第3章 计算机网络与信息安全

学习目标

- 理解计算机网络基础知识的概念
- 熟练掌握浏览器的使用和计算机网络资源的使用
- 理解信息安全的定义
- 理解数据加密、数字签名、数字证书的概念
- 理解防火墙的概念
- 熟练掌握计算机病毒预防和消除的方法

计算机网络是现代计算机技术与通信技术密切结合的产物，在当今信息时代，社会对信息共享和信息传递的日益增强，网络已经成为信息社会的命脉，计算机网络日益成为现代社会中各行业不可或缺的一部分。计算机网络技术为信息的获取和利用提供了越来越先进的手段，同时也为好奇者和入侵者打开了方便之门，于是信息安全问题也越来越受关注。网络和信息传播途径有诸多不安全因素，信息文明还面临着诸多威胁和风险。个人担心隐私泄露，企业和组织担心商业秘密被窃取或重要数据被盗，政府部门担心国家机密信息泄露。信息系统的安全不仅关系到金融、商业、政府部门的正常运作、更关系到军事和国家的安全。信息安全已成为国家、政府、部门、组织、个人都必须重视的问题。

本章首先介绍计算机网络的基础和计算机网络资源的使用，再介绍 IE 浏览器的使用方法，最后介绍信息安全、计算机病毒的防治方法与防火墙的基础知识。

3.1 计算机网络简介

计算机网络是利用通信设备和线路将地理位置不同的、功能独立的多个计算机系统互连起来，以功能完善的网络软件（即网络通信协议、信息交换方式和网络操作系统等）实现网络中资源共享和信息传递的系统。

3.1.1 计算机网络的形成与发展

计算机网络从形成、发展到广泛应用经历六十多年，是由简单到复杂、由低级到高级的发展过程。

1. 计算机网络的发展过程

计算机网络的发展历史大致可以划分为四个阶段。

第一阶段是面向终端的计算机通信网络。1954 年伴随着终端的出现，人们将地理位置分散的多个终端通信线路连接到一台中心计算机上，用户可以在自己的终端上输入程序和数据，通过通信线路传送到中心计算机，通过分时访问技术使用资源进行信息处理，处理结果再通过通信线路回送到用户终端显示或通过打印机打印。


计算机网络

第二阶段是以通信子网为中心的计算机网络。1968 年 12 月，美国国防高级研究计划署(Advanced Research Projects Agency，ARPA)的计算机分组交换网 ARPANET 投入运行，它标志着计算机网络的发展进入了一个新纪元。ARPANET 也使得计算机网络的概念发生了根本性的变化。用户不但共享通信子网资源，还可以共享用户资源子网丰富的硬件和软件资源。

第三阶段是网络体系结构和网络协议的开放式标准化阶段。国际标准化组织(International Standard Organization，ISO)的计算机与信息处理标准化技术委员会 TC87 成立了一个专门研究此问题的分委员会，研究网络体系结构和网络协议国际标准化问题。

第四阶段是 Internet 时代。进入 20 世纪 80 年代，计算机技术、通信技术以及建立在计算机和网络技术基础上的计算机网络技术得到了迅猛的发展，因特网作为覆盖全球的信息基础设施之一，已经成为人类最重要的、最大的知识宝库。互联、高速、智能的计算机网络正成为最新一代的计算机网络的发展方向。

2. 计算机网络的功能

计算机网络使计算机的作用超越了时间和空间的限制，对人们的生活产生着越来越深远的影响。当前计算机网络主要具有以下功能。

1) 计算机通信

使不同地区的网络用户可通过网络进行对话，实现终端与计算机、计算机与计算机之间可互相交换数据和信息。

2) 资源共享

凡是入网用户均能享受网络中各个计算机系统的全部或部分软件、硬件和数据资源，为最本质的功能。

3) 分布式处理

将一个复杂的任务分解，然后放在多台计算机上进行处理，降低软件设计的复杂性，提高效率降低成本。

4) 负载分担

当网络中某一局部负荷过重时，可将某些任务传送给其他的计算机去处理，以均匀负载。

5) 集中管理

对地理位置上分散的组织和部门，通过计算机网络实现集中管理。


计算机网络功能

3. 计算机网络的分类

计算机网络类型的划分方法有许多种，IEEE(国际电子电气工程师协会)根据计算机网络覆盖区域大小，将计算机网络划分为局域网(Local Area Network，LAN)、城域网

(Metropolitan Area Network,MAN)和广域网(Wide Area Network,WAN)3 种。

1) 局域网

局域网指覆盖在较小的局部区域范围内,将内部的计算机、外部设备互联构成的计算机网络。一般较常见于一个房间、一个办公室、一幢大楼、一个小区、一个学校或者一个企业园区等,覆盖的范围相对较小。局域网有以太网(Ethernet)、令牌环网、光纤分布式接口网络几种类型,最为常见的局域网大多采用以太网标准的以太网。以太网的传输速率为 10Mb/s～10Gb/s。

2) 城域网

城域网的规模局限在一座城市的范围内,一般是一个城市内部的计算机互联构成的城市地区网络。城域网比局域网覆盖的范围更广,连接的计算机更多,可以说是局域网在城市范围内的延伸。在一个城市区域,城域网通常由多个局域网构成。这种网络连接的距离在 10～100km 的区域。

3) 广域网

广域网覆盖的地理范围更广,它一般由不同城市和不同国家的局域网、城域网互联构成。网络覆盖跨越国界、洲界,甚至遍及全球范围。局域网是组成其他两种类型网络的基础,城域网一般都加入了广域网。广域网的典型代表是因特网。

3.1.2 计算机网络体系结构

在研究计算机网络时,分层次的论述有助于清晰地描述和理解复杂的计算机网络系统。ISO(国际标准化组织)定义了网络互连的 7 层框架。遵照这个共同的开放模型,各个网络产品生产厂商就可以开发兼容的网络产品,开放系统互连模型的建立,大大推动了网络通信的发展。

1. OSI 参考模型

计算机网络刚刚出现的时候,很多大型公司都拥有了网络技术,公司内部计算机可以相互连接,可是却不能与其他公司连接,因为没有一个统一的规范。计算机之间相互传输的信息对方不能理解。为使不同计算机厂家的计算机能够互相通信,以便在更大的范围内建立计算机网络,有必要建立一个国际范围的网络体系结构标准。OSI 参考模型将计算机网络划分为 7 层,由下至上依次是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层,如图 3.1 所示。

2. OSI 参考模型各个层次划分遵循原则

(1) 网络中各节点都有相同的层次。
(2) 不同节点的同等层具有相同的功能。
(3) 同一节点内相邻层之间通过接口通信。
(4) 每一层使用下层提供的服务,并向其上层提供服务。
(5) 不同节点的同等层按照协议实现对等层之间的通信。

