网络安全监察与犯罪侦查

WANGLUO ANQUAN JIANCHA YU FANZUI ZHENCHA

杨成卫 编著

中国人民公安大学出版社

网络安全监察与犯罪侦查

杨成卫　编著

（[redacted]）
中国人民公安大学出版社
·北　京·

图书在版编目（CIP）数据

网络安全监察与犯罪侦查/杨成卫编著. —北京：中国人民公安大学出版社，2006.6
ISBN 7-81109-432-0

Ⅰ. 网… Ⅱ. ①杨… Ⅲ. ①计算机网络—安全技术—高等学校—教材②计算机犯罪—犯罪侦察—高等学校—教材 Ⅳ. ①TP393.08②D914

中国版本图书馆 CIP 数据核字（2006）第 073754 号

网络安全监察与犯罪侦查

WANGLUOANQUANJIANCHAYUFANZUIZHENCHA

杨成卫 编著

出版发行：中国人民公安大学出版社
地　　址：北京市西城区木樨地南里
邮政编码：100038
印　　刷：北京市泰锐印刷厂

版　　次：2006 年 6 月第 1 版
印　　次：2006 年 6 月第 1 次
印　　张：16
开　　本：787 毫米×1092 毫米　1/16
字　　数：400 千字

ISBN 7-81109-432-0/D·412
定　　价：28.00 元　（[redacted]）

本社图书出现印装质量问题，由发行部负责调换
联系电话：(010) 83903254

E-mail：cpep@public.bta.net.cn
www.phcppsu.com.cn　　www.jgclub.com.cn

前　言

计算机网络技术的迅猛发展和应用普及，给人们的生产、生活和思维方式带来了巨大的变化，极大地推动了人类社会的发展和人类文明的进步，把人类社会带入了信息时代。

人们通过计算机网络可以非常方便地存储、交换以及搜索信息，在工作、生活以及娱乐中都享受到了极大便利，甚至改变了生活、学习、工作方式。

人们在享受计算机网络所带来的巨大利益的同时，也受到了计算机网络所暴露出的各种安全问题的困扰。并且随着计算机网络技术进一步应用普及和发展，计算机网络安全越发突显，计算机网络犯罪已成为一种新型犯罪，越来越多的社会犯罪与计算机有关。

目前，市场上有大量关于计算机网络安全的书籍，也有一定数量的计算机犯罪侦查书籍。但是，适合培养实用型人才的书不多。为适应当前计算机网络安全和犯罪侦查的教学需要，有必要撰写一本理论和实际相结合，注重实用的书。本人结合多年教学实践和探索心得，参考了许多著作和论文编撰成书，奉献给读者。

本书的编写原则是，理论简明扼要，重在实用，强调解决实际问题，着重培养动手能力。

本书内容涵盖计算机网络安全、监察和犯罪侦查诸方面，内容丰富、实用，既有理论阐述，又有相应工具软件使用介绍，还有法律法规内容介绍。语言流畅，层次分明，逻辑性强，特别适合公安机关作为培训教材。

本书在编撰过程中得到了铁道警官高等专科学校的有关领导和同事的大力支持。书中采用许多专家和学者的研究成果，也参考了许多论著和论文在此一并致谢。由于作者水平有限，书中难免有不妥之处，敬请读者批评指正。

编著者

目 录

第6章 数据库系统安全技术

第7章 计算机网络监察与管理

第8章 计算机网络犯罪侦查

第1章 计算机网络安全概论

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、遨游网际、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治、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时候了。

1.1 计算机网络安全概述

1.1.1 计算机网络安全定义

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、更改和泄漏”。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的描述。

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。物理安全是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。完整性是指信息不会被非授权修改及信息保持一致性等；保密性是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；可用性是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 计算机网络安全的主要威胁

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等情况，都是对计算机网络安全的重要威胁。

但我们必须透过现象看本质，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 计算机的技术方面安全隐患

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，但对于信息流量进行分析，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 计算机网络安全的基本需求和管理

1.3.1 计算机网络安全的基本需求

计算机系统要防止资源和数据被独占，防止数据和程序被非法修改、删除及泄露，从一定意义上讲，提高系统的封闭性有利于保证信息的安全。但过度封闭的系统又不利于技术的发展和用户的使用。因此，如何在保持网络开放灵活性的同时保证系统的安全性，已经成为国际计算机界研究的热点。目前看来，使用 TCP/IP 技术构建的网络上的安全措施及其相应的网络安全产品主要有两大类：开放型（如数据加密）及被动防卫型（如防火墙）。他们主要是根据以下四个方面的安全需求而设计和应用的：

