21世纪高等学校规划教材

WANGLUO ANQUAN YUANLI YU YINGYONG

网络安全原理与应用

闫大顺　石玉强　主　编
刘磊安　邹　莹　李　晟　副主编

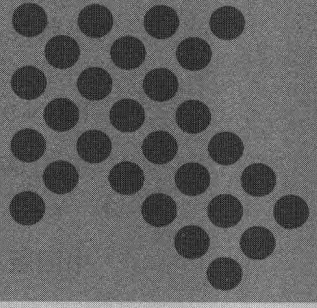
中国电力出版社
http://jc.cepp.com.cn

21世纪高等学校规划教材

WANGLUO ANQUAN YUANLI YU YINGYONG

网络安全原理与应用

主　编　闫大顺　石玉强
副主编　刘磊安　邹　莹　李　晟
主　审　赵春晓



中国电力出版社
http://jc.cepp.com.cn

内 容 提 要

本书为21世纪高等学校规划教材。

本书主要从网络安全的基本原理和实践技术两个方面，系统分析了网络安全各种常见的安全威胁，提出了网络安全原理的本质，给出了网络安全的各种主要防御技术。全书从网络安全体系上分三部分：第一部分，计算机网络安全基础，介绍网络安全概述、物理安全、网络协议安全和网络攻击；第二部分，主动防御技术，包括密码编码学基础、数字认证、PKI与PMI、身份认证、VPN技术、Web安全、操作系统及软件平台安全；第三部分，被动防御技术，包括计算机病毒及其防范、防火墙、入侵检测等。本书既注重基本原理的阐述，又关注网络安全的新动向，适时增加了实践的新技术。每章最后都配有习题，用来检查学习效果。本书重点突出、难易适当、实例丰富、实用性强。

本书可作为高等院校计算机科学与技术等专业网络安全、计算机系统安全等课程的教材，也可供从事网络安全研究和计算机系统安全管理等领域的人员参考。

图书在版编目（CIP）数据

网络安全原理与应用/闫大顺，石玉强主编．—北京：中国电力出版社，2010.6

21世纪高等学校规划教材

ISBN 978-7-5123-0341-6

Ⅰ.①网… Ⅱ.①闫…②石… 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（2010）第070795号

中国电力出版社出版、发行

（北京三里河路6号 100044 http://jc.cepp.com.cn）

航远印刷有限公司印刷

各地新华书店经售

*

2010年7月第一版 2010年7月北京第一次印刷

787毫米×1092毫米 16开本 22印张 533千字

印数0001—3000册 定价 **35.20**元

前 言

随着信息技术的广泛应用和发展，人们对计算机和网络的依赖性越来越大，信息被暴露和非法使用、网络受到攻击的可能性也变得越来越大。随着经济全球化、军事指挥网络化，安全可靠的网络空间已经成为支撑国民经济、关键性基础设施以及国防的支柱。一个国家的网络信息获取能力和网络信息安全保障能力已成为21世纪的综合国力、经济竞争能力和生存能力的重要组成部分，呈上升趋势的网络安全事件已成为信息社会十分突出的问题。

网络安全本质上就是计算机网络上的信息安全，是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或恶意的原因而遭到破坏、更改、泄露，系统连续可靠地运行，网络服务不中断。通过网络安全原理的分析，结合网络安全的实践技术，能够给个人或企业用户使用计算机网络时提供数据传递的机密性、完整性、真实性，保护用户的利益和隐私；也能够给网络运行和管理者提供有效的、安全的网络访问、读写等操作，保护网络资源和服务。

网络安全的概念是与时俱进的，历经了可靠性、保密、保护，而发展到今天的网络信息保障。本书从技术的角度介绍了网络安全保障体系，从应用的角度介绍了提高网络安全的各种措施和技术，并进一步强调网络安全是一个动态的整体安全。本书力图全面、系统、深入地介绍网络安全原理及其应用的相关知识，主要体现在以下几个方面。

(1) 体系完整，内容全面。本书内容全面，突出知识体系的完整性，并用通俗易懂的语言讲述抽象的理论。

(2) 图文并茂，示例丰富。本书图文并茂，精心选取常见示例帮助读者理解相关理论概念。

(3) 循序渐进、深入浅出。本书内容讲解循序渐进，深入浅出，概念清晰，条理性强，符合读者学习网络安全原理的认识规律。

(4) 理论与技术联系密切。全书围绕网络安全原理与应用技术两个核心点展开。叙述基础理论时易懂易学；介绍应用技术时详尽周密。理论与技术的密切结合是本书的一大特色。

本书由闫大顺、石玉强主编，负责全书内容的取材和组织，闫大顺编写了第1章和第14章的第1、第2节，石玉强编写了第4章的第1、第2节和第8章，刘磊安编写了第4章的第3、第4节和第12章，杜淑琴编写了第2、第3章，邹莹编写了第5、第6章，刘佳编写了第7、第9章，邹娟编写了第10章，谢芳清编写了第11章，李晟编写了第13章及第14章的第3节，参编的还有王洁、高杨、张海强、陈滢生等。另外，编者感谢曹天杰教授、沈玉利教授、吴家培副教授给予的指导和各种不同形式的帮助。本书由赵春晓主审。

