高职高专教育“十二五”规划教材

网络安全技术

主　编　吴　锐
副主编　王　伟　陈　亮　武春岭

中国水利水电出版社
www.waterpub.com.cn

高职高专教育“十二五”规划教材

网络安全技术

主　编　吴　锐

副主编　王　伟　陈　亮　武春岭

中国水利水电出版社
www.waterpub.com.cn

内 容 提 要

本书立足于“看得懂，学得会，用得上”的原则，结合目前国内高职高专学生的实际情况，舍弃了大篇幅的原理介绍，而将重点放在与实践中密切相关的黑客技术、网络入侵、密码技术及系统安全等当代网络安全突出问题上，并注重实用，以实训为依托，将实训内容融合在课程内容中，使理论紧密联系实际。在本书中引用了大量实例，并设置了实训操作练习，帮助读者掌握计算机网络安全方面存在的漏洞，以期更好地管理计算机系统。

全书共 12 章。分别从理论、技术、应用各个角度对网络安全进行分析和阐述，主要内容包括网络安全概述、网络安全基础、加密技术、病毒与反病毒、系统安全、应用安全、网络攻击与防御、防火墙、入侵检测、网络安全管理、网络安全的法律法规、安全实训。

本书适合于计算机及相关专业的学生作为教材或参考书，也可作为对网络安全感兴趣的初学者的自学教材。

本书所配教电子教案可以在中国水利水电出版社网站和万水书苑下载，网址为：http://www.waterpub.com.cn/softdown/和 http://www.wsbookshow.com，也可以与编者联系（mr.ruiwu@gmail.com），获取更多教学资源。

图书在版编目（CIP）数据

网络安全技术 / 吴锐主编. -- 北京 : 中国水利水电出版社, 2012.1
高职高专教育“十二五”规划教材
ISBN 978-7-5084-9245-2

Ⅰ. ①网… Ⅱ. ①吴… Ⅲ. ①计算机网络－安全技术－高等职业教育－教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2011)第258755号

策划编辑：雷顺加　责任编辑：杨元泓　加工编辑：陈　洁　封面设计：李　佳

书　名	高职高专教育“十二五”规划教材 **网络安全技术**
作　者	主　编　吴　锐 副主编　王　伟　陈　亮　武春岭
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（发行部）、82562819（万水）
经　售	北京科水图书销售中心（零售） 电话：（010）88383994、63202643、68545874 全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	北京泽宇印刷有限公司
规　格	184mm×260mm　16 开本　16.5 印张　416 千字
版　次	2012 年 1 月第 1 版　2012 年 1 月第 1 次印刷
印　数	0001—4000 册
定　价	30.00 元

高职高专教育“十二五”规划教材
编委会

前　言

网络安全技术涉及硬件平台、软件系统、基础协议等方方面面的问题，复杂而多变，本书写作的主要目的是帮助普通用户了解网络所面临的各种安全威胁，掌握保障网络安全的主要技术和方法，使用户学会在开放的网络环境中保护自己的信息和数据，防止黑客和病毒的侵害，有效地管理和使用计算机网络，保护自己的系统。

本书立足于“看得懂，学得会，用得上”的原则，结合目前国内高职高专学生的实际情况，舍弃了大篇幅的原理介绍，而将重点放在与实践中密切相关的黑客技术、网络入侵、密码技术及系统安全等当代网络安全突出问题上，并在这些章节中都引用了大量实例，设置了实训操作练习，帮助读者了解计算机网络安全方面存在的漏洞，以期更好地管理计算机系统。本书适合于计算机及相关专业的学生作为教材或参考书，也可作为对网络安全感兴趣的初学者的自学教材。希望读者在读完本书之后，可对网络安全技术有进一步的了解，并体验到掌握知识的乐趣。

全书共 12 章，分别从理论、技术、应用各个角度对网络安全进行分析和阐述。使读者对网络安全有一个系统而全面的认识。其中，前 10 章分别介绍网络安全的现状、应用技术、工具软件、规则协议、攻击防御手段等技术知识，第 11 章是与网络安全相关的法律法规，第 12 章给出了一些网络安全实训，帮助读者有效地理解本书所阐述的内容。