1. 数据的保密性

数据的保密性是指数据不泄露给非授权用户、实体或过程，或供其利用的特性。由于系统无法确认是否有未经授权的用户截取网络上的数据，这就需要使用一种手段对数据进行加密处理。数据加密就是用来实现这一目标的，使得加密后的数据能够保证在传输、使用和转换过程中不被第三方非法获取。数据经过加密变换后，将明文转换成密文，只有经过授权的合法用户，使用自己的密钥，通过解密算法才能将密文还原成明文。反之，未经授权的用户因不掌握加密或解密密钥，无法获得原文的信息，限制其对特定数据的访问。数据保密可以说是许多安全措施的基本保证，它分为网络传输保密和数据存储保密。除了使用各种加密技术外，对于数据的存储保密性也可以使用访问控制的办法来实现。网络和系统管理员根据不同的应用需求和等级职责，把数据进行分类，配置不同的访问模式，控制数据的非法流向。

2. 数据的完整性

数据的完整性是指数据未经授权不能进行改变的特性，即只有得到允许的人才能修改数据，并且能够判别出数据是否已被非法篡改。在存储器中或是经过网络传输后的数据，必须和它被输入时或最后一次被修改，或者传输前的内容与形式完全一样。其目的就是保证信息系统上的数据处于一种完整和未受损的状态，数据不会因为其存储和传输的过程，而被有意或无意的事件所改变、破坏和丢失。系统需要一种方法来确认数据在此过程中没有被改变。这种改变可能来源于自然灾难、人的有意和无意行为、因质量和其他因素导致的设备故障、环境和通信的影响以及不可预知的软件错误等方面。显然，要想保证数据的完整性使用一种方法是不够的，在应用数据加密技术的基础上，还应综合运用故障应急方案和多种预防性技术，诸如归档、备份、镜像、检验、崩溃转储和故障前兆分析等手段来实现网络安全的目标。

3. 数据的可用性

数据的可用性是指可被授权实体访问并按需求使用的特性，即攻击者不能占用所有的资源而阻碍授权者的工作。由于互联网络是开放性网络，需要时就可以得到所需要的数据，是网络设计和发展的基本目标，因此数据的可用性要求系统当用户需要时能够存取所需要的数据，或是说能够得到系统提供的服务，能够免于遭受恶劣影响，甚至被完全破坏而不可使用的情形。如果一个合法用户需要得到系统或网络服务时，系统和网络不能提供正常的服务，那么和文件资料被锁在保险柜里，开关和密码系统因混乱而不能取出一样，虽然数据完好无损地存在于系统之中，却眼看着拿不出来。例如，网络环境下拒绝服务、破坏网络和系统的正常运行等都属于对数据可用性的攻击。

4. 数据的可控性

数据的可控性是指可以控制授权范围内的信息流向及行为方式，如对数据的访问、传播及内容具有控制能力。首先，系统需要能够控制谁能够访问系统或网络上的数据，以及如何访问，即是否可以修改数据还是只能读取数据。这首先要通过采用访问控制表等授权方法得以实现；其次，即使拥有合法的授权，系统仍需要对网络上的用户进行验证，以确保他确实是他所声称的那个人，通过握手协议和数据加密进行身份验证；最后，系统还要将用户的所有网络活动记录在案，包括网络中机器的使用时间、敏感操作和违纪操作等，为系统进行事故原因查询、定位、事故发生前的预测、报警以及为事故发生后的实时处理提供详细可靠的依据或支持。容计对用户的正常操作也有记载，可以实现统计、计费等功能，而且往往有些诸如修改数据的“正常”操作恰恰是攻击系统的非法操作，同样需要加以警惕。

5. 其他需求

不可抵赖和不可否认，是指用户不能抵赖自己曾做出的行为，也不能否认曾经接到对方的信息，这在网络交易系统中十分重要。另外，保护网络硬件资源不被非法占有，软件资源免受病毒的侵害，都构成了整个信息网络上的安全需求。

网络安全工作的目的就是在安全法律、法规、政策的支持与指导下，通过采用适当的安全技术与安全管理措施，提供安全系数所要求的保证，具体一点讲，就是指使用访问控制机制，阻止非授权用户进入网络，即“进不来”，从而保证网络系统的可用性；使用授权机制，实现对用户的权限控制，即不该拿走的“拿不走”，同时结合内容审计机制，实

现对网络资源及信息的可控性；使用加密机制，确保信息不暴露给未授权的实体或进程，即“看不懂”，从而实现信息的保密性；使用数据完整性鉴别机制，保证只有得到允许的人才能修改数据，而其他人“改不了”，从而确保信息的完整性；使用审计、监控、防抵赖等安全机制，使攻击者、破坏者、抵赖者“逃不掉”，并进一步对网络出现的安全问题提供调查的依据和手段，实现信息安全的可审查性。

