江 楠 ◎著

计算机网络与信息安全

天津出版传媒集团
天津科学技术出版社

河南省科技攻关项目（202102210176，212102210429）

计算机网络与信息安全

江　楠　著

天津出版传媒集团
天津科学技术出版社

图书在版编目（CIP）数据

计算机网络与信息安全 / 江楠著. -- 天津 : 天津科学技术出版社, 2021.4

ISBN 978-7-5576-9014-4

Ⅰ. ①计… Ⅱ. ①江… Ⅲ. ①计算机网络－信息安全 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2021)第065737号

计算机网络与信息安全

JISUANJI WANGLUO YU XINXI ANQUAN

责任编辑：吴文博

责任印制：兰　毅

出版：天津出版传媒集团
天津科学技术出版社

地址：天津市西康路 35 号

邮编：300051

电话：（022）23332377

网址：www.tjkjcbs.com.cn

发行：新华书店经销

印刷：天津市宏博盛达印刷有限公司

开本 787×1092　1/16　印张 17.50　字数　420 000

2021 年 4 月第 1 版第 1 次印刷

定价：35.00 元

前　言

随着 Internet 技术的不断发展，计算机网络成为信息传递与保存的主要载体之一。计算机网络在人类社会中的作用也越来越重要，对社会影响的范围逐步增大。社会各方面的运转以及各项活动的开展，都已经离不开计算机网络的支持。可以说，计算机网络已经深入生活中的方方面面，如日常生活中的银行、电话、购物、出行、电力等都十分依赖计算机网络，现在已经很难想象没有了计算机网络，人们的生活会变成什么样子。随着人们对计算机网络的依存度逐渐提高，信息安全已经成为一个全世界性的现实问题，信息安全与国家的政治稳定、军事安全、经济发展、民族兴衰等都息息相关，提高国家信息安全体系的保障能力已成为各国优先考虑的战略问题。

但与此同时，网络安全问题也愈发突出，受到越来越广泛的关注。计算机和网络系统不断受到侵害，侵害形式日益多样化，侵害手段和技术日趋先进化和复杂化，令人防不胜防。一方面，计算机网络提供了丰富的资源以便用户共享；另一方面，资源共享度的提高也增加了网络受到威胁和攻击的可能性。事实上，资源共享和网络安全是一对矛盾体，随着资源共享的扩大，网络安全问题也日益突出。计算机网络的安全已成为当今信息化建设的核心问题之一。

本书就结合当前计算机网络中存在的一些安全问题，有针对性地提出了一些安全防护措施。全书共有十二章。第一章对计算机网络及其安全的相关概念进行了全面的介绍；第二章分析了计算机网络安全中存在的问题，并提出了相应的解决策略；第三章对计算机网络的安全体系进行了阐述，并研究了其构建途径；第四章阐述了计算机数据库的基本理论及安全方法；第五章对计算机数字加密与认证技术的相关理论进行了研究；第六章对计算机隐藏技术的原理与应用进行了分析；第七章是关于防火墙理论、技术、产品及应用的全面研究；第八章和第九章对计算机入侵检测与病毒防治技术做了深入分析；第十章对计算机网络攻击与防范进行了研究；第十一章研究了计算机备份与恢复技术；第十二章对计算机网络新技术如云计算、大数据和互联网等进行了研究。

本书由郑州轻工业大学计算机与通信工程学院江楠著。本书论述全面、语言严谨、逻辑清晰。在本书的写作过程中，作者查阅了大量的相关资料，也就一些比较有争议的问题请教了相关的专家，以期本书能对中国的计算机网络安全事业贡献自己的力量。但是，由于作者能力有限，本书可能还存在很多不足之处，还望读者指教。在本书的写作和出版过程中得到了郑州轻工业大学计算机与通信工程学院、信息化管理中心和天津科学技术出版社的大力支持和帮助，在此表示感谢。

目　录

第一章　计算机网络信息安全概述

计算机网络，是指将地理位置不同的具有独立功能的多台计算机及其外部设备，通过通信线路连接起来，在网络操作系统、网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。21 世纪已进入计算机网络时代。计算机网络对人类生活产生了深远的影响：人们出门旅行可以通过网络订购到全国任何车次的车票和任何航班的飞机票；付账时也不用带现金，只需在某个银行开户存钱，在全国乃至全世界都可以提取；可以足不出户在家购物，等等。网络缩短了人与人之间的距离，使宇宙变“小”了许多。本章主要介绍了计算机网络及其信息安全的相关知识。

