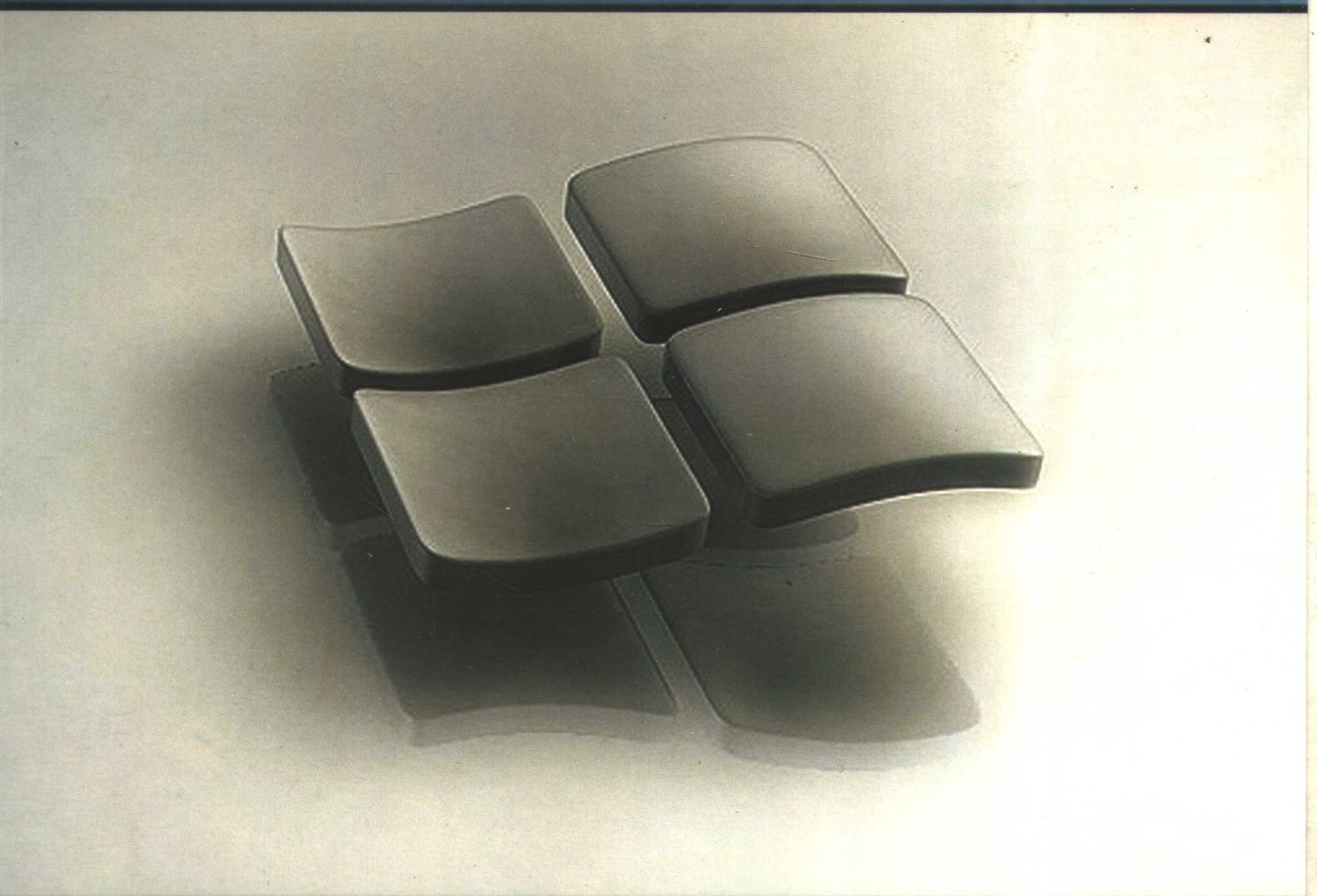
网络安全研究

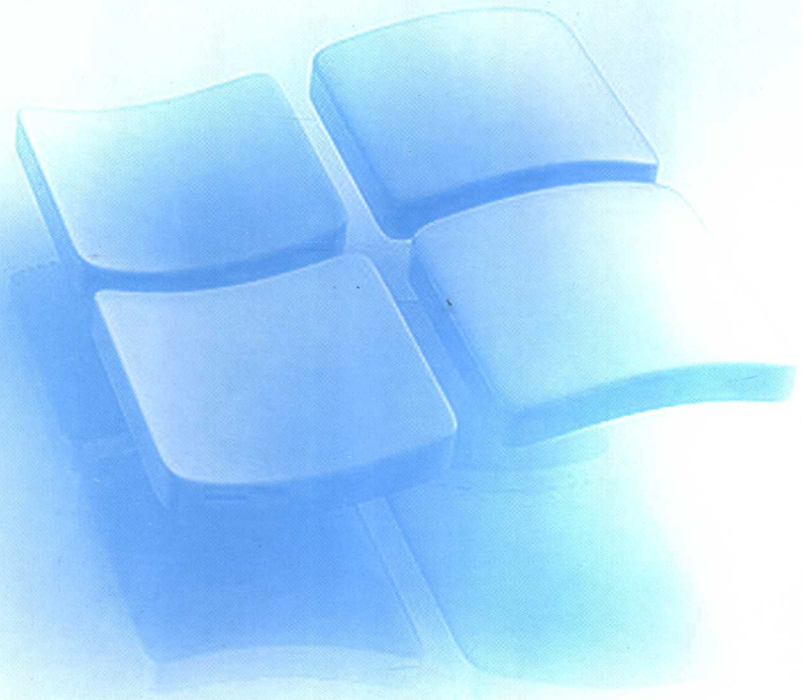
刘振峰　著



黄河出版社

网络安全研究

刘振峰　著



黄河出版社

责任编辑 吴四清　　**封面设计** 刘振峰
监　　制 林志军

图书在版编目(CIP)数据

网络安全研究／刘振峰著．—济南：黄河出版社，2007.9
ISBN 978-7-80152-877-3

Ⅰ．网…　Ⅱ．刘…　Ⅲ．计算机网络—安全技术—研究　Ⅳ．TP393.08

中国版本图书馆 CIP 数据核字（2007）第 139867 号

书名 网络安全研究
作者 刘振峰
出版 黄河出版社
发行 黄河出版社发行部
（济南市英雄山路 21 号　250002）
印刷 山东新华印刷厂
规格 787 毫米×1092 毫米　16 开本
10.125 印张　237 千字
印次 2007 年 9 月第 1 版
版次 2007 年 9 月第 1 次印刷
书号 ISBN 978-7-80152-877-3/Z·022
定价 25.00 元

前　言