1.3.2 计算机网络安全的管理策略

安全管理策略是指在一个特定的环境里，为保证提供一定级别的安全保护所必须遵守的规则。该安全管理策略模型包括了建立安全环境的三个重要组成部分，即：

·威严的法律：安全的基石是社会法律、法规与手段，通过建立一套安全管理的标准和方法，即通过建立与网络信息安全相关的法律、法规，使非法分子慑于法律，不敢轻举妄动。

·先进的技术：先进的安全技术是网络信息安全的根本保障，用户对自身面临的威胁进行风险评估，决定其需要的安全服务种类，选择相应的安全机制，然后集成先进的安全技术。

·严格的管理：各网络使用机构、企业和单位应建立相应的、严格的信息安全管理办法，加强内部管理，建立审计和跟踪体系，提高整体的信息安全意识。

计算机信息网络是基础设施，如果基础设施没有安全保证是不可思议的。在互联网上几乎所有的技术都是开放的，但是唯有安全技术不能开放，这是互联网技术发展的一个核心矛盾。系统既要开放、标准，但同时又要解决安全的问题，所以从技术角度讲，安全问题是整个互联网技术里最困难的方面，也是建立网络安全管理策略的根本出发点。

安全是一个相对概念。相对于不同网络的具体需求不同，有些网络信息系统中使用信息的目的不需要保密，再加上安全和保密技术在实际应用中还存在这样那样不同程度的缺陷，需要不断地发展和完善。因此，每个内部网要根据具体情况制定自己的安全管理策略，防止出现盲目赶时髦，追求大而全，将安全管理策略的制定建立在感觉基础上，而不是在理论的指导下，建立在实事求是的基础上。网络安全是一个综合性课题，涉及立法、技术、管理、使用等许多方面，包括信息系统本身的安全问题以及数据信息量的安全问题。使用一种物理或逻辑的技术措施，只能解决一方面的问题。固守一种或宽或严的安全观念，无法有效地发挥网络的真正效益。安全策略的制定实际上是一种综合度的权衡，也是安全策略研究的重要内容之一。

网络安全管理策略是指在一个网络中关于安全问题而采取的原则，对安全使用的要求，以及如何保护网络的安全运行。制定网络安全管理策略首先要确定网络安全管理要保护什么，其具体的描述原则是“没有明确表述为允许的都被认为是被禁止的”，对于网络安全策略，一般都采用上述原则来加强对网络安全的限制。

网络安全策略在确定了描述原则后所要做的是确定网络资源的职责划分。网络安全策略要根据网络资源的职责确定哪些人允许使用某一设备，对每一台网络设备要确定哪些人能够修改它的配置；更进一步要明确的是授权给某人使用某网络设备和某资源的目的是什么，他可以在什么范围内使用；并确定对每一设备或资源，谁拥有它的管理权，即他可以为其他人授权，使之能够正常使用该设备或资源，并制定授权程序。

在网络安全策略里关于用户的权利与责任中，需要指明用户必须明确了解其所用的计

算机网络的使用规则。其中包括是否允许用户将账号转借给他人，用户应当将自己的口令保密到什么程度；用户应在多长时间内更改其口令，对其选择有什么限制；希望是用户自身提供备份还是由网络服务提供者提供。在关于用户的权利与责任中还会涉及电子邮件的保密性和有关讨论组的限制。在电子邮件组织（Electronic Mail Association）发表的白皮书中指出，Internet 中每个计算机网络都要有策略来保护用户的隐私。事实上，网络安全策略中所能达到的只能是用户希望达到的绝对隐私与网络管理人员为诊断、处理问题而收集用户信息的一个折中。安全策略中必须确定在什么情况下网络管理员可以读用户的文件，在什么情况下网络管理员有权检查网络上传送的信息；另外，网络安全策略还应说明网络使用的类型限制。定义可接受的网络应用或不可接受的网络应用，要考虑对不同级别的人员给予不同级别的限制。但一般的网络安全策略都会声明每个用户都要对其在网络上的言行负责。所有违反安全策略、破坏系统安全的行为都是被禁止的。