本书由吴锐任主编，王伟、陈亮、武春岭任副主编。各章编写分工如下：吴锐编写了第 1、4、5 章，王庆宇编写了第 2、3 章，王伟编写了第 6、第 7 章，陈亮编写了第 8、9 章，武春岭编写了第 10、11、12 章。参加本书案例选择、素材收集及实验验证的还有张丽敏、郑辉、宋蓓蓓、丁俊等，同时他们也是本课程教学团队的老师，感谢他们为本书资源建设所做的有益工作。

此外，还要感谢中国水利水电出版社的雷顺加编审，在本书的策划和写作中提出了很好的建议，对本书的出版给予了大力支持。在本书编写过程中参考了大量国内外计算机网络文献资料，在此，谨向这些作者及为本书出版付出辛勤劳动的同志深表感谢！

如需用到本书中所涉及各种工具软件及相关课件请联系编者索要，联系邮箱为：mr.ruiwu@gmail.com。

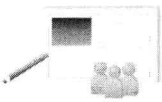
由于时间仓促，加之作者水平及视界所限，书中难免会有错误和疏漏之处，希望广大读者谅解并不吝批评指正。

编者

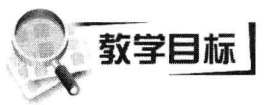
2011 年 10 月

目　　录

第 1 章　网络安全概述



本章简要介绍了计算机网络安全的基本概念，并阐述了网络安全从通信安全到信息安全再发展为信息安全保障的历程。作为网络安全的设计方法，掌握本章所阐述的几大安全原则并将其运用到后面章节的各种具体的技术设计中，将对网络安全的设计具有重要意义。



通过本章的学习，读者应掌握以下内容:

- 理解网络安全的基本概念和术语
- 了解目前主要的网络安全问题和安全威胁
- 了解网络和信息安全的重要性
- 了解国内外的信息安全保障体系

1.1　网络安全的基本概念

在互联网上最著名的搜索引擎中搜索“网络安全”这个词，共查到 80,000,000 余条记录，搜索“Net Safe”这个词，共查到 1,300,000,000 余条记录，而搜索“电视”这个词，共查到 100,000,000 余条记录。由此可见，网络安全随着互联网的发展，正逐渐成为人们生活中密不可分的一部分，而且越来越重要。

1.1.1　网络安全的定义及相关术语

1. 网络安全的定义

在解释网络安全这个术语之前，首先要明确计算机网络的定义，计算机网络是地理上分散的多台自主计算机互联的集合，这些计算机遵循约定的通信协议，使用通信设备、通信介质及网络软件共同实现信息交换、资源共享等功能。

所以，从广义上说，网络安全包括网络硬件资源及信息资源的安全性。硬件资源包括通信线路、通信设备（交换机、路由器等）、主机等，要实现信息快速、安全的交换，一个可靠的物理网络是必不可少的。信息资源包括维持网络服务运行的系统软件和应用软件，以及在网络中存储和传输的用户信息数据等。信息资源的保密性、完整性、可用性、真实性等是网络安全研究的重要课题，也是本书涉及的重点内容。

从用户角度看，网络安全主要是保障个人数据或企业的信息在网络中的保密性、完整性、不可否认性，防止信息的泄露和破坏，防止信息资源的非授权访问。对于网络管理者来说，网

络安全的主要任务是保障合法用户正常使用网络资源，避免病毒、拒绝服务、远程控制、非授权访问等安全威胁，及时发现安全漏洞，制止攻击行为等。从教育和意识形态方面，网络安全主要是保障信息内容的合法与健康，控制含不良内容的信息在网络中的传播。

可见网络安全的内容是十分广泛的，不同的人群对其有不同的理解。在此对网络安全下一个通用的定义：网络安全是指保护网络系统中的软件、硬件及信息资源，使之免受偶然或恶意的破坏、篡改和泄露，保证网络系统的正常运行、网络服务不中断。

2. 网络安全的属性

在美国国家信息基础设施（NII）的文献中，给出了网络安全的 5 个属性：可用性、机密性、完整性、可控性和可审查性。这 5 个属性适用于国家信息基础设施的各个领域，如教育、娱乐、医疗、运输、国家安全、通信等。