计算机网络的发展，特别是 Internet 的发展和普及，为人类带来了新的工作、学习和生活方式，人们与计算机网络的联系也越来越密切。计算机网络已经成为 21 世纪知识经济社会的必要条件和基础设施。由于计算机网络系统的开放性以及现有网络协议和软件系统固有的安全缺陷，使网络系统不可避免地存在一定的安全隐患和安全风险。特别是 Internet 在使用和管理上的无政府状态，使人们在享受网络所带来的方便和效益的同时，也面临着网络安全方面的巨大挑战。各种计算机病毒和黑客攻击已经对网络安全构成严重的威胁，信息安全事件屡有发生，不仅造成了严重的经济损失，其侵犯的社会关系也非常复杂。因此，使计算机网络系统免受破坏，提高系统的安全可靠性，已成为人们关注和亟待解决的问题。每个网络机构的管理人员、网络系统用户和工程技术人员都应该掌握一定的计算机网络安全技术，以使自己的信息系统能够安全稳定地运行，并提供正常的安全服务。

人们已经清醒地认识到，在发展信息网络技术的同时，做好网络安全方面的理论研究与应用技术开发，是网络技术发展的重要内容。当然，解决网络系统的安全问题是一个系统工程，它不仅涉及技术问题，还涉及管理、法律和道德，因而也是一个社会问题。毋庸置疑，网络安全的研究和技术开发，是现在和未来相当长时期内关注的热点问题。但是，我国对信息安全的研究起步较晚，网络安全技术还有待整体提高和发展，面对日益严峻的网络安全问题，我们应该如何去认识、分析和防范，是当前面临的一个迫切问题。