第一节　计算机网络相关概念

一、计算机网络的定义

简单地说，计算机网络就是通过通信设施将两台以上的计算机连接起来所组成的综合系统。

随着计算机网络技术的发展和人们对计算机网络认识的不断深入，对计算机网络的定义存在着以下 3 种不同的观点：

（一）广义上的观点

这种观点认为，计算机网络是计算机技术与通信技术相结合，实现远程信息处理以进一步达到资源共享的系统。

这种观点主要是从计算机通信的意义上看待计算机网络，按照这一观点，20 世纪 50 年代出现的“终端—计算机”网和 20 世纪 60 年代出现的“计算机—计算机”网都是计算机网络。

（二）资源共享的观点

这种观点认为，计算机网络是以资源共享为目的，用通信线路连起来的具有独立功能的计算机系统的集合。

这一观点强调互连的目的是实现资源共享，符合目前的计算机网络的基本特征。

(三)对用户透明的观点

这种观点认为,计算机网络是存在一个能为用户自动管理资源的网络操作系统,由它来调用完成用户任务所需的资源,而整个网络对用户是透明的。

这一观点强调易用性,是把整个网络视为一个计算机系统一样对用户是透明的,用户只要知道如何得到和使用网络共享资源即可,没有必要也不需要知道网络共享资源所在的确切物理位置。

随着计算机网络技术的飞速发展和应用的不断深入,这一观点深为广大用户所认可:只有这样的网络才是人类所真正需要的网络。

综上所述,我们可将计算机网络定义为: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相互连接起来,在网络操作系统、通信协议及网络管理软件的管理协调下,实现资源共享和信息传递的系统。

二、计算机网络的产生

计算机网络是通信技术与计算机技术相结合的一门综合性学科,它的诞生为人类社会的进步做出了巨大贡献,它的迅速发展适应了社会对资源共享和信息传递日益增长的需求。自 1946 年世界上第一台电子计算机诞生,任何人都没有预测到几十年后的今天,计算机在社会各个领域的应用和影响是如此广泛和深远。1954 年,制造出了被称作收发器的终端,人们使用这种终端,将穿孔卡片上的数据从电话线路上发送到远程计算机。此后,又有了电传打字机,用户可在远程电传打字机上键入程序,而计算出来的结果又可以从计算机传送到电传打字机打印出来。计算机与通信的结合就这样开始了。

经过多年的发展,计算机网络技术已经进入了一个崭新的时代,特别是在当今的信息社会,网络技术已日益深入到国民经济的各个部门和社会生活的各个方面,成为人们日常生活与工作中不可缺少的工具。

计算机网络从 20 世纪 60 年代开始,直至今日,已获得飞速的发展,形成了从小型的办公局域网络到全球性的大型广域网的规模。对现代人们的生产、生活、经济等各个方面都产生了巨大的影响。计算机互连系统这个阶段的典型代表是 1969 年 12 月由美国国防部(DOD)资助、国防部高级研究计划局(ARPA)主持研究建立的数据报交换计算机网络 ARPANET。ARPANET 网络利用租用的通信线路连接美国加州大学洛杉矶分校、加州大学圣巴巴拉分校、斯坦福大学和犹太大学 4 个节点的计算机,构成了专门完成主机之间通信任务的通信子网。通过通信子网互连的主机负责运行用户程序,向用户提供资源共享服务,它们构成了资源子网。该网络采用分组交换技术传送信息,这种技术能够保证:如果这四所大学之间的某一条通信线路因某种原因被切断以后,信息仍能够通过其他线路在各主机之间传递。没有人能够预测到几十年后,计算机网络就在现代信息社会中扮演了如此重要的角色。ARPANET 网络已从最初的 4 个节点发展为横跨全世界 100 多个国家和地区,连接几万个网络、几百万台计算机、几亿用户的因特网(Internet),也可以说 Internet 全球互联网络的前身就是 ARPANET 网络。Internet 是当前世界上最大的国际性计算机互联网络,而且还在不断地迅速发展之中。

纵观计算机网络的发展历史可以发现,它和其他事物的发展一样,也经历了从简单到复

杂、从低级到高级的过程。在这一过程中,计算机技术与通信技术紧密结合,相互促进,共同发展,最终产生了计算机网络。总体看来,网络的发展可以分为具有通信功能的单机系统、具有通信功能的多机系统及以共享资源为主的计算机网络和以局域网络及其互连为主要支撑环境的分布式计算机系统三个阶段。

在计算机网络出现之前,人们需要通过软盘、磁带等设备实现本地或异地进行信息资源的相互传递。

假设本地或异地有 A、B 两个用户的计算机要交换数据,当时的解决办法是:用户 A 需要利用磁盘(常用软盘或磁带,软盘容量一般是 720 KB、1.44 MB、2.88 MB 等)复制数据,然后将磁盘安装到用户 B 计算机上,将磁盘上的数据复制到用户 B 计算机上,从而实现数据的传递。使用磁盘而利用人工到处奔走实现数据传递,这样的方法不方便又不安全,而且又耗时间。

