保密技术知识读本

国际互联网安全保密知识

王昌禄　主编

金城出版社

保密技术知识读本

国际互联网安全保密知识

主编　王昌禄

金城出版社

图书在版编目(CIP)数据

国际互联网安全保密知识/王昌禄主编. －北京：金城出版社,2001.4
ISBN 7－80084－340－8

Ⅰ.国… Ⅱ.王… Ⅲ.因特网－安全技术 Ⅳ.TP393.48

中国版本图书馆 CIP 数据核字(2001)第 11945 号

金城出版社出版发行
(北京市朝阳区和平街 11 区 37 号楼 100013)
世界知识印刷厂印刷
850×1168 毫米 1/32 9 印张 220 千字
2001 年 4 月第 1 版 2001 年 4 月第 1 次印刷
印数：1—5000 册
ISBN 7－80084－340－8/T·10
定价：15.00 元

主　编　王昌禄

编　者　王昌禄　林南英　夏连海
　　翟国栋　王玉平　严升明
　　郑晓雯　刘晓辉　蒋小平
　　曾　钢　田　欣　王沈沛

前　言

近年来，国际互联网迅速在全球发展，千百万人上网，参加了网络的各种活动。因此如何保障在网络传输过程中的安全性十分重要。网络安全问题，既是一个复杂的技术问题，又是一个重要的管理问题。因此国际互联网的保密方法的研究是一个十分重要课题。

利用互联网实施违法犯罪活动，我国将立法予以惩处。全国人大常委会第十八次会议就关于维护网络安全和信息安全的决定草案，国务院法制办负责人作了说明。

草案规定，有以下违法犯罪活动者，将依照刑法有关规定追究刑事责任：

违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统；

制作、传播计算机病毒，设置破坏程序，攻击计算机系统及通信网络，致使计算机系统及通信网络遭受损害；

擅自中断计算机网络或者通信服务，造成计算机网络或者通信系统不能正常运行；

利用互联网造谣、诽谤或者发表、传播其他信息，煽动颠覆国家政权、推翻社会主义制度，或者煽动分裂国家、破坏国家统一；

利用互联网窃取、泄露国家秘密、情报或者军事秘密；

利用互联网煽动民族仇恨、民族歧视，破坏民族团结；

利用互联网组织邪教组织、联络邪教组织成员，破坏国家法律、行政法规实施；

利用互联网进行诈骗、盗窃；

利用互联网销售伪劣产品或者对商品、服务作虚假宣传；

利用互联网编造并传播影响证券和期货交易的虚假信息；

在互联网上建立淫秽网站、网页，链接淫秽站点，提供淫秽站点链接服务，或者传播淫秽书刊、影片、音像、图片；

利用互联网侮辱他人或者捏造事实诽谤他人；

非法截获、篡改、删除他人电子邮件或者其他数据资料，侵犯公民通信自由和通信秘密；

利用互联网侵犯他人知识产权；

利用互联网损害他人商业信誉和商品信誉。

编者考虑到保密工作者、广大网络专业工作者及网络爱好者的需要，参考了有关资料编写了《国际互联网安全保密知识》一书。

本书在第一章较详细介绍了国际互联网的基础知识，如网络类型、分类、网络的协议及国际互联网使用方法等内容。第二章介绍了网络安全的重要性，如安全分级、网络安全方法等。第三章介绍了加密方法，为了保证网络安全，加密是重要手段。本章介绍了加密基础、方法

及加密工具。用防火墙解决网络安全是当今重要手段，故在第四章介绍了防火墙概念及技术。第五章介绍了防火墙类型、结构及选择原则方法。在第六章介绍了几种典型防火产品供读者参考。在第七章较详细介绍了在网络各个环节中的保密方法，如 Web 站、在发 E－mail 过程中，以及如何对付“黑客”等方法。病毒对网络的安全也是重要的威胁，因此第八章介绍了网络的病毒防治方法。最后第九章简介了因特网新的安全标准。附录介绍了有关计算机安全法规。

全书简明扼要、语言流畅、通俗易懂，做到深入浅出。适用于保密工作者、广大网络专业工作者及网络爱好者阅读参考。

本书编写分工如下：第一、二、三章由王昌禄、林南美、夏连海编写，第四、五章由翟国栋、王玉平、严升明编写，第六、七章由郑晓雯、刘晓辉、蒋小平编写，第八、九章及附录由曾钢、田欣、王沈沛编写，全书最后由王昌禄统稿并审核。