由于作者水平有限，书中难免有不妥和错误之处，衷心希望读者与同行批评指正。编者信箱：NetworkSecurity09@163.com。

编 者

2010年3月

目　录

第1章　网络安全概述

教学提示

随着计算机网络的迅猛发展和广泛应用，网络安全问题成了整个社会日益关注的核心问题，倘若网络存在大量的安全问题，不仅使机器无法正常工作，还将导致信息的泄密，从而影响国家的经济、金融和军事的安全。本章概要阐述了网络安全问题产生的根源，对当前各种网络威胁进行多种角度的分类，引出网络安全的概念，着重介绍了网络安全的目标。本章从网络安全体系结构和网络安全模型两个侧面论述网络安全，并给出设计安全的网络的基本规则，详细介绍了提高网络安全采用的多种防御技术以及今后网络安全发展的方向。

教学重点

分析当前各种网络安全威胁，引出网络安全的目标，给出多层次的网络安全体系结构和网络安全模型。基于安全性描述了网络安全的各种防御技术。

1.1　网络安全问题

随着社会经济和科学技术的飞速发展，信息技术和计算机网络正大幅度对传统行业的生产、营销和管理模式产生改变，同时也促使相关的新产业诞生与快速成长，以计算机网络进行交流的信息已成为国家和社会发展的重要战略资源。迄今为止，信息技术与计算机网络已经更深地融合到国家的政治、经济、军事、交通、通信、卫生、文教等诸多领域，以电子商务、电子政务、电子税务、电子银行、电子海关、电子证券、网络书店、网上拍卖、网络购物、网络防伪、远程教育、远程医疗、网上交易、网络监控、网络营销、网上选举、网上娱乐等形式发挥越来越大的作用。为此在计算机网络中存储、传输和处理的海量信息中有许多是商业经济信息、银行转账、股票证券、军事国防数据、科研数据等敏感信息或机密信息，开放式的计算机网络自然吸引各式各样怀有不同目的攻击，来窃取信息、泄露信息、修改和删除信息，每年都带来极大的损失。因此计算机网络安全是一个关系到国家的安全、社会的稳定、民族文化的继承和发扬的重要问题，其重要性正随着全球信息化步伐的加快而变得越来越重要。

随着 Internet 的广泛应用，网络上出现的安全问题越来越多、越来越严重。第一起网络安全事件是 1986 年初在巴基斯坦的拉合尔（Lahore），巴锡特（Basit）和阿姆杰德（Amjad）两兄弟编写的 Pakistan 病毒（Brain）在一年内流传到了世界各地。从此之后爆发了众多的网络攻击事件，如网络蠕虫病毒感染、主机被控制、数据库被非法访问、Web 服务器网页被更改、非法电子银行转账等。事实上，相当多的网络入侵或攻击并没有被发现。即使被发现了，由于这样或那样的原因，人们并不愿意公开它。这说明世界上没有绝对安全的网络，只要用户使用联网的计算机或其他接入设备以及网络连接了 Internet，它就存在危险，要使用网络就必须考虑它的安全问题。

1.1.1 网络安全威胁

网络安全的潜在威胁是形形色色的，有的是人为故意的，有的是非故意的；有的是恶意的，有的是非恶意的；有的是来自系统内部的网络攻击，有的是来自网络外部的攻击。网络安全威胁是指对计算机网络的一种潜在的侵害。一般认为，目前计算机网络和信息安全面临的威胁主要表现在三类：信息泄露、信息破坏和拒绝服务。其中信息泄露、信息破坏也可能造成系统拒绝服务。现在从四个方面对网络安全的威胁进行分类，便于对威胁的识别与防护。

1. 按照网络安全威胁表现形式的分类

从威胁的表现形式上大致分为 12 类。

(1) 非法访问。非法访问是指未经授权就使用网络资源或者以未授权的方式获得了某个对象的服务。未授权访问通常是在不安全通道上截获正在传输的信息或者利用对象的固有弱点来实现的，入侵者有意避开系统访问控制机制，对网络设备及资源进行非正常使用，或擅自扩大权限，越权访问信息。它主要有以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作，也有合法用户以未授权方式进行操作等。

(2) 拒绝服务。拒绝服务 DOS (Denial of Service) 是指网络系统的可用性遭到破坏，使合法用户不能正常访问网络资源，或者使有严格时间要求的服务不能及时得到响应。系统被中断的原因可能是被破坏或暂时性不可以使用。当一个实体不能执行它的正当功能，或它的动作妨碍了别的实体执行它们的正当功能的时候便发生拒绝服务。这种攻击可能是一般性的，比如一个实体抑制所有的消息；也可能是有具体目标的，可以是一个实体抑制所有流向某一特定目的端的消息，如安全审计服务。DOS 攻击可以是对通信业务流的抑制，或产生额外的通信业务流，也可能制造出试图破坏网络操作的消息。特别在具有中继实体的网络，由于这些中继实体根据从别的中继实体那里接收到的状态报告来做出路由选择的决定从而破坏网络操作。