三、计算机网络的功能和应用

(一)计算机网络的功能

计算机网络具有如下一些功能,其中最主要的功能是资源共享和通信。

1. 共享硬件与软件

计算机网络允许网络上的用户共享网络上各种不同类型的硬件设备,可共享的硬件资源有巨型计算机、专用的高性能计算机、大容量磁盘、高性能打印机、高精度图形设备、通信线路、通信设备等。共享硬件的好处是节约开支、用户可以通过网络访问各种不同类型的设备。

现在已经有许多专供网上使用的软件,如数据库管理系统、各种 Internet 信息服务软件等。共享软件允许多个用户同时使用,并能保持数据的完整性和一致性。特别是客户机/服务器和浏览器/服务器模式的出现,人们可以使用客户机来访问服务器,而服务器软件是共享的。并且在 B/S 方式下,软件版本的升级修改只要在服务器上进行,全网用户都可立即享受。可共享的软件种类很多,包括大型专用软件、各种网络应用软件、各种信息服务软件等。

2. 共享信息

信息也是一种资源,Internet 就是一个巨大的信息资源宝库,在其上面有极为丰富的信息资源,它就像是一个信息的海洋,有取之不尽、用之不竭的信息与数据。每一个接入 Internet 的用户都可以共享这些信息资源。可共享的信息资源有:搜索与查询的信息,Web 服务器上的主页及各种链接,FTP 服务器中的软件,各种各样的电子出版物,网上消息、报告和广告,网上大学,网上图书馆等。

3. 通信功能

通信功能是计算机网络的基本功能之一,它可以为网络用户提供强有力的通信手段。建设计算机网络的主要目的就是让分布在不同地理位置的计算机用户之间能够相互通信、交流信息。计算机网络可以传输数据、声音、图形和图像等多媒体信息。利用网络的通信功能,可以发送电子邮件,在网上举行电视会议等。

(二)计算机网络的应用

随着现代信息社会进程的推进,通信和计算机技术的迅猛发展,计算机网络的应用也越来越普及,如今计算机网络几乎深入到社会的各个领域。Internet 已成为家喻户晓的计算机网络,它也是世界上最大的计算机网络,是一条贯穿全球的“信息高速公路主干道”。通过计算机网络提供的服务,人们可将计算机网络应用于社会的方方面面。

1. 网络在科研和教育中的应用

通过全球计算机网络,科技人员可以在网上查询各种文件和资料,可以互相交流学术思想和交换实验资料,甚至可以在计算机网络上进行国际合作研究项目。在教育方面可以开设网上学校,实现远程授课,学生可以在家里或其他可以将计算机接入计算机网络的地方,利用多媒体交互功能听课,有什么不懂的问题可以随时提问和讨论。学生可以从网上获得学习参考资料,并且可通过网络交付作业和参加考试。

2. 网络在企事业单位中的应用

计算机网络可以使企事业单位和公司内部实现办公自动化,做到各种软硬件资源共享,而且,如果将内部网络联入 Internet 还可以实现异地办公。例如,通过 WWW 或电子邮件,公司就可以很方便地与分布在不同地区的子公司或其他业务单位建立联系,不仅能够及时地交换信息,而且实现了无纸办公。在外地的员工通过网络还可以与公司保持通信,得到公司的指示和帮助。企业可以通过国际互联网,搜集市场信息并发布企业产品信息,取得良好的经济效益。

3. 网络在商业上的应用

随着计算机网络的广泛应用,电子数据交换(Electronic Data Interchange, EDI)已成为国际贸易往来的一个重要手段。它以一种被认可的数据格式,使分布在全球各地的贸易伙伴可以通过计算机传输各种贸易单据,代替了传统的贸易单据,节省了大量的人力和物力,提高了效率。又如网上商店,实现了网上购物、网上付款的网上消费梦想。

4. 网络在通信与娱乐上的应用

20 世纪个人之间通信的基本工具是电话,21 世纪个人之间通信的基本工具是计算机网络,计算机网络所提供的通信服务包括电子邮件、网络寻呼、BBS、网络新闻和 IP 电话等。目前,电子邮件已广泛应用,初期的电子邮件只能传送文本文件,而现在已经可以传输语音与图像文件。Internet 上存在着很多的新闻组,参加新闻组的人可以在网上对某个感兴趣的问题进行讨论,或是阅读有关这方面的资料,这是计算机网络应用中很受欢迎的一种通信方式。网络寻呼不但可以实现在网络上进行寻呼的功能,还可以在网友之间进行网络聊天和文件传输等。IP 电话也是基于计算机网络的一类典型的个人通信服务。