本书以网络安全通常采取的防护、检测、响应和恢复措施为研究主线，系统地探讨了网络安全知识和技术，重点研究了网络系统的安全运行和网络信息安全保护方面的问题，提出了提高网络安全、加强网络防范的措施。

全书共分 8 章，内容包括：网络安全概述；网络操作系统安全；数据库安全；Internet 安全；防火墙技术；数据加密与鉴别；计算机病毒及其防治；网络实体安全。

由于作者水平有限，书中难免有疏漏和不妥之处，敬请读者批评指正。

作　者

2007 年 6 月

目 录

第 1 章　网络安全概述

21 世纪的今天，科学技术，尤其是信息技术的迅猛发展，使得计算机这一人类伟大的发明已经广泛地深入到社会的各个角落，人们利用计算机存储数据、处理图像、畅游网络、互发 E-MAIL 等，充分地享用计算机带来的无可比拟的功能和智慧，特别是计算机信息网络已经成为社会发展进步的重要保证，它的应用遍及国家的政府、军事、科技、文教等各个领域。其中存储、传输和加工处理的信息，有许多涉及政府宏观调控决策、商业经济信息、银行资金转账、股票证券、能源资源数据、科研数据等重要内容。

与此同时，无情的事实表明，除非我们把计算机锁在一个密闭的房间里，并且没有任何计算机与之相连使其对外界的访问受到隔离，否则该计算机系统就会时刻处于危险之中，随时都可能面临黑客的攻击、少数网民的恶作剧、个别居心叵测分子的作祟、系统硬件及软件不时出现的故障等非法侵入和安全侵犯。同时，计算机网络实体还要经受诸如水灾、火灾、地震、电磁辐射等自然灾害的考验。

近年来，计算机犯罪案件急剧上升，各国的计算机系统特别是网络系统面临着很大的威胁，并成为严重的社会问题之一。据美国联邦调查局的报告，计算机犯罪是商业犯罪中最大的犯罪类型之一，每笔犯罪的平均金额为 45000 美元，每年计算机犯罪造成的经济损失高达 100 亿美元。加之国际互联网络的广域性、开放性和可扩展性，计算机犯罪也已成为具有普遍性的国际问题。由此可见，计算机的安全问题，尤其是计算机网络的安全问题，已经到了不可小视，必须深入探讨研究的非同小可的时候了。

1.1　网络安全的概念

1.1.1　计算机网络安全的定义

当你遨游在 Internet 浩瀚无际的信息海洋，你就会发现计算机只有同网络相连，才是名副其实的计算机，从一定意义上讲，“网络就是计算机”，“计算机就是网络”，二者密不可分。随着计算机网络的飞速发展，这一关于计算机的现代理念已经愈来愈得到人们的认可。因此，要给计算机网络安全下定义，首先要了解“计算机安全”的概念。

国际标准化组织（ISO）将“计算机安全”定义为：“为数据处理系统建立和采取的技术和管理的安全保护，保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露”，此定义偏重于静态信息的保护。

也曾有人将“计算机安全”定义为：“计算机的硬件、软件和数据受到保护，不因

偶然和恶意的原因而遭到破坏、更改和泄露，系统连续正常运行。”该定义着重于动态意义描述。

综合上述计算机安全的定义以及计算机和网络的密切关系。我们可以给“计算机网络安全”作如下定义：“保护计算机网络系统中的硬件、软件及其数据不受偶然或者恶意原因而遭到破坏、更改、泄露，保障系统连续可靠地正常运行，网络服务不中断。”

1.1.2 计算机网络安全的内涵

网络安全的根本目的就是防止通过计算机网络传输的信息被非法使用。如果国家信息网络上的数据遭到窃取、更改或破坏，那么它必将关系到国家的主权和声誉、社会的繁荣和稳定、民族文化的继承和发扬等一系列重要问题。为避免机要信息的泄露对社会产生的危害和对国家造成的极大损失，任何网络中国家机密信息的过滤、防堵和保护将是网络运行管理中极其重要的内容。有时网络信息安全的不利影响甚至超过信息共享所带来的巨大效益。从企业和个人的用户角度来看，涉及个人隐私或商业利益的信息在网络上传输时，其保密性、完整性和真实性也应受到应有的关注，避免他人或商业对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，造成用户资料的非授权访问和破坏。