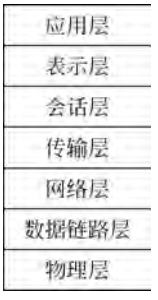

图 3.1 OSI 参考模型

3.1.3　局域网拓扑结构

网络的拓扑结构是抛开网络物理连接来讨论网络系统的连接形式，它反映了网络的整体结构及各模块间的关系，网络中各站点相互连接的方法和形式称为网络拓扑。拓扑图给出网络服务器、工作站的网络配置和相互间的连接，它的结构主要有星状结构、环状结构、总线型结构、树状结构、网状结构等。

1. 星状结构

星状结构是通过中心转发设备向四周连接的链路结构，任何两个普通节点之间都只能通过中心转发设备进行转接。它具有如下优点：结构简单，便于管理；控制简单，便于建网；网络延迟时间较小，传输误差较低。但缺点也是明显的：通信线材消耗较多，成本高，中央节点负载较重，中心转发设备出故障才会引起全网瘫痪，如图 3.2 所示。

2. 环状结构

环状结构由网络中所有节点通过点到点的链路首尾相连形成一个闭合的环，所有的链路都按同一方向围绕着环进行循环传输，信息从一个节点传到另一个节点。特点是：信息流在网络中是沿着固定方向流动的，其传输控制简单，实时性强，但是可靠性差，不便于网络扩充，某个节点出故障就可以破坏全网的通信，如图 3.3 所示。

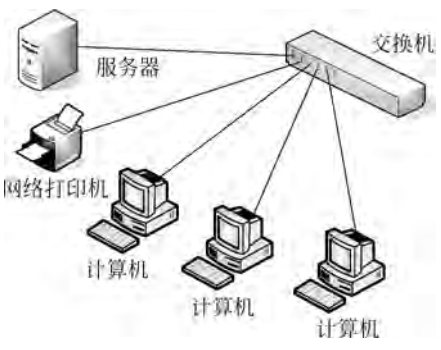

图 3.2　星状结构

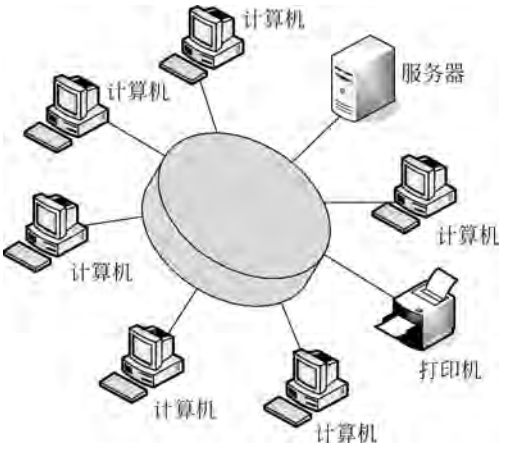

图 3.3　环状结构

3. 总线型结构

总线型结构是指所有接入网络的设备均连接到一条公用通信传输线路上，传输线路上的信息传递总是从发送信息的节点开始向两端扩散。为了防止信号在线路终端发生反射，需要在两端安装终结器。总线型结构的网络优点是结构简单、可充性好、用的电缆少、安装容易。缺点是当其中任何一个连接点发生故障，都会造成全线瘫痪，故障诊断困难、故障隔离困难。一般只被用于计算机数量很少的网络，如图 3.4 所示。

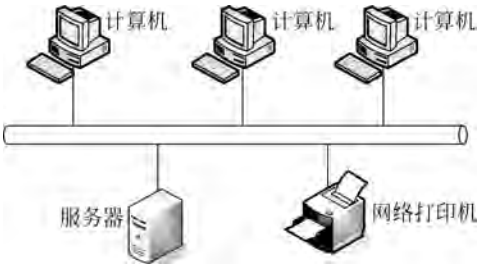

图 3.4　总线型结构

4. 树状结构

树状结构是分级的集中控制式网络,与星状结构相比,它的通信线路总长度短,成本较低,节点易于扩充,寻找路径比较方便,但除了叶节点及其相连的线路外,任意节点或其相连的线路故障都会使系统受到影响,如图 3.5 所示。

5. 网状结构

在网状结构中,网络的每台设备之间均有点到点的链路连接。这种连接安装复杂,成本较高,但系统可靠性高,容错能力强。互联网就是这种网状结构,它将各种结构的局域网连接起来,组成一个大的网络,如图 3.6 所示。

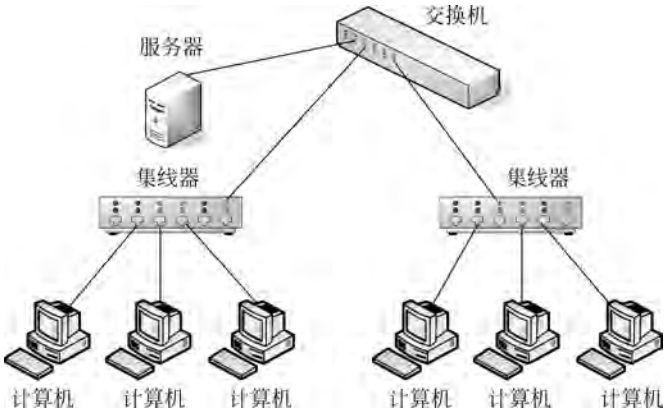

图 3.5　树状结构

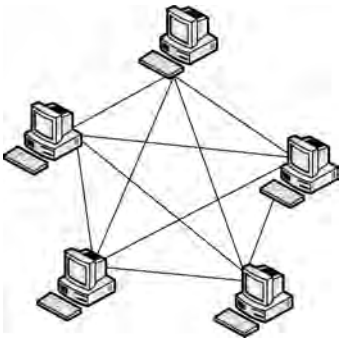

图 3.6　网状结构

以上各种拓扑结构都有其实用价值,对不同的需求采用不同拓扑结构,一个大的网络往往是几种结构的组合使用。

3.1.4　网络协议与 IP 地址

在计算机网络中,两个相互通信的实体处在不同的地理位置,其上的两个进程相互通信,必须对整个通信过程的各个环节制定规则或约定,包括传送信息采用哪种数据交换方式、采用什么样的数据格式来表示数据信息和控制信息、若传输出错则采用哪种差错控制方式、收发双方选用哪种同步方式等,都需要通过按照预先共同约定好的规则进行,这些规则

就是网络协议，不同的计算机之间必须使用相同的网络协议才能进行通信。


计算机网络协议

1. TCP/IP 协议

TCP/IP 协议（Transmission Control Protocol/Internet Protocol）叫作传输控制/网际协议，这个协议是 Internet 国际互联网络的基础。TCP/IP 在计算机网络体系结构中占有非常重要的地位，是 Internet 的核心。TCP 和 IP 是其中最重要的两个协议，即传输控制协议（TCP）和网际协议（IP），现在 TCP/IP 成了一组协议的代名词。它将网络体系结构分为四层，即网络接口层、互联层、传输层和应用层。