网络安全策略中，在确定对每个资源管理授权者的同时，还要确定他们可以对用户授予什么级别的权限。如果没有资源管理授权者的信息，就无法掌握究竟哪些人在使用网络。对于主干网络中的关键通信资源，对其可授权范围应尽可能小，范围越小就越容易管理，相对也就越安全。同时，还要制定对用户授权的过程设计，以防止对授权职责的滥用。网络安全策略中可以确定每个资源的系统级管理员，但在网络的使用中，难免会遇到用户需要特殊权限的时候。其中最好的一种处理办法是尽量只分配给用户够完成任务所需的最小权限。另外，在网络安全策略中要包含对特殊权限进行监测统计的部分，如果对授予用户的特殊权限不可统计，就难以保证整个网络不被侵害。

在明确网络用户、系统管理员的安全责任，正确利用网络资源要求的同时，还要准备检测到安全问题或系统遭受破坏时所采取的策略。对于发生在本网络内部的安全问题，要从主干网向子网逐级过滤、隔离。子网要与主干网形成配合，防止破坏蔓延。对于来自整个网络以外的安全干扰，除了必要的隔离与保护外，还要与对方所在网络进行联系，以进一步确定消除掉安全隐患。每一个网络安全问题都要有文档记录，包括对它的处理过程，并将其送至全网各有关部门，以便预防和留作今后进一步完善网络安全策略的资料。

网络安全策略还要包括本网络对其他相连网络的职责，如出现某个网络告知有威胁来自我方网络。在这种情况下，一般不会给予对方权利，让其到我方网络中进行调查，而是在验证对方身份的同时，自己对本方网络进行调查监控，做好相互配合。

最后，根据上述内容制定的网络安全对策最终一定是要发送至网络的每一个使用者手中。要十分清楚，对付安全问题最有效的手段是教育、提高每个使用者的安全意识，从而提高整体网络的安全免疫力。网络安全策略作为向所有使用者发放的手册，应注明其解释权归属何方，以免出现不必要的争端。

1.4 计算机网络安全的基本措施和安全意识

1.4.1 计算机网络安全的基本措施

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，避免因电磁泄漏而产生信息泄露，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 Internet 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够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 Internet Engineering Task Fore 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 认和服多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、假冒和篡改信息使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 激活底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。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，造成系统地崩溃；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。

1.4.2 计算机网络的安全意识

网络安全教育实际上关系到两个方面的问题。一是如何看待目前计算机网络，尤其是国际互联网中存在的各种各样的安全漏洞。在经过各种媒体对网络安全案例及其影响的报道和宣传后，是否就片面地认为网络是极不安全的，以至于错误地认为网络安全意识的增强仅仅是靠人们对网络的恐惧，从而限制了人们对网络的理解以及网络的进一步应用和发展。显而易见，这种认识是错误的。正如汽车部件和整体的安全缺陷，或是交通管理规则的混乱和不完善，并不能够阻止汽车工业的不断进步，并不能够阻止人们相互之间对物质和思想的交流。二是如何看待网络安全的公开讨论。从某种意义上说，网络安全更多的是对网络和系统知识的深入理解和对其技巧的大胆应用，与不安全因素的斗争实际上是多种技巧的较量。然而，只有很少的网络和系统管理人员关注网络上发布的安全警告消息。对系统中漏洞感兴趣的网民多是些发誓要当黑客的人，他们最先看到最新发布的各种系统的最新问题，这就告诉我们必须时刻关注网络的漏洞和不安全因素，不断提高网络的安全防范能力。

从社会教育和意识形态的角度来讲，网络上不健康的内容，将会对社会的稳定和人类的发明造成障碍，必须对其进行强有力的控制。计算机犯罪大都具有瞬时性、广域性、专业性、时空分离性等特点，通常很难留下犯罪证据，这大大刺激了计算机高技术犯罪案件的发生。安全教育的目的不仅是提高防范意识，同时还要自觉抵制利用计算机进行各类犯罪活动的诱惑；重视信息化的安全教育，还在于尽快培养出一批信息化安全的专门人才，这是实现网络安全之本；提高全民的信息化安全意识，使网络安全意识成为建立在法律约束之下的自律行为，这是实现网络安全的重要因素。

安全的问题归根结底是人的问题，安全问题的最终解决也要靠提高人的道德素质。虽然防火墙是一种好的防范措施，但只是网络整体安全防范政策的一部分。这种安全防范政策必须包括公开的让用户知道自身责任的安全准则、安全培训计划以及与网络访问、当地和远程用户认证、卡拨出拨入呼叫、磁盘和数据加密以及病毒防护的有关政策。在没有全面安全政策的情况下为网络设置防火墙，就如同在一顶棉帐篷上安装一个防盗门。

随着网络技术的发展，网络安全面临的挑战也在加大。一方面，对网络的攻击方式层出不穷：1996 年报道的攻击方式有 400 种，1997 年达到 1000 种，1998 年即达到 4000 种，