家庭娱乐正在对信息服务业产生着巨大的影响,它可以让人们在家里点播电影和电视节目,目前一些发达国家已开展了这方面的服务。新的电影可能成为交互式的,观众在看电影时可以不时参与到电影情节中去。家庭电视也可以成为交互形式的,观众可以参与到猜谜等活动之中。家庭娱乐中最重要的应用可能是在游戏上,目前,已经有很多人喜欢上多人实时仿真游戏。如果使用虚拟现实的头盔和三维、实时、高清晰度的图像,我们就可以共享虚拟现实的很多游戏和进行多种训练。

随着网络技术的发展和各种网络应用的需求,计算机网络应用的范围在不断扩大,应用

领域越拓越宽，越来越深入，许多新的计算机网络应用系统不断地被开发出来，如工业自动控制、辅助决策、虚拟大学、远程教学、远程医疗、管理信息系统、数字图书馆、电子博物馆、全球情报检索与信息查询、网上购物、电子商务、电视会议、视频点播等。

第二节　计算机网络服务及其安全

一、计算机网络服务的类型

网络服务是基于超文本传输协议（HTTP 协议）的服务，HTTP 协议是一个面向连接的协议，在 TCP 的端口 80 上进行信息的传输。大多数 Web 服务器和浏览器都对 HTTP 协议进行了必要的扩展，一些新的技术接口 CGI 通用网关程序、Java 小程序、ActiveX 控件、虚拟现实等，也开始应用于各种服务器，使信息交互显得更加容易。

网络服务是指在网络上所使用的一些应用服务，典型的网络应用服务有如下几种。

（一）Web 服务

Web 服务是一个基于超文本（Hypertext）方式的信息查询工具。它是由位于瑞士日内瓦的欧洲粒子物理实验室 CERN 最先研制的。Web 把位于全世界不同地方的互联网上数据信息有机地组织起来，形成一个巨大的公共信息资源网。Web 带来的是全世界范围的超文本服务。通过操纵电脑的鼠标器，人们就可以在互联网上浏览到分布在全世界各地的文本、图像、声音和视频等信息。

（二）电子邮件服务

电子邮件是互联网上使用最广泛的一种服务。用户只要能与互联网连接，具有能收发电子邮件的程序及个人的 E-mail 地址，就可以与互联网上具有 E-mail 的所有用户方便、快速、经济地交换电子邮件，可以在两个用户间交换，也可以向多个用户发送同一封邮件，或将收到的邮件转发给其他用户。电子邮件中除文本外，还可包含声音、图像、应用程序等各类计算机文件。此外，用户还可以邮件方式在网上订阅电子杂志、获取所需文件、参与有关的公告和讨论组，甚至还可浏览 Web 资源。

（三）FTP 服务

FTP 服务允许用户在计算机之间传送文件，并且文件的类型不限，可以是文本文件，也可以是二进制可执行文件、声音文件、图像文件、数据压缩文件等。FTP 服务是一种实时的联机服务，在进行工作前必须首先登录到对方的计算机上，登录后才能进行文件搜索和文件传送等有关操作。普通的 FTP 服务需要在登录时提供相应的用户名和口令，当用户不知道对方计算机的用户名和口令时，就无法使用其 FTP 服务。为此，一些信息服务机构为了方便互联网的用户通过网络使用他们公开发布的信息，提供了一种“匿名 FTP 服务”。

(四)DNS 服务

DNS 服务主要的功能是将域名转换为相应的 IP 地址,提供 DNS 服务的系统就是 DNS 服务器。当网络上的一台客户机访问某一服务器上的资源时,用户在浏览器地址栏输入的是便于识记的主机名和域名,而网络上的计算机之间实现连接却是通过每台计算机在网络中拥有的唯一的 IP 地址来完成的,这样就需要在用户容易记忆的地址和计算机能够识别的地址之间有一个解析,DNS 服务器便充当了解析的重要角色,它将用户输入的便于记忆的主机名和域名映射为 IP 地址。

(五)Telnet 服务

Telnet 服务是互联网提供的基本信息服务之一,是提供远程连接服务的终端仿真协议。它可以使你的计算机登录到互联网上的另一台计算机上。你的计算机就成为你所登录计算机的一个终端,可以使用那台计算机上的资源,例如打印机和磁盘设备等。Telnet 提供了大量的命令,这些命令可用于建立终端与远程主机的交互式对话,可使本地用户执行远程主机的命令。