- 保密性：信息不泄露给非授权用户、实体或过程，或供其利用的特性。
- 完整性：数据未经授权不能进行改变的特性，即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。
- 可用性：可被授权实体访问并按需求使用的特性，即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等，都属于对可用性的攻击。
- 可控性：对信息的传播及内容具有控制能力。
- 可审查性：出现安全问题时提供依据与手段。

1.1.2 网络安全现状

近年来，随着网络安全事件的频频发生，人们对外部入侵和互联网的安全日益重视，但来自内部网络的攻击却越演越烈，内网安全已成为企业管理的隐患。信息资料被非法泄露、复制、篡改，往往给各行业企事业单位造成重大损失。而如何使内部网络始终处于安全、可靠、保密的环境之下运行，帮助企业各类业务统一优化、规范管理，保障各类业务正常安全运行等一系列的问题困扰着各行业企、事业单位的 IT 部门。

1. 资产管理失控

在现代化大型企业中，拥有数以百计的客户端等 IT 资产是常见的事情。由于客户端分布分散，资产统计与维护十分困难。另外，企业为员工提供的软硬件资产是要求员工在工作的环境下，为企业创造价值，可是很多员工却把这些资产滥用，甚至挪为私用，管理不善的笔记本、CPU、内存，甚至网卡、主板、硬盘等都被使用者更换掉，导致不必要的信息数据泄露。

2. 外接设备滥用

市场战略规划、产品价格体系、自主研发的核心技术等商业机密成为企业目前关注的重点。如何保证企业数据信息的安全性，降低安全风险，这些问题亟待解决。同时公司的软驱、光驱、USB、并口、串口等各种外部存储设备滥用带来的一系列信息安全隐患，增加商业机密外泄机率，如何对网内计算机各种外接设备进行控制，并防止利用移动存储设备进行数据文件的拷贝？

3. 补丁管理混乱

每隔一段时间微软发布修复系统漏洞的更新版本，但很多终端用户不了解系统补丁状态，不能及时使用这些更新修复系统（打补丁）。网络规模越来越庞大，网络管理员要保证每台终端及时、全面地安装响应更新，统一进行补丁的下载、分析、测试和分发，工作量很大且很难实现，从而为蠕虫与黑客入侵保留了通道。

4. 病毒蠕虫入侵

由于补丁更新不及时，网络滥用、移动设备（如笔记本电脑）和新增设备未经过安全检查和处理非法接入等因素导致内网病毒泛滥、黑客入侵、网络阻塞、数据损坏丢失等不安全因素，而且无法找到灾难的源头以迅速采取隔离等处理措施，给我们的内网安全带来了巨大的隐患，从而为正常业务带来灾难性的持续影响。

5. 违规上网行为

“水能载舟亦能覆舟”，互联网在帮助企业提高生产力、促进企业发展，并为人们的生活与工作带来便捷性的同时也带来很多安全隐患；而企业内部却存有各种与工作无关的非许可性上网行为现象，如泡论坛、写博客、在线聊天、发私人邮件，甚至长时间访问非法网站等已经司空见惯，然而信息的机密性、健康性、政治性等问题也随之而来。

6. 网络流量异常

P2P 下载、看电影、玩游戏、炒股票以及访问如色情、赌博等具有高度安全风险的网页，企业员工于互联网上的应用可谓五花八门，如果员工长期沉迷于这些应用，在成为企业生产效率的巨大杀手的同时，都在抢占着有限的带宽资源，并可能造成网速缓慢、信息外泄的可能。面对日益紧张的带宽资源，若无法了解客户端流量应用信息，一旦发生流量异常，IT 运维人员无法及时了解流量异常情况。

7. IP 地址随意更改

企业网络中由于用户原因造成使用管理混乱；网管人员无法知道 IP 地址的使用、IP 同 MAC 地址的绑定情况及网络中 IP 分配情况；没有严格的管理策略，员工随意设置 IP 地址，可能造成 IP 地址冲突、关键设备发生异常。若出现恶意盗用、冒用 IP 地址以谋求非法利益，后果将更为严重。如何防止单位内部员工私自更改个人计算机的 IP 地址和 MAC 地址上网，导致与其他员工的 IP 冲突，从而保证企业员工的正常办公。