编者

2001 年 2 月

责任编辑：苏　雷
孙德全
封面设计：顾　华

目　录

第一章　国际互联网基础知识

第一节　网络的基本概念

一、计算机网络

计算机及其应用技术不断发展，为了使计算机之间能够交换信息数据，资源共享，则需要将它们之间互相联系起来，才能实现上述目的。

计算机网络是一种地理上分散的，具有独立功能的多台计算机，通过通信设备和线路联接，并配有相关的网络软件，以实现资源共享的系统。

在网络中，用户必须明确地指定在哪台机器上登录，明确地指定远程递交任务，明确地指定文件传输源和目的地。

二、计算机网络的主要功能

1. 发送电子邮件

计算机网络允许使用电子邮件系统进行复杂的通信和交互服务。例如将一条信息发送给许多接收者，可以发送文字、声音、图像及图形等信息，可以在发送一条信息后，使某台计算机作出响应。

2. 电子公告牌

计算机网络可以实现电子公告牌功能。即允许一个用户加入

到多个讨论小组,讨论某一课题。可以定期检查每个讨论课题中是否有新的内容。在集体讨论中,某一成员发表的新见解,可以供其它成员阅读。某一成员也可以发表对其他成员见解的看法。电子公告牌还可以发表网络新闻,用户可以自由选择新闻订阅。

3. 文件传输(FTP)

计算机网络可以实现将一台计算机中磁盘文件传输到其他计算机磁盘上。而且是高效、快速地拷贝大量的文件。磁盘上的数据是存放在命名文件中,而一些命名文件的集合又形成文件夹或目录。

文件传输服务使用文件传输协议(File Trcmsfer Protocol)简称 FTP,一般用来表示文件传输服务。

FTP 是一个应用程序。当激活 FTP 后,给用户显示提示符,然后等待接收一系列交互命令,完成命令后,即实现文件传输。

4. 远程登录(TELNET)

计算机网络可以实现远程登录服务。它是在普通的分时计算机系统上登录机制的一种扩展。用户成功登录后,远程计算机允许用户通过键盘输入或通过鼠标进行交互。用户可以运行任何命令或激活任何应用程序。

5. 信息浏览服务(Gopher)

信息浏览服务是一种可支持个人用户查找并估量存储于远程计算机上的信息的联机服务类型。信息浏览服务是以交互方式进行。用户可以寻找感兴趣的信息,可以阅读某个远程计算机所存文件信息,检索或打印选定的信息。

第二节　网络的分类

一、概　述

计算机网络种类很多，若按传输技术划分，计算机网络可分为广播式网络和点到点网络；若按网络作用范围分，可分为局域网、城域网和广域网；若按网络数据传输与交换系统所有权划分，分为专用网与公用网；若按交换技术分，分为电路交换网、报文交换网络、分组交换网络等。下面重点介绍几种。

二、常见几种网络

1. 专用网和公用网

专用网是由某个部门或公司组建的网络，不允许其它部门或单位使用。公用网一般由电信部门组建，并由其管理与控制。网络内的传输和交换装置可以对外出租给任何单位使用。

2. 广播式网络和点到点网络

广播式网络：仅有一条通信信道，由网络上所有机器共享。短的信息，按某种数据结构组织分组。可以从任何机器发送到其它所有机器接收。广播系统通常允许在它的地址字段中使用一段特殊代码，以便分组发送到所有目标。这种操作称为广播。

点到点网络：由一对机器之间的多条连接构成。为了能使从源达目的地，这种网络上的分组，必须通过一台或多台中间机器。

一般情况下，小的、地理上处于本地的网络采用广播方式。而大的网络多采用点到点方式。

3. 局域网(Local area network)

局域网又简称 LAN，它适用的地理范围一般在 10 公里以内。属于单位专用网性质。用于连接单位内部计算机资源，共享信息、

交换信息。

局域网使用的传输技术是用一条电缆连接所有机器。其特点是组建方便、灵活，局域网也可以连接到广域网或公用网上。用户可以享受外部网上提供的资源。

4．城域网(Metropolitan area network)

城域网简称 MAN，它是一种大型网络，使用的是与局域网相似的技术，它可覆盖一个城市，可以是专用的也可以是公用的。其传输速率通常在 10Mbps 以上，作用距离为 5～50km。城域网可以支持数据和声音传输，仅使用一条或两条电缆，不包含交换单元。城域网重要的特点是使用了两条单向总线，所有的计算机都连接在上面。