二、网络服务的安全隐患

网络服务在方便用户发布信息的同时,也给用户带来了不安全因素。尤其是在标准协议基础之上扩展的某些服务,在向用户提供信息交互的同时,也使得网络基础又增加了新的不安全因素。

(一)Web

通过 HTTP 浏览信息是人们获取信息非常重要的手段。但是浏览器一般只能理解基本的数据格式,如 HTML、JPEG 和 GIF 等静态的格式,一些含有脚本的 Web 文件,例如 ASP、JSP、PHP 等,需要系统提供的服务进行解析,但是这些服务,例如 IIS、Apache 等,其程序本身都会有很多漏洞和安全隐患,所以也是重点被攻击的对象。

(二)电子邮件

如今,人们通过邮件发送信息进行生活和工作中的交流。因此,通过电子邮件来攻击站点是入侵者常用的方法。其中一个安全问题是邮件的溢出,即通过无休止的垃圾邮件耗尽用户的存储空间(包括链式邮件)。通过邮件系统,可以发送包含程序的电子邮件,这种程序如果在管理不严格的情况下运行,能产生“特洛伊木马”或已感染蠕虫病毒的附件。

(三)FTP

FTP 服务是通过建立 FTP 站点,可以允许网络用户远程登录服务器获取或上传文件。其中很多 FTP 站点提供匿名 FTP,它允许用户采取匿名(用户名为 Anonymous,密码为空)方式访问 FTP 服务器上的文件,这时不正确的配置将严重威胁系统的安全。因此需要保证使用它的人不会申请系统上其他的区域或文件,也不能对系统做任意的修改,否则可能会传输一些如“特洛伊木马”文件、不良信息文件、盗版软件等带来安全隐患,同时会消耗系统的物理磁盘空间。

（四）DNS

DNS 服务使用 UDP 协议，对于攻击者而言，更容易把攻击焦点集中在 DNS 服务上。DNS 服务会查漏内部的网络拓扑结构，故 DNS 存在较大安全隐患，整个网络架构中的主机名、主机 IP 列表、路由器名、路由器 IP 列表、计算机所在位置等都可以被轻易窃取。攻击者一旦控制了 DNS 服务器，就会篡改 DNS 的记录信息，利用被篡改的记录信息达到入侵整个网络的目的，使到达原目的地的数据包落入攻击者控制的主机。

（五）Telnet

Telnet 是一种远程终端登录服务。Telnet 早期是比较安全的，它需要用户认证。但 Telnet 送出的所有信息是不加密的，很容易被黑客攻击。现在 Telnet 被认为是从远程系统申请目的站点时最危险的服务之一。

三、典型应用服务安全的分析

随着时代的进步，科学的发展，越来越多的网络应用服务进入人们的视野，与人们的生活息息相关，网络服务也日益呈现多元化。电子邮件、DNS、电子商务的安全受到人们的普遍重视，相应的安全技术也快速发展起来。

（一）电子邮件安全技术

电子邮件十分脆弱，从浏览器向因特网上的另一个人发送电子邮件时，不仅信件像明信片一样是公开的，而且也无法知道在到达其最终目的地之前，信件经过了多少机器。电子邮件到达收件人之前，会经过大学、政府机构和服务提供商。因为邮件服务器可接收来自任意地点的任意数据，所以任何人只要可以访问这些服务器，或访问电子邮件经过的路径，就可以阅读这些信息。唯一的安全性取决于人们对你的邮件有多大兴趣。为了保证客户资料的安全，现代电子邮件系统纳入了一些保护电子邮件的技术和方法，但要做到全方位地保证电子邮件的安全，仅仅这些是不够的。

1. 电子邮件系统中的安全技术

（1）端到端的安全电子邮件技术

端到端的安全电子邮件技术保证邮件从被发出到被接收的整个过程中，内容保密，无法修改，并且不可否认（Privacy、Integrity、Non-Repudation）。目前的 Internet 上，有两套成型的端到端安全电子邮件标准：PGP 和 S/MIME。PGP（Pretty Good Privacy）的特点是通过单向散列算法对邮件内容进行签名，以保证信件内容无法修改，使用公钥和私钥技术保证邮件内容保密且不可否认。在 PGP 系统中，信任是双方之间的直接关系，或是通过第三者、第四者的间接关系，但任意两方之间都是对等的，整个信任关系构成网状结构，这就是所谓的 Web of Trust。最近，基于 PGP 的模式又发展出了另一种类似的安全电子邮件标准，称为 GPG（Gnu Privacy Guard）。S/MIME（Secure Multi-Part Internet Mail Extension）的认证机制依赖于层次结构的证书认证机构，所有下一级的组织和个人的证书由上一级的组织负责认证。而最上一级的组织（根证书）之间相互认证，整个信任关系基本是树状的，S/MIME 将信件内容加密签名后作为特殊的附件传送。