(3) 截取。截取是信息泄露的一种形式，它可以通过直接搭到通信线路、拦截广播数据包、接收电磁波辐射信号进行实施。对截取的预防非常困难，发现截取几乎不可能，其会造成严重的危害性。非授权者是利用信息处理、传送、存储中存在的安全漏洞截收或窃取各种信息。例如卫星、无线局域网等无线信号可方便进行窃收，因此必须加以重视。中国有关部门明确规定，在无线信道上传输秘密信息时必须安装加密机进行加密保护。

(4) 篡改。非授权者用各种手段对信息系统中的数据进行增加、修改、删除、插入等非授权操作，破坏数据的完整性，以达到其恶意目的。当所传送的内容被改变而未发觉，并导致一种非授权后果时出现消息篡改。例如非法用户能够接收银行的交易信息，通过修改账户的数据，就可以把资金转移到自己的账号中。

(5) 冒充。冒充是指通过出示伪造的凭证来冒充别的对象，进入系统盗窃信息或进行破坏。冒充攻击的表现形式主要有盗窃密钥、访问明码形式的口令或者记录授权序列并在以后重放，也可以冒充领导发布命令、调阅文件，冒充主机欺骗合法主机及合法用户。冒充具有很大的危害性，因为它回避了用于结构化授权访问的信任关系。

冒充通常与其他的主动攻击形式一起使用，特别是消息的重演与篡改，构成对用户的诈骗。例如，鉴别序列能够被截获，并在一个有效的鉴别序列发生之后被重演。特权很少的实体为了得到额外的特权可能使用冒充装扮成具有这些特权的实体。

冒充带来极大的危害。以冒充的身份访问网络系统，非授权用户 A 声称是另一用户 B，然后以 B 的名义访问服务与资源，A 窃取了 B 的合法利益，如果 A 破坏了计算机系统，则 A 不会承担责任，这必然损坏了 B 的声誉。再如进程 A 以伪装的身份欺骗与它通信的进程 B，如伪装成著名的售货商的进程要求购物进程提供信用卡号、银行账号，这不仅损害购物者的利益，也损害了售货商的声誉。总之冒充通过越权使用网络设备和资源，接管合法用户，欺骗系统，占有合法用户的资源，是网络安全中威胁最大的形式之一。

（6）抵赖。抵赖，通常是网络的实体之间交流信息之后，否认自己曾经发送过消息或者否认自己发送过某些内容或者接收者事后否认曾经接收过某些信息。可以说抵赖行为发生在通信中，涉及到的那些实体之一事后不承认参加了该通信的全部或一部分，不管原因是故意的还是意外的，都会导致严重的争执，造成责任混乱。

（7）重放。在网络上截取一个消息或部分消息的数据流，该消息中包含了重要的信息或者授权信息，在必要的时候非法入侵者把该数据流重新发送到消息目的地而非法获取授权，或者达到恶意的目的，以搅乱系统的正常运行，这就是消息的重放。由于重放的数据是合法信息，因而如果不采取有效措施，将难以辨认真伪。例如，一个含有鉴别信息的有效消息可能为另一个实体所重演，目的是鉴别它自己（把它当做其他实体）。恶意系统可以克隆一个实体或实体产生的信息。如截获订单，然后反复发出订单。

（8）数据分析。在网络上非法截取的数据由于加密，无法获得数据包含的信息。非法入侵者可以通过对网络中的信息流、流向、通信频度和长度等参数的分析来掌握信息网络或整体部署的敏感信息。虽然这种攻击没有窃取到信息内容，但仍然可获取许多有价值的情报。由于窃取通常是被动的形式，隐蔽性比较强，通信者由于采用了加密而警惕性降低，造成的安全威胁更大。

（9）隐蔽信道。在计算机网络中服务系统或者应用系统，经常设计一些信道来合法传送信息，这些信道为公开通道。隐蔽信道是通过公开通道传送隐蔽信息的一种秘密方法，即信息隐藏。隐蔽信道通常也称为阈下信道，或者隐通道。未经授权的用户也可以用隐蔽信道传送机密信息，从而比较容易地躲开网络安全检查。例如公司的高级经理要用文件名传送公司财务或战略信息时，将文件名编码加密。如果网络系统允许文件名对外部用户是可访问的，则未经授权用户可将收到的在文件名中编码的信息解码，从而了解信息内容。用于传送文件名的信道可能被滥用为传输某些秘密信息。