网络安全的具体含义涉及社会生活的方方面面，从使用防火墙、防病毒、信息加密、身份确认与授权等技术，到企业的规章制度、网络安全教育和国家的法律政策，直至采用必要的实时监控手段、应用检查安全漏洞的仿真系统和制定灵活有效的安全策略应变措施，加强网络安全的审计与管理等。

在涉及“安全”词汇时，通常会与网络、计算机、信息和数据相联系，而且具有不同的侧重和含义。网络安全较全面地对计算机和计算机之间相连接的传输线路这个全过程进行管理，特别是对网络的组成方式、拓扑结构和网络应用的重点研究。它包括了各种类型的局域网、通信与计算机相结合的广域网，以及更为广泛的计算机互联网络。因此，保护网络系统中的硬件、软件及其数据不受偶然或者恶意原因而遭到破坏、更改、泄露，系统连续可靠地正常运行，网络服务不中断，成为网络安全的主要内容。例如，电子邮件系统不能因为安全原因使用户的数据丢失，等等。

安全问题是一个动态的过程，不能用静止的观点去看待，不仅仅是计算机硬件存在形式上的安全，还存在着计算机软件特殊形式的安全问题，因为有运行故障的软件同非法存取数据一样对计算机的安全性构成威胁。人为的有意或无意的操作、某种计算机病毒的发作、不可预知的系统故障和运行错误，都可能造成计算机中数据的丢失。

因此，计算机安全的内容应包括两方面，即物理安全和逻辑安全。物理安全指系统设备及相关设施受到物理保护，免于破坏、丢失等。逻辑安全包括信息的完整性、保密性和可用性。完整性指信息不会被非授权修改及信息保持一致性等；保密性指仅在授权情况下高级别信息可以流向低级别的客体与主体；可用性指合法用户的正常请求能及时、正确、安全地得到服务或回应。

1.2 网络面临的不安全因素

对计算机网络的威胁可以来自方方面面，从其表现形式上看，自然灾害、意外事故、硬件故障、软件漏洞、人为失误、计算机犯罪、“黑客”攻击、内部泄露、外部泄密、信息丢失、电子谍报、信息战、网络协议中的缺陷等人为和非人为的情况，都是对计算机网络安全的重要威胁。

但我们透过现象看本质，认真地回顾反思，造成上述威胁的原因到底何在？为什么计算机网络如此容易受到侵害？这一问题绝不能简单地从表面上去看，必须对其深层次的原因有所了解，才能提高我们的防患意识。

从技术角度看，计算机网络的不安全因素，主要存在于两个方面：一方面，因为它的所有资源可以为所有用户共享，不可避免的漏洞给不法分子以可乘之机；另一方面，是因为它的技术是开放和标准的，研制者开始并没有刻意去提高它的安全性能。因此，计算机技术，包括网络技术，虽然已经从过去的研究阶段进入了商品实用阶段，但是它的技术基础却是不安全的，有其脆弱的一面，这是我们不可否认的客观事实。

1.2.1 计算机技术存在的隐患

计算机网络安全的根本威胁是计算机基本技术自身存在的种种隐患而导致的结果。从它多年的发展历史看，网络信息安全问题在相当一个时段内并未摆到十分重要的议事日程。计算机基本技术最主要的设计目标就是加快运算速度，即以运算为核心进行大量数据的计算。尤其是在多用户计算机系统设计中，安全设计的目的是多用户分时管理和系统管理员进行系统维护等，形成了中心计算机和服务器是以系统管理员即超级用户为核心的管理体制，从而造就了一个权力过大的系统管理员，他有权处理和阅读所有的资料和资源，其特权远远超过他的顶头上司，形成了行政隶属与计算机管理体系中权力倒置的严重危险局面。