(2)传输层的安全电子邮件技术

目前主要有两种方式实现电子邮件在传输过程中的安全,一种是利用 SSL SMTP 和 SSL POP。另一种是利用 VPN 或者其他的 IP 通道技术,将所有的 TCP/IP 传输封装起来,当然也就包括了电子邮件。

SMTP 是发信的协议标准,POP(Post Office Protocol)是收信的协议。SSL SMTP 和 SSL POP 是在 SSL 所建立的安全传输通道上运行 SMTP 和 POP 协议,同时又对这两种协议做了一定的扩展,以更好地支持加密的认证和传输。这种模式要求客户端的 E-mail 软件和服务器端的 E-mail 服务器都支持,而且都必须安装 SSL 证书。

基于 VPN 和其他 IP 通道技术,封装所有的 TCP/IP 服务,也是实现安全电子邮件传输的一种方法,这种模式往往是整体网络安全机制的一部分。

(3)邮件服务器的安全与可靠性

建立一个安全的电子邮件系统,采用合适的安全标准非常重要。但仅仅依赖安全标准是不够的,邮件服务器本身必须是安全、可靠、久经实战考验的。

2. 电子邮件服务攻击方法

为了方便用户通过浏览器进行收发邮件,电子邮件服务器也是一台 Web 服务器,所以电子邮件服务也同样具有 Web 服务的一些安全漏洞及威胁。同时因为电子邮件服务主要提供电子邮件的收发服务,所以它又面临一些仅提供 Web 服务所没有的网络威胁。例如,用户收到的邮件附件可能是一个计算机病毒文件。针对电子邮件攻击的方法很多,除了针对电子邮件提供的 Web 服务进行攻击的方法,如 DDoS 等,还有一些针对电子邮件服务的攻击方法。下面主要介绍此类方法。

(1)垃圾电子邮件

垃圾邮件也称为电子邮件 Spamming。可被描述为不停地接到大量同一内容的电子邮件。一条信息被传给成千上万的而且不断扩大的用户。更糟的是,如果一个人回复了电子邮件 Spamming,那么表头里所有的用户都会收到这封回信。

这种方式主要的风险来自电子邮件服务器。如果服务器接到很多的电子邮件,服务器就会变得无法正常通过网络访问或响应超时,系统甚至可能崩溃。因此,如果系统突然变得迟钝,或察觉电子邮件速度大幅减慢,或不能收发电子邮件,就应该小心。此时电子邮件服务器可能正忙于处理极大数量的信息。如果感到站点正受侵袭,试着找出轰炸或电子邮件 Spamming 的来源,然后设置防火墙或路由器,过滤来自那个地址的邮包。

(2)电子邮件炸弹

电子邮件炸弹,英文是电子邮件 Bomb,指的是发件人以不名来历的电子邮件地址,不断重复将电子邮件寄给同一收件人,由于情况就像战争中利用某种战争工具对同一个地方进行大轰炸,人们就将它形象地称为电子邮件炸弹,它是黑客常用的一种攻击手段。

电子邮件炸弹与 Spamming 有些类似,但其实两者不尽相同,Spamming 指的是同一发件者在同一时间将同一电子邮件寄往许多不同的用户(或新闻组),它主要是一些公司用来宣传其产品的广告方式,但 Spamming 不会对收件人造成太大的伤害。而电子邮件炸弹则不然,由于一般网络用户的个人邮件信箱容量是有限的,如果你在短时间内收到成千的电子邮件,而每个电子邮件又占据了一定的容量,它就会把用户的信箱挤爆。在这样的情况下,你的信箱不仅不能够再收到其他人寄给你的电子邮件,同时也会占用大量的网络资源,常常导

致网络塞车,使大量用户不能正常地工作,导致整个电脑瘫痪,所以电子邮件炸弹的危害是相当大的。

有些用户可能会想利用电子邮件的 reply 和 forward 的功能“回礼”,将整个炸弹“反丢”回给发件人,但万一对方将电子邮件的 from 和 to 的两个栏目都改换成你的电子邮件地址的话,你的“回礼”行动就不能成功,还会置自己和你的邮件服务器于死地。你所寄出的电子邮件会永无止境地“反弹”回给你自己,因为这个时候你的发件人和收件人已被认为是你自己,你的邮件服务器忙于处理你的大量的电子邮件的来往交通时,会导致其他用户的交通缓慢下来,延迟了整个过程,如果邮件服务器承受不了这样繁忙的工作,网络随时就会瘫痪。例如流行的 UP Yours 和 KaBoom 等。