5．广域网(Wide area network)

广域网又简称 WAN，是一种跨越大的地域的网络。通常覆盖一个国家。网络上的计算机称为主机(host)，又名端点系统(end system)。主机通过通信子网连接，通信子网的功能把信息从一台主机传送到另一台主机。通信子网由两个不同部件组成，即传输线和交换单元。传输线也称为线路、通道。交换单元是一种特殊计算机，用于连接两条以及多条传输线。

第三节　网络的兼容问题

一、网络兼容问题

各种局域网(LAN)不能互相连在一起，例如企业或公司内部有两个局域网(LAN)，一个在运输部门一个在会计部门，不能将多个局网连在一起。有技术上原因：例如特定的局域网，只能在有限距离内使用。因为规定了电缆的最大长度，例如有技术规定不能超过 500M，超距离后可能工作不正常。又如每种局域网的电

压、频率等都有自己的规范。此外每种技术都有自己的信息编码方法。

二、广域网(WAN)与局域网(LAN)互不兼容

首先研究人员开发出多种广域网(WAN)技术,每一种有自己独特设计,在可靠性及速率、距离等方面互不相同。每种网在技术上不兼容,使用自己的信号电压,以及信号调制技术。以致大多数局域网在电信号方面不兼容。不能通过简单插拨到另一种广域网中去。这样不能将若干广域网(WAN)组成更大网络。

其次一个问题是 WAN 与 LAN 之间在电信号上也不兼容,导致它们之间隔离。

20 世纪 60 年代美国国防部对计算机网络产生兴趣,通过高级研究计划署 ARPA(Adranced Research Projects Agency)向军队投资进行多种技术联网的研究。20 世纪 70 年代末 ARPA 已有几个计算机网在运行。其中一个称为 ARPANET 的广域网和使用卫星和无线电传输进行的通信网络。

ARPA 研究计划中,一个重要思想是研究一种方法及局域网(LAN)与广域网(WAN)互相连接起来,使它成为网际网(internetwork),有时缩写为 Internet。中心思想是希望研究出一种网络之间连接方法。

第四节　网络的协议

一、概　述

在设计网络时硬件与软件是一整体,需统一考虑。为了减少网络设计复杂性,必须分层考虑,并使其符合协议和标准。一般硬件处于网络低层,软件处于高层。

(一)协议分层

为了解决网络设计复杂性,一般网络都是按层(layer)或级(level)的方式来组织,每一层都建立在下层之上。一般不同网络,其层的数量和名字、内容、功能不尽相同。

协议基本上是通信双方关于通信如何进行达成的一致规则。n层的协议层次结构图如图1—1所示:

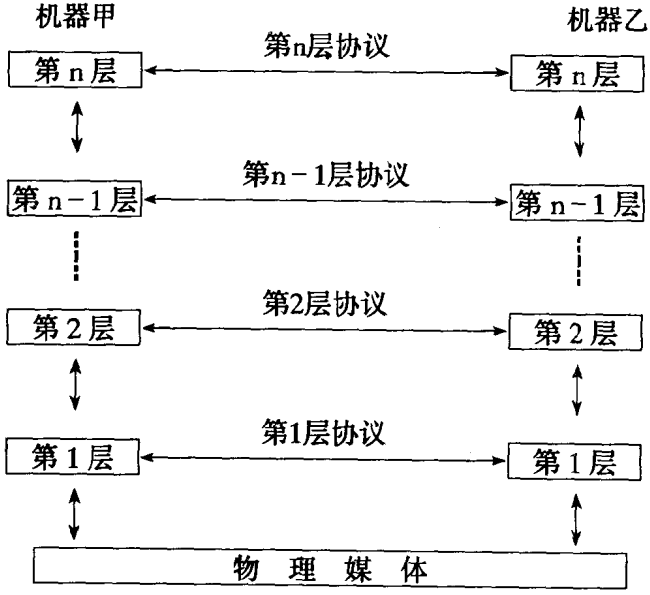

图1—1 协议层次结构图

第1层下面是物理媒体,它进行实际通信。每一对相邻层之间都有一个接口,接口定义下层向上层提供的原语操作和服务。

层和协议的结合称为网络体系结构。体系结构的描述必须包含足够的信息,可以用来为每一层编写程序和设计硬件,并使之符合有关协议。

(二)接口和服务