2. IP 地址

通过 TCP/IP 协议进行通信的计算机之间，为了确保计算机在网络中能相互识别，每台计算机都必须有一个唯一的标识，即 IP 地址。按照 TCP/IP 协议规定，IP 地址长 32 位，平均分成四段，每段由 8 位二进制数组成，为便于书写，将每段 8 位二进制数用十进制数表示，中间用小数点分开，每组数字介于 0～255，如 192.168.0.1，10.0.0.1 等。IP 地址按网络规模的大小主要可分成三类：A 类地址、B 类地址、C 类地址。

1）A 类 IP 地址

一个 A 类 IP 地址由 1 字节的网络地址和 3 字节主机地址组成，网络地址的最高位必须是“0”，地址范围从 1.0.0.0 到 126.0.0.0。可用的 A 类网络有 126 个，每个网络能容纳 1 亿多个主机。

2）B 类 IP 地址

一个 B 类 IP 地址由 2 字节的网络地址和 2 字节的主机地址组成，网络地址的最高位必须是“10”，地址范围从 128.0.0.0 到 191.255.255.255。可用的 B 类网络有 16 382 个，每个网络能容纳 6 万多个主机。

3）C 类 IP 地址

一个 C 类 IP 地址由 3 字节的网络地址和 1 字节的主机地址组成，网络地址的最高位必须是“110”。范围从 192.0.0.0 到 223.255.255.255。C 类网络可达 209 万余个，每个网络能容纳 254 个主机。

3. 域名

域名（Domain Name）是由一串用点分隔的名字组成的 Internet 上某一台计算机或计算机组的名称，用于在数据传输时标识计算机的电子方位（有时也指地理位置，地理上的域名，指代有行政自主权的一个地方区域）。域名是一个 IP 地址上有“面具”。设置域名的目的是使服务器的地址便于记忆和沟通（如网站、电子邮件、FTP 等）。

网络是基于 TCP/IP 协议进行通信和连接的，每一台主机都有一个唯一的标识固定的 IP 地址，由于 IP 地址是数字标识，使用时难以记忆和书写，因此在 IP 地址的基础上又发展出一种符号化的地址方案，来代替数字型的 IP 地址。每一个符号化的地址都与特定的 IP 地址对应，这样网络上的资源访问起来就容易得多了。这个与网络上的数字型 IP 地址相对应的字符型地址，就被称为域名。以“百度”域名为例，标号“baidu”是这个域名的主域名体，而最后的标号“com”则是该域名的后缀，代表的这是一个 com 国际域名，是顶级域名。

3.2 局域网

局域网(Local Area Network,LAN)是指在某一区域内由多台计算机互联成的计算机组,一般在方圆几千米以内。局域网可以实现文件管理、应用软件共享、打印机共享、工作组内的日程安排、电子邮件和传真通信服务等功能。局域网由网络硬件(包括网络服务器、网络工作站、网络打印机、网卡、网络互联设备等)、网络传输介质及网络软件组成。

3.2.1 局域网的简介

一般把在有限的范围内,彼此之间的距离不太远的外部设备和通信设备互联在一起的网络系统称为局域网。它可以是一个办公室内的几台计算机互相连接组成的网络,也可以是一栋楼房上下几百台,甚至上千台计算机互相连接而组成的网络。因此,这里所谓的"局域",其实是指相互连接的计算机相对集中于某一区域。

3.2.2 局域网连接设备

网络连接设备用于将一个网络的几个网段(segments)连接起来,或将几个网络(LAN-LAN,WAN-WAN,LAN-WAN)连接起来形成一个互联网络(interwork or internet)。常用的连接局域网设备主要有网卡、交换机、集线器以及路由器等。

3.3 计算机网络资源使用

计算机网络资源是现代计算机网络的最主要的作用,它包括软件共享、硬件共享及数据共享。软件共享包括各种语言处理程序、应用程序和服务程序。硬件共享是指可在网络范围内提供对处理资源、存储资源、输入输出资源等硬件资源的共享,特别是对一些高级和昂贵的设备,如巨型计算机、大容量存储器、绘图仪、高分辨率的激光打印机等的共享。

3.3.1 局域网中设置共享磁盘

通过网络实现资源共享是网络中最常见的应用,在小型家庭或办公网络中,实现磁盘共享也是常见的典型应用。下面通过实例介绍局域网中设置共享磁盘的过程。

(1) 打开"资源管理器"或"计算机",找到要共享的磁盘,在该磁盘上右击,在弹出的快捷菜单中选择"共享",打开"高级共享"对话框,如图 3.7 所示。

(2) 进行磁盘共享设置,选择"共享"设置,如图 3.8 所示。

(3) 选择"高级共享"选项卡,弹出"高级共享"对话框,选择"共享此文件夹",并设置"共享名"。

(4) 单击"确定"按钮,完成共享设置。该磁盘前面会加一个"群"的图标,表示此磁盘可以通过网上邻居进行共享相关操作了。

图 3.7　“高级共享”对话框

图 3.8　“共享”选项设置

3.3.2　局域网中设置共享打印机

当计算机安装了一台打印机，并希望将此打印机在局域网中进行共享时，可按照如下步骤。

(1) 单击“开始”按钮,选择“设备和打印机”命令,打开此窗口。

(2) 在“打印机与传真”窗口右击要共享的打印机,在弹出的快捷菜单中选择“共享”,如图 3.9 所示。

图 3.9 打印机属性选项

(3) 在打开的“打印机属性”对话框中选择“共享这台打印机”,在“共享名”中输入一个名字,单击“确定”按钮,完成打印机共享设置。

至此,打印机已被设置成共享,当同一局域网中的其他用户要使用此打印机,只需在他自己的计算机上按提示“安装网络打印机”后,便可与你共同使用此打印机。

3.4 Internet Explorer 9 浏览器的使用

Internet Explorer,全称 Windows Internet Explorer,简称 IE,是美国微软公司推出的一款网页浏览器。从 IE4 开始,IE 集成在 Windows 操作系统中作为默认浏览器(IE9 除外,并未在任何 Windows 系统中集成)。

3.4.1 IE 浏览器简介

Windows Internet Explorer(旧称 Microsoft Internet Explorer,简称 IE,俗称“网络探索者”),是微软公司推出的一款网页浏览器。浏览器的种类有几十种,常见的有火狐浏览器 Mozilla-Firefox、Opera、Tencent Traveler(腾讯 TT)、360 浏览器、百度浏览器、agicMaster(M2,魔法大师)、miniie、Thooe(随 E 浏览器)、遨游、绿色浏览器 Greenbrowser、Safari 等。