因此采取防范电子邮件炸弹措施是非常必要的。安装电子邮件过滤器能有效地阻止电子邮件的攻击。现在有些电子邮件服务器已带有邮件过滤功能。

(3)电子邮件欺骗

电子邮件欺骗行为的表现形式可能各异,但原理相同,通常是骗用户进行一个毁坏性操作或暴露敏感信息(例如口令)。欺骗性电子邮件会制造安全漏洞。电子邮件欺骗行为的一些迹象是:电子邮件假称来自系统管理员,要求用户将他们的口令改变为特定的字串,并威胁如果用户不照此办理,将关闭用户的账户。用户应了解,任何管理人员都不会用电子邮件发出这样的要求。相反的,会发出一份备忘录,或有其他的验证手段。

由于简单邮件传输协议(SMTP)没有验证系统,伪造电子邮件十分方便。如果站点允许与 SMTP 端口联系,任何人都可以与该端口联系并且以其他人的名义发出电子邮件。还有的欺骗方式是发送一封邮件,邮件的附件其实是一个恶意程序或病毒,如“特洛伊木马”等。这些文件常常取一个吸引人的标题,诱使人们去点击。点击后的结果很可能导致用户的计算机被黑客控制。

对于这种欺骗方式,用户应花时间查看电子邮件错误信息,其中经常会有闯入者的线索。注意查看电子邮件信息的表头,它们通常会记录下电子邮件到达目的地前经过的所有“跳跃”或暂停地。注意表头中诸如“接到”和“信息—ID”的信息,并与电子邮件的发出和收到记录比较,看它们是否吻合。

有时,电子邮件阅读器不允许用户看到这些表头。此时,可查看包含原始信息的 ASCII 文件,但小心这些表头也被伪造了。如果闯入者直接与系统的 SMTP 接口连接,系统甚至无法分辨闯入者的来源。

(4)匿名转发

在正常的情况下,发送电子邮件会尽量将发送者的名字和地址包括进邮件的附加信息中。但是,有时发送者希望将邮件发送出去而不希望收件者知道是谁发的。这种发送邮件的方式称为匿名邮件。

实现匿名的一种最简单的方法,是简单地改变电子邮件软件里的发送者的名字。但这是一种表面现象,因为通过信息表头中的其他信息,仍能跟踪发送者。让你的地址完全不出现在邮件中的唯一方法是让其他人发送这封邮件,邮件中的发信地址就变成了转发者的地址了。

3. 安全电子邮件工作模式

一般情况下,安全电子邮件的发送必须经过邮件签名和邮件加密两个过程,而对于接收

到的安全电子邮件,则要经过邮件解密和邮件验证两个过程,其工作模式如图 1-1 所示。

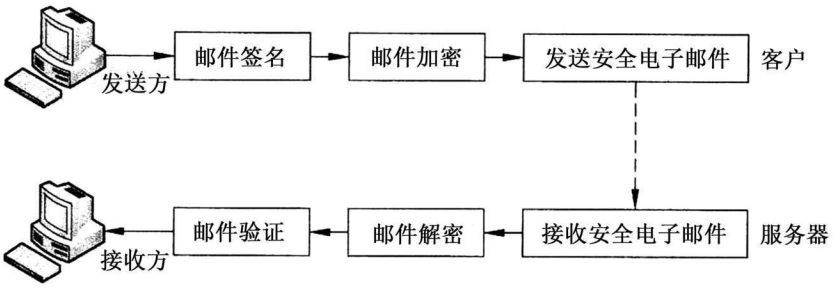

图 1-1 安全电子邮件工作模式

对于邮件加密,需要仔细研究采用什么样的加密算法。对称加密算法简便高效、安全性高,但密钥必须秘密分配,管理大量的密钥十分困难。公开密钥算法虽然密钥分配简单,密钥保存量少,但加、解密速度慢,效率较低。所以在实际应用中可将两种算法结合起来使用,以充分发挥其各自的优势。邮件加密主要提供邮件的保密性,邮件签名主要提供邮件的完整性和不可抵赖性服务。一般地,通过随机生成一个会话密钥,采用对称加密算法加密邮件体,利用消息摘要、公钥技术来实现邮件的签名与验证,通过数字信封技术实现会话密钥的传递。从而有机地将这两种加密技术结合起来,使邮件加密安全高效,同时又具备良好的密钥管理功能。

以下分别介绍邮件签名、邮件加密、邮件解密和邮件验证的具体过程。

(1)邮件签名

对于一封已格式化好的电子邮件(如 MIME 格式),用相应摘要算法(如 MD5、SHA-1)计算其摘要值,然后用发送者的私钥对数字摘要采用相应的公钥算法(如 RSA)加密得到该邮件的数字签名,最后合成数字签名和原邮件体得到已签名的邮件。对普通邮件进行签名的过程如图 1-2 所示。