个人计算机（PC）的发展设计目标是进行个人事务处理。和多用户系统一样，在个人计算机的设计中同样也没有考虑任何信息安全性的要求，这样的安全设计标准在没有出现网络、单机盛行的时代是可以接受认可的。虽然后来 PC 机的 CPU 不断升级，硬件不断升档，但出于兼容性的设计考虑，个人计算机系统的安全性一直没有能够完善起来，并且由于其开放性的设计模式，使得几乎每个使用者都可以了解其内部结构和工作原理，极易发现系统存在的可攻击的漏洞，根本就没有安全性可言。如今已进入网络时代，昔日的个人计算机在网络中充当了重要角色，在频繁的信息传输通信过程中，自身的安全漏洞不断暴露，使得计算机网络的安全问题日益严峻。

对计算机软件技术而言，由于现在软件设计本身的水平所限，软件设计人员不可能考虑到影响网络安全因素的每一个细节，以致出现了包括世界上最有名的微软公司等一些重要的软件公司，频频发布系统安全隐患的软件补丁，以解决软件漏洞弥补之急的现象。

从网络协议结构设计看，如今使用最广泛的网络协议是 TCP/IP 协议，它是在资源

管理及网络技术均不成熟的情况下设计的。它的主要设计目标是互联、互通、共享，而不是安全。实践证明，该协议中已被发现有许多安全漏洞和隐患。

1.2.2 网络资源共享导致的威胁

资源共享是计算机网络的重要特点，对无数的计算机用户无疑是天大的好事，否则，网络也不会受到人们的如此青睐。但也正是因为“共享”，却被一些别有用心者钻了空子，使得网络信息及网络设备的安全受到了种种不同程度的威胁。

人为的无意失误：是指操作人员使用不当、系统安全配置不规范、用户安全意识不强，选择用户口令不慎，将自己的账号随意转告他人或与别人共享等等情况，都会对网络安全构成威胁。

人为的恶意攻击：此类攻击可以分为两类，一类是主动攻击，它的目的在于篡改系统中所含的信息，或者改变系统的状态和操作，它以各种方式有选择地破坏信息的有效性、完整性和真实性；另一类是被动攻击，它在不影响网络正常工作的情况下，进行信息的截获和窃取，对信息流量进行分析，并通过信息的破译以获得重要的机密信息。它不会导致系统中信息的任何改动，而且系统的操作和状态也不被改变，因此，被动攻击主要威胁信息的保密性。这两种攻击均可对网络安全造成极大的危害，并导致机密数据的泄漏。

网络软件的漏洞：网络软件不可能百分之百地没有缺陷和漏洞，例如，TCP/IP 网络协议的安全问题。然而，这些漏洞和缺陷恰恰是黑客对系统进行攻击的首选目标，导致黑客频频侵入网络内部的主要原因就是相应系统和应用软件本身的脆弱性和安全措施不完备。另外，许多软件中的“后门”往往都是软件编程人员为了自己方便而设置的，一般不为外人知晓，可是一旦“后门”被侵入，将使黑客对网络系统资源的非法攻击成为可能。

虽然人为因素和非人为因素都可以对网络安全构成威胁，但是相对于自然灾害及无意侵害对计算机网络系统造成的危害，精心设计的人为攻击威胁最大。这是因为人的因素最为复杂，人的思想最为活跃，不可能完全用静止的方法和法律法规加以防护。这是网络安全目前所面临的最大威胁，黑客的攻击和计算机犯罪就属于这一类。其采取的方法主要表现为以下几种：

●非授权访问：预先没有经过同意就使用网络或计算机资源被视作非授权访问。如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；擅自扩大权限，越权访问信息；通过欺骗系统（或用户）变非法伪装为合法，或者小特权冒充成为大特权，从而侵入系统，对网络进行非法访问。

●信息泄漏或丢失：指敏感数据在有意或无意中被泄漏出去或丢失。它通常包括信息在传输过程中丢失或泄漏，在存储介质中丢失或泄漏两种情况。黑客们常利用各种可能的合法或非法的手段窃取系统中的信息资源和敏感数据。例如，对通信线路中传输的信号进行搭线监听，或者利用通信设备在工作过程中产生的电磁泄漏截获有用的机密信息等。他们还采用分析手段，通过对系统进行长期监视，利用统计分析方法对诸如通信频度、通信的信息流向、通信总量的变化等参数进行研究，以求发现有价