Internet Explorer 的市场占有率高达 70%。它是使用最广泛的网页浏览器。目前最新版本是 Internet Explorer 11,此版本在速度、标准支持和界面均有很大的改善。在其他操作系统的 Internet Explorer 包括前称 Pocket Internet Explorer 的 Internet Explorer Mobile,用在 Windows Phone 及 Windows Mobile 上。

3.4.2　如何启动 IE 浏览器

启动 IE 浏览器的方法很简单，双击桌面上的 Internet Explorer 图标，或是单击快速启动工具栏上的 Internet Explorer 按钮，或是通过单击“开始”菜单查找 Internet Explorer 图标，均可启动 IE 浏览器。

1. 桌面快捷方式

在桌面上双击 Internet Explorer 图标启动 IE 浏览器。

2. 快速启动栏

通过在桌面底部快速启动栏的 Internet Explorer 图标启动 IE 浏览器。

3. 通过“开始”菜单

在桌面单击“开始”菜单→“选择所有程序”→Internet Explorer 图标，即可启动 IE 浏览器。

3.4.3　Internet Explorer 的窗口界面

在网上进行网页浏览时，主要通过 Internet Explorer 完成。Internet Explorer 提供了直观、方便、友好的用户界面，如图 3.10 所示。

图 3.10　IE 浏览器的窗口组成

1. IE 浏览器的窗口组成

(1) 标题栏。显示浏览器当前正在访问网页的标题。
(2) 菜单栏。包含了在使用浏览器浏览时能选择的各项命令。
(3) 工具栏。包括一些常用的按钮,如前后翻页键、停止键等。
(4) 地址栏。可输入要浏览的网页地址。
(5) 网页区。显示当前正在访问网页的内容。
(6) 状态栏。显示浏览器下载网页的实际工作状态。

2. IE 浏览器的几个主要按钮功能

1) 后退

回到浏览器访问过的上一个网页。如果要查看浏览过的网页列表,可单击工具栏上的"后退"或"前进"按钮右侧的小箭头,然后单击要查看的网页。

2) 前进

回到浏览器访问过的下一个网页,单击此按钮可以方便地前进到任意一个启动浏览器后已访问过的网页。

3) 停止

停止下载当前网页,有时发觉网页的下载没完没了或对下载网页不感兴趣,可以单击此按钮停止当前网页的下载。

4) 刷新

当打开一些更新得很快的页面时,需要单击"刷新"按钮;或者是当打开的站点因为传输问题页面出现残缺时,也可单击"刷新"按钮,重新打开站点。

5) 主页按钮

可以回到起始页,也就是启动浏览器后显示的第一个页面。浏览器的起始网页可以通过对菜单的选择来改变。

6) 搜索按钮

可以登录到指定的搜索网站,搜索 WWW 的资源。

7) 收藏夹按钮

可以打开收藏夹下拉列表。

3.4.4 使用 IE 浏览器浏览网页

从 Web 服务器上搜索需要的信息、浏览 Web 网页、下载、收发电子邮件、上传网页等很多都是通过 IE 浏览器来完成的。通过 IE 浏览器浏览 Web 网页是最主要的也是最常见的工作。

1. 输入网址

启动浏览器后,在"地址"栏中输入所要浏览的页,如输入易网站的网址"www.163.com",然后按 Enter 键,即可打开网易主页。

如果以前浏览过网易的内容,也可单击"地址"栏右侧的向下箭头,在弹出的下拉式列表框中选择 http://www.163.com 也可以很方便地打开网易主页。

2. 在 IE 浏览器浏览所需内容

在打开的网页上，找到自己感兴趣的文章或话题，移动鼠标，使指针指向该标题，鼠标指针就变成一个“小手”的形状，则表示该标题上带有“超链接”，单击，即可打开关于该新闻的 IE 浏览器窗口。打开并浏览“新闻”栏目内容。

如在所示的 IE 窗口中，单击任意的带有超链接的文本或图片，即可打开一个新的关于该超链接的 IE 窗口。

3. 结束浏览

单击窗口右上角的“关闭”按钮，即可关闭目前打开的 IE 窗口。

3.5　计算机信息安全

信息安全是指信息系统的硬件、软件和数据因为偶然和恶意的原因而遭到破坏、更改和泄露，保障系统连续正常运行和信息服务不中断。信息安全的本质和目的就是保护合法用户使用系统资源和访问系统中存储的信息的权利和利益，保护用户的隐私。

3.5.1　信息安全的定义

从技术角度看，计算机信息安全是一个涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术等多种学科的边缘性综合学科。

信息安全包括两个方面：一方面是信息本身的安全，即在信息传输过程中是否有人把信息截获，尤其是重要文件的截获，造成泄密，此方面偏重于静态信息保护；另一方面是信息系统或网络系统本身的安全，一些人出于恶意或好奇进入系统使系统瘫痪，或者在网上传播病毒，此方面着重于动态意义描述。

信息安全是研究在特定应用环境下，依据特定的安全策略，对信息及信息系统实施防护、检测和恢复的科学。

3.5.2　信息安全的要素

计算机信息安全包括物理安全、运行安全、数据安全、信息安全四个方面。

1. 物理安全

物理安全主要是指因为主机、计算机网络的硬件设备、各种通信线路和信息存储设备等物理介质造成的信息泄露、丢失或服务中断等不安全因素。主要涉及网络与信息系统的机密性、可用性、完整性、生存性、稳定性、可靠性等基本属性。所面对的威胁主要包括电源故障、通信干扰、信号注入、人为破坏、自然灾害、设备故障等；主要的保护方式有加扰处理、电磁屏蔽、数据检验、容错、冗余、系统备份等。

2. 运行安全

运行安全是指对网络与信息系统的运行过程和运行状态的保护。主要涉及网络与信息

系统的真实性、可控性、可用性、合法性、唯一性、可追溯性、占有性、生存性、稳定性、可靠性等。

所面对的威胁包括非法使用资源、系统安全漏洞利用、网络阻塞、网络病毒、越权访问、非法控制系统、黑客攻击、拒绝服务攻击、软件质量差、系统崩溃等；主要的保护方式有防火墙与物理隔离、风险分析与漏洞扫描、应急响应、病毒防治、访问控制、安全审计、入侵检测、源路由过滤、降级使用、数据备份等。

3. 数据安全

数据安全是指对信息在数据收集、处理、存储、检索、传输、交换、显示、扩散等过程中的保护，使得在数据处理层面保障信息依据授权使用，不被非法冒充、窃取、篡改、抵赖。主要涉及信息的机密性、真实性、实用性、完整性、唯一性、不可否认性、生存性等。

所面对的威胁包括窃取、伪造、密钥截获、篡改、冒充、抵赖、攻击密钥等；主要的保护方式有加密、认证、非对称密钥、完整性验证、鉴别、数字签名、秘密共享等。

4. 内容安全

内容安全是指对信息在网络内流动中的选择性阻断，以保证信息流动的可控能力。被阻断的对象可以是通过内容能够判断出来的会对系统造成威胁的脚本病毒；因无限制扩散而导致消耗用户资源的垃圾类邮件；导致社会不稳定的有害信息，等等。主要涉及信息的机密性、真实性、可控性、可用性、完整性、可靠性等。

