。星形网的特点是终端节点的异常不会影响整个网络系统的运行，但若中心站点异常将导致整个系统的停机，所以有些重要的网络系统其中心服务器都采用多台并行工作，互为备份，并可自动地实现热切换。

②树形网：指的是两个网络节点之间只有一个信息通路，或者是一种分级的集中式网络。

③环形网：这种网络结构形式表现为每个节点计算机都有通路与相邻的两个节点相连，从而形成