值的信息和规律，如用户口令、账号等重要信息，并通过建立隐蔽隧道等方法窃取敏感信息。

●破坏数据完整性：以非法手段窃得对数据的使用权，删除、修改、插入或重发某些重要信息，以取得有益于攻击者的响应；恶意添加、修改数据，以干扰用户的正常使用。其篡改手法是通过改变信息的标签、内容和属性，或者将其他信息插入其中，甚至删除部分内容等手段，从而用假信息代替原始信息，使对方误认为修改后的信息为合法信息；还有一种来自合法用户的攻击，即抵赖，比如否认自己曾经发布过某条消息、伪造过一份对方来信、修改过来信等。

●其他情况：比如破坏通信规程和协议、拒绝合法服务请求、设置陷阱等。所谓拒绝服务攻击，就是不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序使系统响应减慢甚至瘫痪，影响正常用户的使用，甚至使合法用户被排斥而不能进入计算机网络系统或不能得到相应的服务。此外，还有人通过网络传播计算机病毒，其破坏性大大高于单机系统，而且用户很难防范。

要保证网络中的信息安全，就必须想办法尽可能抵御以上的种种威胁. 学会识别这些破坏手段，以便采取技术策略和法律制约两方面的努力，确保信息系统的安全。需要特别指出的是，无论采取何种防范措施都不可能绝对保证信息系统的安全。安全是相对的，不安全才是绝对的。社会的发展如此，计算机网络安全技术的发展同样如此。

1.3 网络安全级别

从 1981 年起，美国国防部计算机安全中心就开始全面研究计算机系统所处理的机密信息的保护要求和控制手段。1985 年开发出计算机安全标准——《可信任计算机标准评估准则》（Trusted Computer Standards Evaluation Criteria），即橙皮书，其中的一些计算机安全级别被用来评价一个计算机系统的安全性。自从 1985 年它成为美国国防部的标准以来，就一直没有改变过，多年来一直是评估多用户主机和小型操作系统的主要方法。其他子系统（如数据库和网络等）也一直是用橙皮书来解释评价的。

计算机系统就其安全性的程度，分为若干安全级别，依照安全等级由低到高的顺序是：D 级安全、C 级安全、B 级安全、A 级安全。

1.3.1 D 级安全

D 级是最低的安全级别，拥有这个级别的操作系统就像一个门户大开的房子，任何人都可以自由进出，是完全不可信的，是可用的最低安全形式。其硬件缺乏保护，操作系统容易受到损害，用户和存储器在计算机上的信息，少有身份验证控制访问权限。属于这个级别的操作系统有：MS - DOS、Windows 和 Macintosh System 7. x 等操作系统，它们不区分用户，无法确定谁在敲击键盘，对硬盘上的信息可以几乎不受限制地访问。然而，评价的作用并不意味着此类操作系统不向用户提供任何安全功能，而仅仅表示那种操作系统不具备更高级别的安全功能。它们提供简单的用户识别、验证、

审核，也有一些访问控制和加密等功能，只是不如 C 级的操作系统。

1.3.2 C 级安全

C 级有两个安全子级别，即 C1 级和 C2 级。

1. C1 级安全

C1 级，又称自由选择性安全保护（Discretionary Security Protection）级别，它包含两个安全等级，它描述了一种典型的用在 UNIX 系统上的安全级别。这种级别的系统对硬件提供了某种程度的保护；用户拥有注册账号和口令，系统通过账号和口令来识别用户是否合法，并决定用户对程序和数据有什么的访问权，但其硬件受到损害的可能性仍然存在。

用户拥有的访问权是指对文件的访问权。文件的拥有者和超级用户（root）可以改动文件中的访问属性，从而对不同的用户给予不同的访问权，例如，让文件拥有者具有读写和执行的权力，而给其他用户以部分权力。

另外，许多日常的管理工作由超级用户来完成，他有很大的权力，所以他的口令一定要保存好，不能共享。

C1 级安全保护的不足之处在于用户能直接访问操作系统的超级用户。C1 级不能控制进入系统的用户的访问级别，所以用户可以将系统中的数据任意移走，他们可以控制系统配置，获取比系统管理员允许的更高权限，如改变和控制用户名。