（10）逻辑炸弹。逻辑炸弹是指修改了应用系统的可执行程序，使它在某种特殊条件下按某种不同的方式运行。在正常条件下程序运行正常，如果某种触发条件出现，系统就会按不同于预期的方式运行。预防逻辑炸弹几乎不可能，发现也很困难，破坏性极大。比如一些正规的软件开发商为了防止盗版软件的使用而在程序中放置了逻辑炸弹，当盗版软件运行过程造成死机或者修改、删除计算机上的数据，造成的危害比较大，这也是法律所不允许的。

（11）后门。后门是不用经过授权就可以进入应用系统或者获得网络服务的一种方法。后门通常是由系统的设计者在应用系统开发时，为了方便直接使用系统的功能而故意设置机关，用以监视计算机系统，有时也因偶然考虑不周而造成后门。后门也是程序设计、调试、测试或维修期间编程员使用的常用检验手段。例如当程序运行时，在正确的时间按下正确的键，或提供正确的参数，就会对预定的事件或事件序列产生非授权的影响。发现后门非常困难。因为证明程序满足规范的要求是困难的，证明在任何其他情况下，该程序不做任何别的

事情是更困难的。

(12) 恶意代码。恶意代码包括病毒、蠕虫、特洛伊木马、恶意 Java 程序、愚弄程序、恶意 ActiveX 控件以及 Web 脚本等。如 Web 页面放入了恶意代码，在访问者不知情的情况下，自动修改 Internet Explorer 浏览器默认首页、标题内容、鼠标右键项目等，给正常的 Web 访问带来严重的影响。在网络上提供的正版软件的非法下载，开源软件、绿色软件、共享软件的非正规提供商通常为了获得非法利益而绑定了恶意代码。

2. 按照威胁来源的分类

造成网络安全的威胁的原因可能是多方面的，有来自外部，也有可能来自企业网络内部。从威胁的来源看可分为内部威胁和外部威胁。

(1) 内部威胁。按照中国互联网信息中心（China Internet Network Information Center）的统计，多半的计算机犯罪都和系统安全遭受损害的内部攻击有密切的关系。内部人员对单位的运作、系统结构、防护手段熟悉，导致攻击不易被发觉，内部人员最容易接触敏感信息，危害的往往是单位最核心的数据、资源等。各单位的信息安全保护往往是在网络边缘设置强大的防护措施，假定内部网络是安全的，为此给内部人员的非法使用资源提供了方便。要防止内部威胁应该对工作人员进行仔细审查；制定完善的安全策略；增强访问控制系统；审计跟踪以提高检测出这种攻击的可能性。

(2) 外部威胁。来自互联网其他部分的威胁称为外部威胁，威胁的实施也称远程攻击。外部网络是互联的，受到各种利益的引诱，全球范围内不同类型的人员采用各种方法对内部系统实施攻击，现在的外部威胁不再是单个人员的作战，有了协作远程攻击的趋势，给防止外部的网络威胁带来了更大的困难。

3. 按照造成威胁的结果形式的分类

从造成的结果上看可以分成主动威胁和被动威胁。

(1) 被动威胁。这种威胁是对信息的非授权泄露而未改变系统状态。如信息窃取、密码破译、信息流量分析等。被动威胁的实现不会导致对系统中所含信息的任何篡改，而且系统的操作与状态也不受改变，但有用的信息可能被盗窃并被用于非法目的。例如通过网络攻击手段获取电子商务系统中供货商的信息，或者价格信息，或者公司的营销策略，出售给竞争对手，这对于电子商务公司都是非常严重的打击。由于被动威胁对系统的影响非常小，甚至没有任何影响，从而变得非常隐蔽，对这类威胁的防护变得非常不容易。

(2) 主动威胁。这种威胁是对系统的状态进行故意的非授权的篡改，比如对网络通信中数据的增删改，对应用系统运行所依赖的系统进行增删改，对应用系统中所含信息的篡改，或对系统的状态或操作的改变，或者对网络设备的故意损坏等，造成网络系统的直接危害。非法人员实施的主动攻击会直接进入应用系统内部，往往可影响整个系统的运行、造成巨大的损失，可能给网络带来灾难性的后果，比如非法人员攻击核心 DNS 服务器，可以造成网站不能正常得到访问，修改核心路由器的路由信息致使网络不能正常使用等。

4. 按照安全威胁的动机的分类

从威胁的动机上看分为偶发性威胁与故意性威胁。

(1) 偶发性威胁。偶发性威胁是指那些不带预谋的威胁，是由于偶然因素影响了网络系统的正常运行，比如网络设备所在地突然发生了自然灾害、系统硬件故障和软件出错等。人为的无意失误包括：操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选

择不慎，用户将自己的账号随意转借他人或与他人共享等都会对网络安全带来威胁。

（2）故意性威胁。故意性威胁是指对网络的有目的、有策划实施的威胁。网络安全事件涉及到网络威胁多数是故意性的威胁，故意性威胁包括的内容非常多，其范围可从使用易用的监视工具进行随意的检测到使用特别的系统知识进行精心的攻击。故意性威胁是网络安全研究的核心，必须给网络系统设计合理的安全防护技术，抵御故意性的威胁。