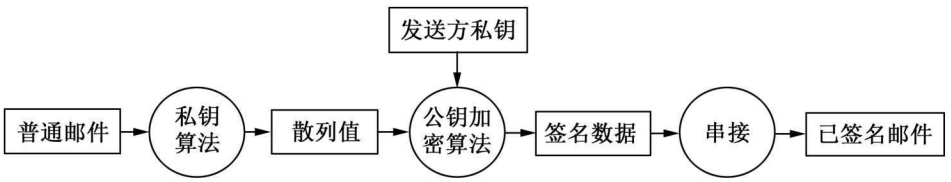

图 1-2 邮件签名过程

(2)邮件加密

只实现了数字签名的邮件在传送中仍然是明文,邮件有可能在传送过程中被截获而泄密,因此还必须对其加密,使其在传送过程中传送的是密文。这样即使邮件中途被截获,截获者得到的也只是密文,从而保证了邮件内容的安全性。对签名邮件进行加密的过程如图 1-3 所示。

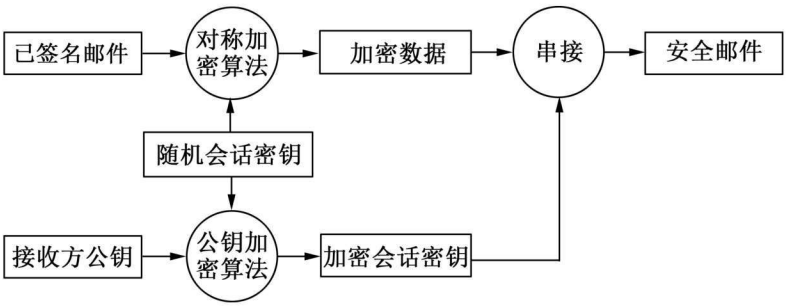

图 1-3　邮件加密过程

(3)邮件解密

当收到一封安全电子邮件后,首先将邮件按照相关协议拆分为两个部分(一部分为经相应公钥算法加密后的会话密钥,另一部分是经相应对称加密算法加密后的签名邮件),然后用收件人的私钥解密会话密钥,最后用会话密钥解密加密的邮件得到明文的签名邮件。对安全邮件进行解密的过程如图 1-4 所示。

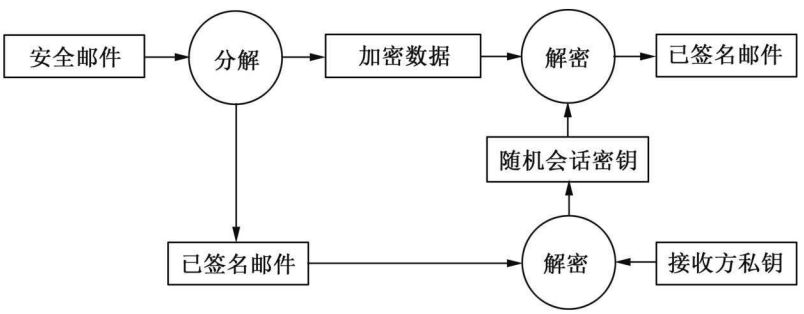

图 1-4　邮件解密过程

(4)邮件验证

当邮件接收者得到签名邮件后,首先按照相关协议将邮件拆分为数字签名和原始邮件两部分,然后用发送者的公钥对数字签名进行解密得到数字摘要,同时对得到的原始邮件利用相应的摘要算法重新计算其数字摘要,将两个数字摘要进行比较。如果相等,则邮件通过完整性验证,确实来源于邮件声称的发送方;否则,邮件验证失败,该邮件不可信。对邮件进行验证的过程如图 1-5 所示。

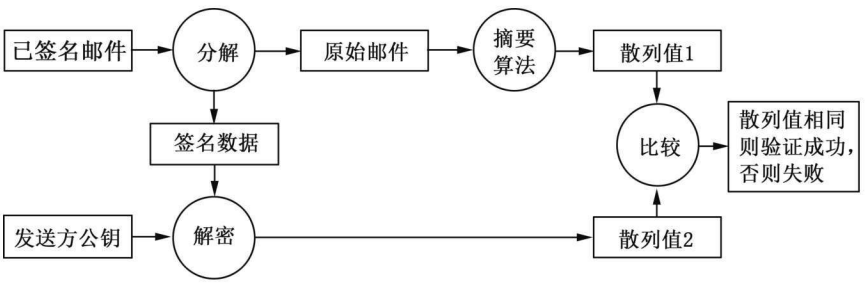

图 1-5　邮件验证过程