8. 安全设备成摆设

为了保障企业网络安全，“堵漏洞、砌高墙、防外攻、防内贼，防不胜防”，防火墙越“砌”越“高”，入侵检测越做越复杂，病毒库越来越庞大，身份系统层层设保，却依然无法应对层出不穷网络安全威胁，难道那么多安全产品都是摆设？企业已有如防火墙、IDS 入侵检测系统、防病毒系统、网闸、加密系统等各种安全设备，但是各自为政，无法协同工作，导致单独系统的信息孤岛。如何真正地保障业务系统的安全，并将各种安全设备进行综合管理。

1.2　主要的网络安全威胁

由于计算机信息系统已经成为信息社会另一种形式的“金库”和“保密室”，成为一些人窥视的目标；再者，由于计算机信息系统自身所固有的脆弱性，使计算机信息系统面临威胁和攻击的考验，而计算机信息系统的安全主要体现在计算机网络的安全上，保护网络安全的最终目的就是保护计算机信息系统的安全。计算机网络的安全同时来自内、外两个方面。

1.2.1　外部威胁

1. 自然灾害

计算机网络是一个由用传输介质连接起来的地理位置不同的计算机组成的“网”，易受火灾、水灾、风暴、地震等破坏及环境（温度、湿度、振动、冲击、污染）的影响。目前，不少

计算机机房并没有防震、防火、防水、避雷、防电磁泄漏或干扰等措施，接地系统也疏于周到考虑，抵御自然灾害和意外事故的能力较差。日常工作中因断电使设备损坏、数据丢失的现象时有发生。

灾害轻则造成业务工作混乱，重则造成系统中断，甚至造成无法估量的损失。例如，1999年8月吉林省某电信业务部门的通信设备被雷击中，造成惊人的损失；还有某铁路计算机系统遭受雷击，造成设备损坏、铁路运输中断等。

2. 黑客

计算机信息网络上的黑客攻击事件愈演愈烈，已经成为具有一定经济条件和技术专长的形形色色攻击者活动的舞台。黑客破坏了信息网络的正常使用状态，造成可怕的系统破坏和巨大的经济损失。

3. 计算机病毒

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、毁坏数据、影响计算机使用并能自我复制的一组计算机指令或者程序代码。

“计算机病毒”将自己附在其他程序上，在这些程序运行时进入到网络系统中进行扩散。一台计算机感染上病毒后，轻则系统工作效率下降，使部分文件丢失，重则造成系统死机或毁坏，使全部数据丢失。1999年4月26日，CIH病毒在全球造成的危害足以显露计算机病毒的可怕。

据一份市场调查报告表明，我国约有 90%的网络用户曾遭到过病毒的侵袭，并且其中大部分因此受到损失。病毒危害的泛滥说明了计算机系统和人们在安全意识方面的薄弱。

4. 垃圾邮件和黄毒泛滥

一些人利用电子邮件地址的“公开性”和系统的“可广播性”进行商业、宗教、政治等活动，把自己的电子邮件强行“推入”别人的电子邮箱，甚至塞满别人的电子邮箱，强迫别人接收他们的垃圾邮件。

国际互联网的广域性和自身的多媒体功能也给黄毒的泛滥提供了可乘之机。

5. 经济和商业间谍

通过信息网络获取经济、商业情报和信息的威胁大大增加。大量的国家和社团组织上网，在丰富网上内容的同时，也为外国情报收集者提供了捷径，通过访问公告牌、网页及内部电子邮箱，利用信息网络的高速信息处理能力，进行信息分析以获取情报。

6. 电子商务和电子支付的安全隐患

计算机信息网络的电子商务和电子支付的应用给人们展现了美好前景，但网上安全措施和手段的缺乏阻碍了它的快速发展。

7. 信息战的严重威胁

所谓信息战，就是为了国家的军事战略而采取行动，取得信息优势，干扰敌方的信息和信息系统，同时保卫自己的信息和信息系统。这种对抗形式的目标不是集中打击敌方的人员或战斗技术装备，而是打击敌方的计算机信息系统，使其神经中枢似的指挥系统瘫痪。