所面对的难题包括信息不可识别(因加密)、信息不可更改、信息不可阻断、信息不可替换、信息不可选择、系统不可控等；主要的处置手段是密文解析或形态解析、流动信息的裁剪、信息的阻断、信息的替换、信息的过滤、系统的控制等。

3.6 信息安全基础

随着网络的普及与发展，人们十分关心在网络上交换信息的安全性，普遍认为密码技术是解决信息安全保护的一个最有效的方法。事实上，现在网络上应用的保护信息安全的技术(如数据加密技术、数字签名技术、消息认证与身份识别技术、防火墙技术以及反病毒技术)都是以密码技术为基础的。

3.6.1 数据加密

数据密码加密技术是为了提高信息系统及数据的安全性和保密性，防止秘密数据被外部破解所采用的主要技术之一。数据加密的基本思想就是伪装信息，使非法接入者无法理解信息的真正含义。借助加密手段，信息以密文的方式归档存储在计算机中，或通过网络进行传输，即使发生非法截获数据或数据泄露的事件，非授权用户也不能理解数据的真正含义。

1. 加密与解密的概念

用某种方法伪装消息以隐藏它的内容的过程称为加密，加了密的消息称为密文，而把密

文转变为明文的过程称为解密，如图 3.11 所示。

图 3.11　数据加密、解密过程

数据加密技术的术语如下。

(1) 明文。需要传输的原文。

(2) 密文。对原文加密后的信息。

(3) 加密算法。将明文加密为密文的变换方法。

(4) 解密算法。将密文解密为明文的变换方法。

(5) 密钥。控制加密结果的数字或字符串。

发送方用加密密钥，通过加密设备或算法，将信息加密后发送出去。接收方在收到密文后，用解密密钥将密文解密，恢复为明文。如果传输中有人窃取，他只能得到无法理解的密文，从而对信息起到保密作用。

2. 现代密码体制

密码体制是指实现加密和解密功能的密码方案，从密钥使用策略上，可分为对称密码体制(Symmetric Key Cryptosystem)和非对称密码体制(Asymmetric Key Cryptosystem)两种。

1) 对称加密算法

对称算法有时又叫传统密码算法，就是加密密钥能够从解密密钥中推算出来，反过来也成立。在对称加密技术中，文件的加密和解密使用的是同一密钥。这些算法也叫秘密密钥算法或单密钥算法，它要求发送者和接收者在安全通信之前，商定一个密钥。对称算法的安全性依赖于密钥，泄漏密钥就意味着任何人都能对消息进行加密/解密。

对称密码算法有两种类型：分组密码(Block Cipher)和流密码(Stream Cipher，或称序列密码)。分组密码一次处理一个输入块，每个输入块生成一个输出块。流密码对单个输入元素进行连续处理，同时产生连续单个输出元素。分组密码将明文消息划分成固定长度的分组，各分组分别在密钥的控制下变换成等长度的密文分组。分组密码的工作原理如图 3.12 所示。

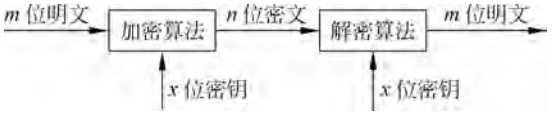

图 3.12　对称密钥加、解密过程

2) 非对称加密算法

非对称加密算法的设计原理为：用作加密的密钥不同于用作解密的密钥，而且解密密钥不能根据加密密钥计算出来(至少在合理假定的有限时间内)。非对称算法也叫作公开密钥算法，是因为加密密钥能够公开，即陌生者能用加密密钥加密信息，但只有用相应的解密密钥才能解密信息。在这些系统中，加密密钥叫作公开密钥，解密密钥叫作私有密钥。

公开密钥和私有密钥是成对出现的，使用公开密钥加密的数据，只有使用对应的私有密钥才能解密；使用私有密钥加密的数据，只有使用对应的公开密钥才能解密。

3.6.2 数字签名

数字签名的概念最早在1976年由美国斯坦福大学的W. Diffie和M. Hellman提出,其目的是使签名者对文件进行签署且无法否认该签名,而签名的验证者无法篡改已被签名的文件。1978年,麻省理工学院Rivest、Shamir和Adleman给出了数字签名的具体应用方案。

数字签名(digital signature)是在数字文档上进行身份认证技术,类似于纸张上的手写签名,是无法伪造的。它利用数据加密技术,按照某种协议来产生一个反映被签署文件的特征和签署人特征,以保证文件的真实性和有效性的数字技术。

1. 数字签名的作用

1) 信息传输的保密性

交易中的商务信息均有保密的要求。如果信用卡的账号和用户名被别人获悉,就可能被盗用;订货和付款的信息被竞争对手获悉,就可能丧失商机,因此在电子商务的信息传播中一般都有加密的要求。

2) 交易者身份的可鉴别性

网上交易的双方很可能素昧平生,相隔千里。商家要确认客户端不是骗子,而客户也要相信网上的商店不是一个玩弄欺诈的黑店,因此能方便而可靠地确认对方的身份是网上交易的前提,为了做到安全、保密、可靠地开展服务活动,都需要进行身份认证的工作。

3) 数据交换的完整性

交易的文件是不能被修改的,以保障交易的严肃性和公正性。

4) 发送信息的不可否认性

由于商情的千变万化,交易一旦达成是不能被否认的,否则必然会损害一方的利益。因此电子交易通信过程的各个环节都必须是不可否认的。

5) 信息传递的不可重放性

在数字签名中,如果采用了对签名报文添加流水号、时间戳等技术,可以防止重放攻击。

2. 数字签名的用途

在网络应用中,数字签名比手工签字更具优越性,数字签名是进行身份鉴别与网上安全交易的通用实施技术。

数字签名的特点如下:

(1) 签名的比特模式依赖于消息报文。

(2) 数字签名对发送者来说必须是唯一的,能够防止伪造和抵赖。

(3) 产生数字签名的算法必须相对简单、易于实现,且能够在存储介质上备份。

(4) 对数字签名的识别、证实和鉴别也必须相对简单,易于实现。

(5) 无论攻击者采用何种手法,伪造数字签名在计算上是不可行的。

3.6.3 数字证书

数字证书如同我们日常生活中使用的身份证,它是持有者在网络上证明自己身份的凭证。在一个电子商务系统中,所有参与活动的实体都必须用证书来表明自己的身份。

1. 数字证书的定义

证书是一个经证书授权中心数字签名的包含公开密钥拥有者信息以及公开密钥的文件。证书一方面可以用来向系统中的其他实体证明自己的身份；另一方面，由于每份证书都携带着证书持有者的公钥，所以证书也可以向接收者证实某人或某个机构对公开密钥的拥有，同时也起着公钥分发的作用。