1.1.2 影响网络安全的因素

计算机网络提供了资源共享性、系统的可靠性、工作的效率和系统的可扩充性；同时也正是这些特点增加了网络安全的脆弱性和复杂性，资源共享和分布式服务增加了网络受威胁和攻击的可能性。本书从三个主要方面分析影响网络安全的主要因素，便于在网络设计时提高安全。

1. 网络硬件设备和线路的安全问题

（1）网络脆弱性。从计算机网络设计与建设之初，网络就缺乏总体安全构想，网络体系结构的各个层次都存在大量的安全隐患。网络系统的易欺骗性、易被监控性、薄弱的认证环节、有缺陷的局域网服务和相互信任的主机、系统主机的复杂设置和控制，这些都使得计算机网络容易遭受到威胁和攻击。特别是在设计互联网之初就缺乏对安全性的总体设计，所用的 TCP/IP 协议族是建立在理想的可信环境之下，主要考虑的是网络互联可靠性，尽最大能力来传输数据，在安全方面则缺乏整体考虑。这种基于网络地址的 TCP/IP 协议族本身就会泄露敏感数据，而且该协议是完全公开的，任何人可以分析以寻找漏洞，远程访问使许多攻击者无须到现场就能够实施。网络通信的脆弱性致使黑客具备攻击的可能性，这就是造成网络不安全的根源。

（2）电磁泄漏。网络端口、传输线路和处理机都有可能因屏蔽不严或未屏蔽而造成电磁泄漏。目前，大多数机房屏蔽和防辐射设施都不健全，通信线路也同样容易出现信息泄露。现在能够在 200m 之外接收到 CRT 显示器的电磁辐射，能够把显示器上的信息完整地显示出来。因为电磁泄漏非常隐蔽，当前也不是很注意，所以安全问题很严重。

（3）搭线窃听。随着信息传递量的不断增加，传递数据的密级也在不断提高，犯罪分子为了获取大量情报，可监听通信线路，非法接收信息。计算机网络的主干网络都是采用光纤模式，虽然从一定程度上限制了搭线窃听，但仍然存在窃听的威胁。城域网、局域网和接入网很多是采用了金属介质为导体，甚至采用无线传输模式，大大增加了搭线窃听的危险。

（4）非法终端。有可能在现有终端上并接一个终端或合法用户从网上断开时，非法用户乘机接入，并操纵该计算机通信接口或由于某种原因使信息传到非法终端。

（5）非法入侵。非法分子通过技术渗透或利用电话线侵入网络，非法使用、破坏或获取数据或系统资源。目前的网络系统大都采用口令验证机制来防止非法访问，一旦口令被窃，就无安全可言。

（6）注入非法信息。通过网线等通信线路有预谋地注入非法信息，截获所传信息，再删除原有信息或注入非法信息后再发出，使接收者收到错误信息。

（7）线路干扰。当公共转接载波设备陈旧和通信线路质量低劣时，会产生线路干扰。如调制解调器会随着传输速率的上升，错误迅速增加。同样非法分子可以使用各种设备对线路进行电磁干扰，攻击网络通信。

（8）意外原因。包括人为地对网络设备进行破坏、设备偶然出现故障。如在处理非预期

中断过程中，通信方式留在内存中未被保护的信息段在通信方式意外出错时，被传到别的终端上，造成信息泄露。

2. 网络系统和软件的安全问题

计算机网络是由网络硬件设备和软件系统构成的，各种软件都有可能存在漏洞，造成了网络的不安全。网络系统和软件的主要问题有以下 7 种。

（1）网络软件系统的漏洞或缺陷被利用，使网络遭到入侵和破坏。操作系统是最为核心的软件，操作系统漏洞造成的安全问题也更为严重。

（2）网络系统的软件安全功能不健全，比如采用安全性不高的软件防火墙，致使主动攻击非常容易达到目标。应加安全措施的软件可能未给予标识和保护；重要的软件系统可能没有安全措施，使软件非法使用或破坏或产生错误结果。对软件更改的要求没有充分理解，导致软件缺陷。

（3）未对用户进行分类和标识，使数据的存取未受限制和控制，因此被非法用户窃取数据或非法处理用户数据。由于数据库是很多应用系统的运行基础，对数据库软件的分析越来越多，发现的漏洞及安全问题越来越多，造成了很多网络的安全问题，比如电子商务网站保存的信用卡信息的泄露等。

（4）错误地进行路由选择，为一个用户与另一个用户之间的通信选择了不合适的路径。拒绝服务，中断或妨碍通信，延误对时间要求较高的操作，造成网络安全问题。

（5）没有正确的安全策略和安全机制，缺乏先进的安全工具和手段。

（6）不妥当的文档管理，导致所修改的程序出现版本错误。如程序员没有保存程序变更的记录，没有做拷贝，未建立保存记录的业务。

（7）病毒和蠕虫入侵，计算机病毒能以多种方式侵入计算机网络，并不断繁殖，然后扩散到网络上的计算机来破坏系统。轻者使系统出错，重者可使整个系统瘫痪或崩溃。

3. 网络管理人员的安全意识问题

可以采用各种手段来提高网络设备和计算机设备的安全性，也可以采用安全的软件来实现应用系统的运行，但是整个系统的管理、维护都是需要操作人员来实施，甚至网络安全机制也是网络管理人员来实现的。操作人员的素质高低以及管理制度的严格与松散就直接决定了整个网络系统的安全性。