2. C2 级安全

C2 级以 C1 级标准为基础，除了具有 C1 包含的特性外，C2 级别系统还具有访问控制环境（Controlled - Access Environment）的权力。该环境具有进一步限制用户执行某些命令或访问某些文件的权限，而且还加入了身份认证级别。另外，系统对发生的事件加以审计（audit），并写入日志当中，如什么时候开机，哪个用户在什么时候从哪儿登录等等，这样通过查看日志，就可以发现入侵的痕迹，如多次登录失败，也可以大致推测出可能有人想强行闯入系统。审计除了可以记录下系统管理员执行的活动以外，还加入了身份认证级别，这样就可以知道谁在执行这些命令。审计的缺点在于它需要额外的处理器时间和磁盘空间。

使用附加身份验证，就可以让一个 C2 级系统的用户能够在不是超级用户的情况下，有权执行系统管理任务。这样，一个单独的用户而不是系统管理员在执行了工作后，使得追踪与系统管理有关的任务变得更加精细和准确。

能够达到 C2 级的常见操作系统有：UNIX、XENIX、Novell 3.0、Windows NT 等。

1.3.3 B 级安全

B 级也叫强制性安全保护，包括三个子级别，即 B1、B2 和 B3。

1. B1 级安全

B1 级即标志安全保护（Labeled Security Protection），是支持多级安全（如秘密和绝密）的第一个级别，这个级别说明一个处于强制性访问控制之下的对象（如磁盘或文件服务器目录），系统不允许文件的使用者修改其许可权限。这种用户标识和加密标

志的双重保护，加强了系统信息的安全性。

B1 级的计算机安全措施，视操作系统而定。政府机关和安全承包商们是 B1 级计算机系统的主要拥有者。

2. B2 级安全

B2 级安全叫做结构保护（Structured Protection），它要求计算机系统中所有的对象都要加上标签，而且给设备（磁盘、磁带及终端）分配单个或多个安全级别。它是提供较高安全级别的对象与另一个较低安全级别的对象相互通信的第一个级别。

3. B3 级安全

B3 级安全称作安全域级别（Security Domain），使用安装硬件的办法来加强域，例如，内存管理硬件用于保护安全域免遭无授权访问或其他安全域对象的修改。该级别也要求用户的终端通过一条可信任途径连到该系统上。

1.3.4 A 级安全

A 级安全亦称验证设计（Verify Design），是当前橙皮书中规定的最高安全级别，它包含了一个严格的设计、控制和验证过程。与前面提到的各个级别一样，该级别包含了较低级别的所有特性。其设计必须是从数学上经过验证的，而且必须进行对秘密通道和可信任分布的分析。可信任分布（Trusted Distribution）的含义是，硬件和软件在传输过程中要受到保护，以防止破坏整个安全系统，即所有部件来源必须有安全保证，在销售和运输过程中受到严密跟踪。

在上述几种标准的基础上，美国、加拿大和欧洲联合研制信息技术安全评测公共标准（CC），并于 1996 年颁布了 1.0 版；1993 年加拿大颁布可信计算机产品评测标准（CTCPEC）；1993 年，美国国防部国防信息系统局又提出在 C4I 系统（Command, Control, Communication, Computer, and Intelligence system）上采用多级安全（MLS）技术与概念。

1.4 网络安全措施

不同环境和应用方式的网络安全各有不同的含义和侧重，相应的安全措施也各不相同。例如，运行系统的安全，主要是保证信息处理和传输系统的安全，侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免因电磁漏而产生信息泄露，干扰他人或受他人干扰；系统信息的安全，包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治和数据加密等措施；信息传播的安全，是信息传播后果的安全，通过信息过滤等措施，侧重于防止和控制非法、有害的信息进行传播后的后果，避免公用网络上大量自由传输的信息失控；信息内容的安全，侧重于保护信息量的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为，本质上是保护用户的利益和隐私。