数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密、解密。每个用户自己设定一把特定的仅为本人所有的私有密钥（私钥），用它进行解密和签名；同时设定一把公共密钥（公钥）并由本人公开，为一组用户所共享，用于加密和验证签名。

2. 常用的数字证书

数字证书必须具有唯一性和可靠性。为了达到这一目的，需要采用很多技术来实现。常用的数字证书有如下几种。

1）SPKI（Simple Public Key Infrastructure）

SPKI 是由 IETF SPKI 工作组指定的一系列技术和参考文档，包括 SPKI 证书格式。SPKI 证书又叫授权证书，主要目的是传递许可权。目前只有很少的 SPKI 证书应用需求，而且缺乏市场需求。

2）PGP（Pretty Good Privacy）

PGP 是一种对电子邮件和文件进行加密与数字签名的方法。它规范了在两个实体间传递信息、文件和 PGP 密钥时的报文格式。

PGP 证书与 X.509 证书之间存在着显著不同，它的信任策略主要基于个人而不是企业。因此，虽然在 Internet 上的电子邮件通信中得到了一定范围内的应用，但对企业内部网来说，却不是最好的解决方案。

3）SET（Secure Electronic Transaction）

SET（安全电子交易）标准定义了在分布式网络上进行信用卡支付交易所需的标准。它采用了 X.509 第 3 版公钥证书的格式，并指定了自己私有的扩展。非 SET 应用无法识别 SET 定义的私有扩展，因此非 SET 应用无法接受 SET 证书。

4）属性证书

属性证书用来传递一个给定主体的属性，以便于灵活、可扩展的特权管理。属性证书不是公钥证书，但它的主体可以结合相应公钥证书通过“指针”来确定。

3. 数字证书的验证

数字证书的验证，是验证一个证书的有效性、完整性、可用性的过程。证书验证主要包括以下几方面的内容。

（1）验证证书签名是否正确有效，这需要知道签发证书的 CA 的公钥。

（2）验证证书的完整性，即验证 CA 签名的证书散列值与单独计算的散列值是否一致。

（3）验证证书是否在有效期内。

（4）查看证书撤销列表，验证证书没有被撤销。

（5）验证证书的使用方式与任何生命的策略及使用限制一致。

数字证书的用途很广泛,它可以用于方便、快捷、安全地发送电子邮件、访问安全站点、网上招标投标、网上签约、网上订购、网上公文的安全传送、网上办公、网上缴费、网上缴税、网上购物等安全电子事务处理和安全电子交易活动。

3.7 计算机病毒的防治

计算机病毒(Computer Viruse)是编制者在计算机程序中插入的破坏计算机功能或者数据的代码,能影响计算机使用,能自我复制的一组计算机指令或程序代码。从 1984 年第一个病毒"小球"诞生以来,计算机病毒不断翻新。计算机病毒的防治工作的基本任务是在计算机的使用管理中,利用各种行政和技术手段,防止计算机病毒的入侵、存留、蔓延。

3.7.1 计算机病毒的概念

"病毒"一词来源于生物学,计算机病毒与医学上的"病毒"不同,计算机病毒最早是由美国加州大学的 Fred Cohen 提出的。他在 1983 年编写了一个小程序,这个程序可以自我复制,能在计算机中传播。该程序对计算机并无害处,能潜伏于合法的程序当中,传染到计算机上。

计算机病毒有很多种定义,国外最流行的定义为:计算机病毒是一段附着在其他程序上的可以实现自我繁殖的程序代码。在《中华人民共和国计算机信息系统安全保护条例》中的定义是:"计算机病毒是指编制或者在计算机程序中插入的破坏计算机功能或者数据,影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。"广义上说,凡能够引起计算机故障,破坏计算机数据的程序通常为计算机病毒。

3.7.2 计算机病毒的特点与分类


计算机病毒

病毒到底有多少,各种说法不一。但不管怎样,病毒的数量确实在不断地增加,而且它们种类不一,感染目标和破坏行为也不尽相同。对病毒进行分类、研究病毒的特点,是为了更好地了解病毒,找到防治方法,使计算机免遭病毒的侵害。

1. 计算机病毒特点

计算机病毒是一段特殊的程序,除了与其他程序一样,可以存储和运行外,计算机病毒还有寄生性、传染性、潜伏性、隐藏性、破坏性等特征。

1) 寄生性

计算机病毒寄生在其他程序之中,当执行这个程序时,病毒就起破坏作用,而在未启动这个程序之前,它是不易被人发觉的。

2) 传染性

计算机病毒不但本身具有破坏性,更有害的是具有传染性,一旦病毒被复制或产生变种,其速度之快令人难以预防。传染性是病毒的基本特征。

3）潜伏性

有些病毒像定时炸弹一样，让它什么时间发作是预先设计好的。例如“黑色星期五”病毒，不到预定时间一点都觉察不出来，等到条件具备的时候一下子就爆炸开来，对系统进行破坏。

4）隐藏性

计算机病毒具有很强的隐藏性，有的可以通过病毒软件检查出来，有的根本就查不出来，有的时隐时现，变化无常，这类病毒处理起来通常很困难。

5）破坏性

计算机中毒后，可能会导致正常的程序无法运行，把计算机内的文件删除或受到不同程度的损坏。通常表现为增加、删减、改变、移动。

2. 病毒类型

按照计算机病毒的诸多特点及特性，其分类方法有很多种，按寄生方式分为引导型病毒、文件型病毒和混合型病毒；按照计算机病毒的破坏情况分类可分为良性计算机病毒和恶性计算机病毒；按照计算机病毒攻击的系统分为攻击 DOS 系统的病毒和攻击 Windows 系统的病毒。

某些病毒结合了诸多病毒的特性，例如将黑客、木马和蠕虫病毒集于一身，这种新型病毒对计算机网络有着致命的破坏性。甚至有的病毒给全球的计算机网络带来了不可预估的灾难。病毒发展初期，一些编程高手只是想要炫耀自己的高超技术，现如今有人想要通过某些病毒，来谋取一些非法利益，其中“木马盗号”便是商业用途病毒中最为典型的一个代表，通过木马病毒来盗取用户的银行卡账号、QQ 密码和个人资料等。

3.7.3　计算机病毒的防范

计算机病毒防范，是指建立合理的计算机病毒防范体系和制度。对于计算机病毒，需要树立以防为主、清除为辅的观念，防患于未然。

1. 计算机病毒的预防

计算机病毒的传染是通过一定途径实现的，为此要以预防为主，制定出一系列的安全措施，堵塞计算机病毒的传染途径，降低病毒的传染概率，即使受到传染，也可以立即采取有效措施将病毒消除，使病毒造成的危害减少到最低限度。对用户来说，抗病毒最有效的方法是备份，抗病毒最有效的手段是病毒库升级要快。