（1）网络管理人员保密观念不强或不懂保密规则，无意泄露机密信息，例如，打印、复制机密文件；随便打印出系统密码或向无关人员泄露有关机密信息；或者把密码保存到计算机系统中，甚至记录到随身的笔记本上，都非常容易泄露秘密。

（2）网络管理人员业务不熟练，因操作失误使文件出错或误发或因未遵守操作规程而造成泄密。

（3）因规章制度不健全造成人为泄密事故。如网络上的规章制度不严，对机密文件管理不善，各种文件存放混乱，违章操作等造成不良后果。

（4）网络管理人员素质差，缺乏责任心，没有良好的工作态度，明知故犯或有意破坏网络系统和设备。

（5）熟悉系统的工作人员故意改动软件或用非法手段访问系统或通过窃取他人的口令字和用户标识码来非法获取信息。

（6）身份证被窃取，从而使一个或多个参与通信的用户身份证很容易被他人窃取，继而

被非法使用。

(7) 利用硬件的故障部位和软件的错误非法访问系统或对系统各部分进行破坏。

(8) 利用窃取系统的磁盘、磁带或纸带等记录载体或利用废弃的打印纸、复写纸来窃取系统或用户的信息。

(9) 由于网络管理人员的操作不当、误用媒体、设置错误造成的操作失误，致使网络变得不安全。

除了上述因素之外，还有环境因素影响着网络的安全，如地震、火灾、水灾、风灾等自然灾害或掉电、停电等事故。网络系统中各种设备的环境和场地条件，如温度、湿度、电源、地线和其他防护设施不良造成的网络安全。也可能由于硬件设备的突然故障、断电或者电源波动大、测不到的软件错误或者缺陷致使网络受到安全的威胁。

因此，为了保证网络安全，必须从网络设备、硬件、软件、操作人员等多方面高度重视，从法律保护和技术上采取一系列安全和保护措施来提高网络的安全。

1.1.3 网络安全的目标

从专业角度看，网络安全是一个涉及网络技术、计算机科学、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的边缘性综合学科。

计算机网络（Computer Network）是由计算节点和传输网络的软硬件构成的，完成数据的处理、存储、传输等功能。网络安全（Computer Network Security）是指将计算机网络的服务与共享资源的脆弱性降低到最低限度。网络安全为数据安全传输而建立和采取的技术和管理的安全保护，保护计算机网络硬件、软件数据不因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。在 ISO7498-2 开放系统安全架构中提出，要解决网络安全问题，需要在四方面提供服务，而 IATF 则要求网络具备八个方面的性质。本文是从六个主要属性来描述网络安全要达到的目标。

1. 秘密性

秘密性是指防止信息被非法获得，确保信息不暴露给未授权的用户、实体或进程。即秘密性保证了信息不能被非授权访问，也就是信息的内容不会被未授权的第三方所知、所使用。这里所指的信息不但包括国家军事经济秘密，而且包括各种企事业单位的工作秘密、商业秘密以及个人秘密。防止信息失窃和泄露的保障技术称为保密技术。通常通过访问控制阻止非法授权用户获得秘密信息，通过加密变换阻止非授权用户获知信息内容。

2. 完整性

完整性就是网络信息未经授权不能被改变的特性。即网络信息在存储或传输过程中不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。网络必须保证信息没有被第三方修改，如果被篡改就能判断出来。完整性就是要求保持信息的原样，即信息的正确生成、正确存储和正确传输。完整性与秘密性不同，信息的完整性不一定要求秘密性，比如政府的公告文件发布到网络上，必须要求各个网站上的电子版必须保证完整性，即没有任何改动，这样文件才能正确传达政策信息。有的时候保证信息的秘密性也需要保证信息的完整性，这时秘密性与完整性都是网络信息都必须具备的。要保证信息的完整性，特别是在开放的互联网上，要依靠协议、纠错编码、秘密校验、数字签名等技术来保障。