实际上，网络安全措施以及相应的控制技术种类繁多而且还相互交叉。虽然没有

完整统一的理论基础，但是在不同的场合下，为了不同的目的，这些技术确实能够发挥出色的功效。目前普遍采用的措施有：利用操作系统、数据库、电子邮件、应用系统本身的安全性，对用户进行权限控制；在局域网的桌面工作站上部署防病毒软件；在 Intranet 系统与 Internet 连接之处部署防火墙；某些行业的关键业务在广域网上采用加密传输，而其他业务采用明文传输等等。下面简要介绍一些常用的网络安全措施：

●防火墙：防火墙并非万能，但对于网络安全来说是必不可少的。它是位于两个网络之间的屏障，一个是可以信赖的内部网络，另一个是不可以信赖的外部网络，防火墙按照系统管理员预先定义好的安全策略和规则控制两个网络之间数据包的进出。大部分防火墙都采用了以下三种工作方式中的一种或多种：使用一个过滤器来检查数据包的来源和目的地址，按照规定接收或拒绝数据包；扫描数据包，查找与应用相关的数据；在网络层对数据包进行模式检查，看是否符合已知“友好”数据包的位（bit）模式。

●身份认证：防火墙是系统的第一道防线，用以防止非法数据的进入。而身份认证的作用则是阻止非法用户的不良访问。有多种方法可以鉴别一个用户的合法性，密码是最常用的，但由于有许多用户采用了很容易被猜到的单词或短语作为密码，使得该方法经常失效。其他方法包括对人体生理特征（如指纹、眼睛视网膜底纹等）的识别等。

●数据加密：加密是通过对信息的重新组合，使得只有收发双方才能解码还原信息的传统方法。一般的加密系统是以密钥为基础的，这是一种对称加密，即用户使用同一个密钥加密和解码。目前，随着技术的进步，加密正逐步被集成到系统和网络中，如正在发展的下一代网际协议 IPV6。在硬件方面，Intel 公司也在研制用于 PC 机和服务器主板的加密处理器。通过密码技术对各类数据进行加密处理，能够有效防止信息泄露。典型的加密算法有数据加密标准 DES 和公开密钥密码体制 PKC。

●数字签名：这种技术主要用于防止非法伪造、假冒和篡改信息。接收者能够核实发送者，以防假冒；发信者无法抵赖自己所发的信息；除合法发信者外，其他人无法伪造信息；发生争执时可由第三方做出仲裁。目前，大多数电子商务交易采用两个密钥加密：密文和用来解码的密钥一起发送，而该密钥本身又被加密，还需要另一个密钥来解码。这种组合加密被称为数字签名，它有可能成为未来电子商务中首选的安全技术。美国政府有一个自己的加密标准，DSS（Digital Signature Standard），使用了 Secure Hash 运算法则。用该法则对信息处理可得到一个 160 位（bit）的数字，把这个数字与信息的密钥以某种方式组合起来，从而得到数字签名。

●安全监控：即使有防火墙、身份认证和加密，人们仍然担心会遭到病毒的攻击。这些病毒通过 E-mail 或用户下载的 Java 和 ActiveX 小程序（Applet）进行传播。带病毒的 Applet 激活后，又可能会自动下载别的 Applet。现有的反病毒软件可以清除 E-mail 病毒，对付新型的 Java 和 ActiveX 病毒也有一些办法，如完善防火墙，使之能够监控 Applet 的运行，或者给 Applet 加上标签，让用户知道它们的来源。

高效的网络安全性关键因素之一就是安全监控。监控网络安全性的方法就是检查网络中的各个系统的文件和登录，要想检查系统中的不正常活动，就必须知道什么是

正常的活动？哪些进程是正常的运行？谁是正常登录？为了对系统各种正常活动行为有感觉，就要知道这一切。“知己知彼，百战不殆”。如一些常用的 UNIX 命令：ps、who、netstat、af、diff、find、last 等都可以帮助系统管理员了解系统运行是否处于正常状况。

要指出的是，不要认为实现了以上的安全措施，系统就非常安全了。事实上，这样的系统远没有达到必要的安全性，系统还非常脆弱。如系统很容易遭到黑客和病毒的入侵，造成系统的崩溃；数据在局域网或广域网上传输时，可能被截取、偷换、冒名顶替；远程访问系统经常被未授权的用户入侵。这就需要通过利用审计技术、访问控制技术和安全协议等多种技术手段进行综合管理。