2. 计算机病毒的检测

计算机病毒的检测通常采用手工检测和自动检测两种方法。

1）手工检测

它的基本过程是利用工具软件，对易遭病毒攻击和修改的内存及磁盘的有关部分进行检查，通过与在正常情况下的状态进行对比分析，判断是否被病毒感染。用这种方法检测病毒，费时费力，但可以检测识别未知病毒，以及检测一些自动检测工具不能识别的新病毒。

2) 自动检测

自动检测是指通过病毒诊断软件来识别一个系统是否含有病毒的方法。自动检测相对比较简单,一般用户都可以进行。这种方法可以方便地检测大量的病毒,但是,自动检测工具只能识别已知病毒,对未知病毒不能识别。

3. 计算机病毒的清除

1) 清除病毒的原理

清除计算机病毒要建立在正确检测病毒的基础之上。清除病毒主要应做好以下工作:

(1) 清除内存中的病毒。

(2) 清除磁盘中的病毒。

(3) 病毒发作后的善后处理。

2) 清除病毒的方法

由于计算机病毒不仅干扰受感染的计算机的正常工作,更严重的是继续传播病毒、泄密和干扰网络的正常运行。通常用人工处理或反病毒软件两种方式进行清除。

(1) 人工清除法。

人工处理的方法有:用正常的文件覆盖被病毒感染的文件;删除被病毒感染的文件;重新格式化磁盘,但这种方法有一定的危险性,容易造成对文件数据的破坏。

(2) 杀毒软件清除法。

杀毒软件是专门用于防堵、清除病毒的工具。采用杀毒软件清除法对病毒进行清除是一种较好的方法。对于感染主引导型病毒的机器可采用事先备份的该硬盘的主引导扇区文件进行恢复。

(3) 程序覆盖法。

程序覆盖法适用于文件型病毒,一旦发现文件被感染,可将事先保留的无毒备份重新拷入系统即可。

(4) 格式化磁盘法。

格式化磁盘法不能轻易使用,因为它会破坏磁盘的所有数据,并且格式化对磁盘亦有损害,在万不得已情况下,才使用此方法。

3.8 防火墙技术

防火墙是为了防止火灾蔓延而设置的防火障碍,网络系统中的防火墙的功能与之类似,它是用于防止网络外部恶意攻击的安全防护措施。因此防火墙(Firewall)就是各企业及组织在设置信息安全解决方案中最常被优先考虑的安全控管机制。

3.8.1 防火墙的定义

在计算机网络中,防火墙通过对数据包的筛选和屏蔽,可以防止非法的访问进入内部或外部计算机网络。

1. 防火墙的概念

我国公安安全行业标准中对防火墙的定义为："设置在两个或多个网络之间的安全阻隔，用于保证本地网络资源的安全，通常由包含软件部分和硬件部分的一个系统或多个系统的组合。"

防火墙作为网络防护的第一道防线，由软件和硬件设备组合而成，它位于企业或网络群体计算机与外界网络的边界，限制着外界用户对内部网络的访问以及管理内部用户访问外界网络的权限。

防火墙是一种必不可少的安全增强点，它将不可信任网络同可信任网络隔离开，如图 3.13 所示。防火墙筛选两个网络间所有的连接，决定哪些传输应该被允许，而哪些应该被禁止。

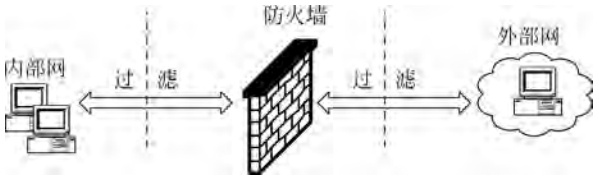

图 3.13　防火墙

2. 防火墙的特性

防火墙是放置在两个网络之间的一些组件，防火墙一般有 3 个特性：

(1) 所有的通信都经过防火墙。

(2) 防火墙只放行经过授权的网络流量。

(3) 防火墙能经受得住对其本身的攻击。

防火墙主要提供以下 4 种服务：

(1) 服务控制：确定可以访问的网络服务类型。

(2) 方向控制：特定服务的方向流控制。

(3) 用户控制：内部用户、外部用户所需的某种形式的认证机制。

(4) 行为控制：控制如何使用某种特定的服务。

3.8.2　防火墙的分类

防火墙的分类方法很多，可以分别从采用的防火墙技术、软硬件形式等标准来划分。

1. 按防火墙软硬件形式分类

1) 软件防火墙

软件防火墙运行于特定的机器上，它需要客户预先安装好的计算机操作系统的支持，一般来说这台计算机就是整个网络的网关，俗称"个人防火墙"。软件防火墙就像其他的软件产品一样，需要先在计算机上安装并配置才可以使用。

2) 硬件防火墙

这里说的硬件防火墙是指所谓的硬件防火墙，之所以加上"所谓"二字是针对芯片级防

火墙说的,它们最大的差别在于是否基于专用的硬件平台。目前市场上大多数防火墙都是这种所谓的硬件防火墙。

3) 芯片级防火墙

芯片级防火墙基于专门的硬件平台,没有操作系统。

2. 按防火墙技术分类

1) 包过滤(Packing Filtering)型防火墙

包过滤防火墙工作在 OSI 网络参考模型的网络层和传输层,它根据数据包头源地址、目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据包才被转发到相应的目的地,其余数据包则从数据流中被丢弃。

2) 应用代理(Application Proxy)型防火墙

应用代理型防火墙工作在 OSI 参考模型的最高层,即应用层。其特点是完全"阻隔"了网络通信流,通过对每种应用服务编制专门的代理程序,监视和控制应用层通信流。

3. 按防火墙结构分类

从防火墙结构上分,防火墙主要分为单一主机防火墙、路由器集成式防火墙和分布式防火墙三种。

1) 单一主机防火墙

单一主机防火墙是最为传统的防火墙,独立于其他网络设备,位于网络边界。

2) 路由器集成式防火墙

原来的单一主机防火墙价格非常昂贵,仅有少数大型企业才能承受得起,为了降低企业网络成本,现在许多高档路由器都集成了防火墙功能。

3) 分布式防火墙

有的防火墙已不再是一个独立的硬件实体,而是由多个软硬件组成的系统,这种防火墙俗称"分布式防火墙"。分布式防火墙再也不是只位于网络边界,而是渗透于网络的每一台主机,对整个内部网络的主机实施保护。