3. 可用性

可用性就是网络信息可被授权的用户、实体和进程在需要时可访问的特性，即网络的资

源和服务在需要时允许授权用户或实体使用的特性，即使网络部分受损或者需求降级时仍能为授权用户提供有效服务的特性。可用性是指无论何时，只要用户需要，网络信息必须是可用的，也就是说网络系统不能拒绝服务。网络最基本的功能是向用户提供所需的信息和通信服务，而用户的通信要求是随机的、多方面的（如话音、数据、文字和图像等），有时还要求时效性，网络还必须随时满足用户通信的要求。可用性是网络信息资源服务功能和性能的可靠性度量，涉及网络信息系统面向用户的安全性，以及物理设备、网络、系统、数据、应用和用户等多方面的因素，是对信息网络总体可靠性的总体要求。可用性一般采用系统正常使用时间和整个工作时间之比来度量。攻击者通常采用占用资源的手段阻碍授权者的工作。可以使用身份识别与确认、业务流控制、访问控制机制、路由选择控制、审计跟踪来保证网络系统的可用性。增强可用性还包括如何有效地避免因各种灾害（战争、地震等）造成的系统失效。

4. 不可抵赖性

不可抵赖性也称作不可否认性或抗否认性，是面向通信双方（用户、实体或进程）信息真实同一的安全要求，它保障用户无法在事后否认曾经对信息进行的生成、签发、接收等行为，也就是收、发双方均不能对自己的行为抵赖。一是信息源证据，它提供给信息接收者以证据，这将使发送者谎称未发送过这些信息或者否认它的内容的企图不能得逞；二是递交接收证据，它提供给信息发送者，这将使接收者谎称未接收过这些信息或者否认它的内容的企图不能得逞。不可抵赖性一般是通过数字签名来提供。

5. 可控性

可控性是对信息的传播及内容具有控制能力，也就是对网络信息及网络信息系统实施安全监控。为此在网络系统中要根据需要或者实际情况把网络划分成不同的安全等级，通过各种安全技术控制输入，满足信息安全等级的需求。如果网络系统通过现有技术能够达到网络状态的完全控制，则称网络系统是可控的，如果通过现有的技术不能达到某个网络系统的安全等级或者达到了部分要求，则称对该网络系统是部分可控的；如果通过现有技术不能满足对网络系统最低的安全等级，则称对该网络系统是不可控的。为此需要管理机构对危害国家、社会、军事等重要信息的流向、传播及行为方式，通过对网络上信息系统实施安全监控，控制网络资源的使用及使用资源的人员、实体或进程的使用方式。

6. 真实性

网络中的信息，组成网络的各种软硬件设备以及使用网络的人员、实体或进程的身份都需要经过权威部分的鉴定，来保证信息的来源、信息的内容、实体的身份、用户身份、进程的标记是真实的、可信的。要达到真实性要采用信息内容的鉴别、实体鉴别和身份鉴别等各种鉴别手段。同时鉴别也是保证信息秘密性、不可否认性、完整性的前提，没有合法、有效的身份证明或数据来源证明，是不允许对网络系统进行任何操作的。因此，保证信息和网络的真实性，是实现信息的其他安全属性的根本要求。

7. 可靠性

可靠性是指网络系统在规定条件下和规定时间内、完成规定功能的概率。可靠性是网络安全的基本要求之一，网络不可靠，事故不断，也就谈不上网络的安全。目前，对于网络可靠性的研究基本上偏重于硬件可靠性方面。研制高可靠性元器件设备，采取合理的冗余备份措施仍是最基本的可靠性对策，然而，有许多故障和事故，则与软件可靠性、人员可靠性和

环境可靠性有关。

8. 可审查性

可审查性是使用审计、监控、防抵赖等安全机制，使得使用者的行为有证可查，并能够对网络出现的安全问题提供调查依据和手段。审计是通过对网络上发生的各种访问情况记录日志，并对日志进行统计分析，是对资源使用情况进行事后分析的有效手段，也是发现和追踪事件的常用措施。审计的主要对象为用户、主机和节点，主要内容为访问的主体、客体、时间和成败情况等。

要在安全法律、法规、政策的支持与指导下，通过采用合适的安全技术与安全管理措施，来保障网络安全。为此要保障计算机及其配套的设备、设施（含网络）的安全，运行环境的安全，保障信息的安全，保障计算机功能的正常发挥，以及网络系统的安全运行。

1.2 网络安全体系

随着计算机网络的不断发展，全球信息化已成为人类发展的大趋势。但由于计算机网络具有连接形式多样性、终端分布不均匀性和网络的开放性、互联性等特征，致使网络易受黑客、恶意软件和其他不轨行为的攻击，所以网上信息的安全和保密是一个至关重要的问题。对于军用的自动化指挥网络、C3I 系统和银行、证券等传输敏感数据的计算机网络系统而言，其网上信息的安全和保密尤为重要。因此，计算机网络必须有足够强的安全措施，需要一个完整的网络安全体系结构，否则该网络将是个无用，甚至会危及国家安全的网络。无论是在局域网还是在广域网中，都存在着自然和人为等诸多因素造成的安全脆弱性和潜在威胁。为此要从网络安全体系的各个层面来分析网络安全的实现，同时给出三种网络安全模型，来对网络安全体系进行研究与部署。