3.8.3 黑客

一般来说,以入侵他人计算机系统为乐趣并进行破坏的人,被称为"黑帽子","Cracker"指的也是这种人。

1. 黑客的定义

黑客一词,源于英文 Hacker,原指热衷于计算机技术,水平高超的计算机专家,尤其是程序设计人员,也有人把他们比作"侠客"。黑客是那些检查系统完整性和安全性的人,他们精通计算机硬件和软件知识,并有能力通过新的方法剖析系统。黑客通常会去寻找网络中的漏洞,但是往往并不破坏计算机系统。正是因为黑客的存在,人们才会不断了解计算机系统中存在的安全问题。

入侵者(Cracker,有人翻译成"骇客")是那些利用网络漏洞破坏系统的人,他们往往会通过计算机系统漏洞来入侵。他们具有广泛的计算机知识,与黑客不同的是,他们以破坏为

目的。真正的黑客应该是负责任的人，他们认为破坏计算机系统是不正当的。但是现在Hacker 和 Cracker 已经混为一谈，人们通常将入侵计算机系统的人统称为黑客。

2. 黑客的主要行为

黑客利用漏洞来做以下几方面的工作。

1）获取系统信息

有些漏洞可以泄漏系统信息，暴露敏感资料（如银行客户账号），黑客们利用系统信息进入系统。

2）入侵系统

通过漏洞进入系统内部，取得服务器上的内部资料，甚至完全掌管服务器。

3）寻找下一个目标

一个胜利意味着下一个目标的出现，黑客会充分利用自己已经掌管的服务器作为工具，寻找并入侵下一个相似的系统。

3. 黑客的预防措施

常用的黑客预防措施有如下几种。

1）防火墙技术

使用防火墙来防止外部网络对内部网络的未经授权访问，建立网络信息系统的对外安全屏障，以便对外部网络与内部网络交流的数据进行检测，符合的予以放行，不符合的则拒之门外。

2）安全监测与扫描工具

经常使用安全监测与扫描工具作为加强内部网络与系统的安全防护性能和抗破坏能力的主要手段，用于发现安全漏洞及薄弱环节。当网络或系统被黑客攻击时，可用该软件及时发现黑客入侵的迹象，并进行处理。

3）网络监控工具

使用有效的控制手段抓住入侵者。经常使用网络监控工具对网络和系统的运行情况进行实时监控，用于发现黑客或入侵者的不良企图及越权使用，及时进行相关处理，防患于未然。

4）备份系统

经常备份系统，以便在被攻击后能及时修复系统，将损失减少到最低程度。

5）防范意识

加强安全防范意识，有效地防止黑客的攻击。

3.9　本章小结

计算机网络是现代计算机技术与通信技术密切结合的产物，计算机网络经历了由简单到复杂、由低级到高级的发展过程。计算机网络类型按照计算机连网络覆盖区域大可划分为局域网、城域网和广域网。其拓扑图结构主要有星型结构、环型结构、总线型结构、树型结构、网状结构等。TCP/IP 协议在计算机网络体系结构中占有非常重要的地位，它将网络体

系结构分为网络接口层、互联层、传输层和应用层。

局域网是指在某一区域内由多台计算机互联成的计算机组。局域网可以实现文件管理、应用软件共享、打印机共享、工作组内的日程安排、电子邮件和传真通信服务等功能。局域网由网络硬件和网络传输介质,以及网络软件所组成。

Internet Explorer 是美国微软公司推出的一款网页浏览器。它提供了直观、方便、友好的用户界面,通过它可以从 Web 服务器上搜索需要的信息、浏览 Web 网页、下载、收发电子邮件、上传网页等。电子邮件是一种用电子手段提供信息交换的通信方式,它可以是文字、图像、声音等多种形式。免费空间就是指网络上的免费提供的网络空间,通过它可以搭建个人网络空间。

随着信息化建设的不断深入,复杂应用系统和计算机网络的广泛应用,特别是政府上网工程和电子商务的开展,信息系统的安全问题日益显得重要。由于网络系统的开放性、互联性和资源共享性,以及网络协议本身先天的缺陷和安全漏洞,使得网络极易受到"黑客"、病毒、恶意软件的攻击,给信息系统带来各种各样的安全问题。本章介绍了信息安全的基本概念,信息安全的相关技术和措施,如数据加密、数字签名、数字证书、防火墙等,以及计算机病毒的防治技术。

习题 3

一、单选题

1. TCP/IP 体系结构中,最低层是(　　)。

A. 网络接口层　　B. 网际层　　C. 传输层　　D. 物理层

2. 下列不属于网页浏览器的是(　　)。

A. Internet Explorer　　B. FireFox

C. Google Chrome　　D. CNKI25

3. 下列能完成邮件发送的服务器的是(　　)。

A. SMTP　　B. ISP　　C. POP　　D. FTP

4. 保存当前网页时要指定保存类型,可以有(　　)种选择。

A. 1　　B. 2　　C. 3　　D. 4

5. 电子邮件地址 liming@ 163. net 中的 163. net 是 (　　)。

A. 电子信箱服务器　　B. 电子邮局

C. IP 地址　　D. 域名

6. 从冯·诺依曼计算机理论模式来看,目前的计算机在(　　)上还无法消除病毒的破坏和黑客的攻击。

A. 理论　　B. 技术　　C. 资金　　D. 速度

7. 信息安全主要涉及信息存储安全、信息传输安全以及信息内容的(　　)。

A. 审计　　B. 过滤　　C. 加密　　D. 签名

8. 计算机病毒是影响计算机使用并能自我复制的一组计算机指令或(　　)。

A. 程序代码　　B. 二进制数据

C. 黑客程序　　D. 木马程序

9. 发现计算机感染病毒后，可用来清除病毒的操作是(　　)。

A. 使用杀毒软件　　B. 扫描磁盘

C. 整理磁盘碎片　　D. 重新启动计算机

10. 为了预防计算机病毒，对于外来磁盘应(　　)。

A. 禁止使用　　B. 先查毒，后使用

C. 使用后，就杀毒　　D. 随便使用

二、简答题

1. 计算机网络的发展过程。
2. 计算机网络的用途有哪些？
3. 计算机网络有哪些分类？
4. OSI 参考模型如何划分的？
5. 局域网最基本的拓朴结构有哪几种？
6. 什么是数据加密？
7. 计算机病毒的特点？
8. 什么是防火墙？

实验 3　网络组建

【实验目的】

1. 熟悉无线网络设备的基本功能及基本参数
2. 了解家庭无线网络设置的需求
3. 根据家庭需要组建家庭无线网络

【实验题目】

实验 3-1　组建家庭无线网络

计算机技术和电子信息技术的日渐成熟，电子产品以前所未有的速度迅速进入千家万户。随着网络的普及，千家万户对 Internet 的需求也越来越多。大学新生小明打算自己动手组建家庭无线网络，请你根据所学的网络知识，为他设计一下方案。

【实验要求】

无线路由器的种类很多，价格相差很多，请根据当前网上报价，结合当地电子市场实际选择性价比高的产品，准备好长度适合的网线，最后要熟练掌握 WiFi 的设置步骤和方法。