1.2.1 网络安全体系层次与实现

一般的网络系统都要涉及网络设施、网络操作系统和网络应用程序，仅仅从这三个方面保护网络不能完全保证网络的整体安全。因为在网络中信息是核心，如何保证数据的安全性以及使用这些信息的用户、实体和进程的安全性也是必须考虑，只有从这五个层次综合考虑，才能从整体上做到安全的防护。基于五层的网络系统安全体系理论已得到了国际网络安全界的广泛承认和支持，均已将这一安全体系理论应用在其产品之中。下面就将对每层的安全问题做出简单的阐述和分析。

1. 网络的安全性

网络安全性（Network Security）问题的核心是计算机网络能不能被有效控制，具体来讲就是如何控制用户接入计算机网络？是否需要认证？如果能够合理控制网络用户的接入，使合理的用户正常使用网络，有效验证用户身份，从而能拒绝非法用户，这样就为计算机网络的使用构建了简单方便的环境。

在互联网中用户对网络系统进行访问的时候，每一个用户都会拥有一个独立的 IPv4 地址，该 IPv4 地址能够大致表明用户的来源所在地。网络服务系统通过对来源 IP 地址进行分析，便能够初步判断来自该 IPv4 地址的数据是否安全，是否会对本网络系统造成危害，以及来自该 IPv4 地址的用户是否有权使用本网络的数据。一旦发现某些数据来自于不可信任的 IPv4 地址，系统便会自动将这些数据阻挡在系统之外；并且大多数系统能够自动记录那

些曾经造成过危害的 IPv4 地址，使得它们的数据将无法第二次造成危害。

当前大规模的互联网络致使对 IPv4 地址的有效验证变得非常吃力，非法用户可以盗用合法的 IPv4 地址使用网络服务，采用 IPv4 地址验证功能性就会降低。当前使用的 TCP/IP 协议族是为了使用更加简单、易扩展、尽力传送而设计的，这也带来很多问题，比如 IPv4 地址的验证就没有包括在互联网的协议中，给现在的 Internet 网络带来一系列的安全缺陷。为此要对现有的互联网结构进行改造，或者对协议族的某些协议修订来提高网络的安全性，比如引入 IPv6、IPSec 协议、TLS 协议等。

2. 系统的安全性

系统安全性（System Security）主要问题是计算机系统受到安全威胁，计算机软硬件系统遭到破坏或者计算机系统遭到入侵致使信息泄露。影响系统安全的主要是病毒和黑客的威胁和破坏。

随着绝大多数的计算机接入到计算机网络中，病毒对计算机系统的感染已经从过去的移动存储介质转变为网络入侵。因为网络时时刻刻都与计算机系统关联，病毒感染的速度变得更加快，在一个局部网络，如果一台计算机感染了病毒，很快网络中其他计算机也会感染病毒，因为局部网络中计算机是相互信任的，提高了病毒感染的速度。同时电子邮件、文件传输以及 Web 页面中的恶意 Java 小程序、ActiveX 控件、JavaScript 脚本程序、VBScript 脚本程序，甚至 Office 文档文件的宏病毒都能够携带对网络和计算机系统有破坏作用的病毒。这些病毒在网络上进行传播和破坏的途径和手段变得多样化，也使得网络环境中的防病毒工作变得更加复杂。网络防病毒工具必须能够针对网络中各个可能的病毒入口来进行防护。

在互联网中任何计算机系统都可以被访问，从而致使全球范围内的黑客都可能对某个计算机系统入侵，窃取数据和非法修改系统。黑客主要手段之一是窃取合法用户的口令和密码，伪装合法用户进行非法操作；其次是利用网络操作系统的默认安全提供的权限来访问计算机系统，这些权限是由于系统管理员或用户疏忽所致或者他们根本都不知道，例如，在 Unix 系统的默认安装过程中，会自动安装大多数系统工具软件。据统计，其中大概有约 300 个工具是大多数合法用户所根本不会使用的，但这些工具往往会被黑客所利用。最后是黑客利用网络操作系统的漏洞，利用工具入侵计算机系统。由于用户操作的规范和管理水平的提高，致使黑客的主要入侵方式是寻找计算机系统中软件的漏洞进行非法访问和操作。要弥补这些漏洞，就需要使用专门的系统风险评估工具，来帮助系统管理员找出哪些工具软件是不应该安装的，哪些工具是应该缩小其用户使用权限的。在完成了这些工作之后，操作系统自身的安全性问题在一定程度上得到了保障。

3. 用户的安全性

对于计算机网络中用户类型很多，不同的类型具有不同的权限；用户的针对网络安全的认识和安全性敏感性不同，这些都可能影响到用户的安全性，必须采用足够的安全机制来保证合法用户对计算机系统中资源和数据的访问。

为了提高计算机系统访问权限的合理划分和权限的管理，多数网络是把系统的权限划分为用户组来进行管理，比如 Unix 和 Windows 网络操作系统都是采用这样的方式。针对不同的用户类别，可以合理地划分出该类别用户的权限，其安全性得到充分的考虑，也可以把该用户类别进一步按照安全类别划分，针对不同层次的安全性授权使用户只能访问与其安全级别相对应的系统数据资源。