信息技术从根本上改变了进行战争的方法，信息武器已成为继原子武器、生物武器、化学武器之后的第四类战略武器。

在海湾战争中，信息武器首次进入实战。伊拉克的指挥系统吃尽了美国的苦头：购买的智能打印机被塞进了一片带有病毒的集成电路芯片，加上其他因素，最终导致系统崩溃，指挥失灵，几十万伊军被几万联合国维和部队俘虏。美国的维和部队还利用国际卫星的全球计算机

网络，为其建立军事目的的全球数据电视系统服务。所以，未来国与国之间的对抗首先来自信息技术的较量。网络信息安全应该成为国家安全的前提。

8. 计算机犯罪

计算机犯罪是利用暴力和非暴力形式，故意泄漏或破坏系统中的机密信息，以及危害系统实体和信息安全的不法行为。《中华人民共和国刑法》对计算机犯罪做了明确定义，即利用计算机技术知识进行犯罪活动，并将计算机信息系统作为犯罪对象。

利用计算机犯罪的人通常利用窃取口令等手段，非法侵入计算机信息系统，利用计算机传播反动和色情等有害信息，或实施贪污、盗窃、诈骗和金融犯罪等活动，甚至恶意破坏计算机系统。

1.2.2　内部威胁

由于计算机信息网络是一个“人机系统”，所以内部威胁主要来自使用的信息网络系统的脆弱性和使用该系统的人。外部的各种威胁因素和形形色色的进攻手段之所以起作用，是由于计算机系统本身存在着脆弱性，抵御攻击的能力很弱，自身的一些缺陷常常容易被非授权用户不断利用，外因通过内因起变化。

（1）软件工程的复杂性和多样性使得软件产品不可避免地存在各种漏洞。世界上没有一家软件公司能够做到其开发的产品设计完全正确，而且没有缺陷，这些缺陷正是计算机病毒蔓延和黑客“随心所欲”的温床。

（2）电磁辐射也可能泄漏有用信息。已有试验表明，在一定的距离以内接收计算机因地线、电源线、信号线或计算机终端辐射导致的电磁泄漏产生的电磁信号，可复原正在处理的机密或敏感信息，如“黑客”们利用电磁泄漏或搭线窃听等方式可截获机密信息，或通过对信息流向、流量、通信频率和波段等参数的分析，推断出有用信息，如用户口令、账号等重要信息。

（3）网络环境下电子数据的可访问性对信息的潜在威胁比对传统信息的潜在威胁大得多。

非网络环境下，任何一个想要窃密的人都必须先解决潜入秘密区域的难题；而在网络环境下，这个难题已不复存在，只要有足够的技术能力和耐心即可。

（4）不安全的网络通信信道和通信协议。信息网络自身的运行机制是一种开放性的协议机制。网络节点之间的通信是按照固定的机制，通过协议数据单元来完成的，以保证信息流按“包”或“帧”的形式无差错地传输。那么，只要所传的信息格式符合协议所规定的协议数据单元格式，那么，这些信息“包”或“帧”就可以在网上自由通行。至于这些协议数据单元是否来自真正的发送方，其内容是否真实，显然无法保证。这是在早期制定协议时，只考虑信息的无差错传输所带来的固有的安全漏洞，更何况某些协议本身在具体的实现过程中也可能会产生一些安全方面的缺陷。对一般的通信线路，可以利用搭线窃听技术来截获线路上传输的数据包，甚至重放（一种攻击方法）以前的数据包或篡改截获的数据包后再发出（主动攻击），这种搭线窃听并不比用窃听器听别人的电话困难多少。对于卫星通信信道而言，则既需要有专门的接收设备（类似于电视信号的地面接收器），又要求有较高的技术安装设备（如天线方位和角度的调整及其他参数的设置等）。

（5）内部人员的不忠诚、人员的非授权操作和内外勾结作案是威胁计算机信息网络安全的重要因素。

“没有家贼，引不来外鬼”就是这个道理。他们或因利欲熏心，或因对领导不满，或出

于某种政治、经济或军事的特殊使命，从机构内部利用权限或超越权限进行违反法纪的活动。统计表明，信息网络安全事件中 60%～70%起源于内部。我们要牢记“防内重于防外”。

1.2.3 网络安全威胁的主要表现形式

网络中的信息和设备所面临的安全威胁有着多种多样的具体表现形式，而且威胁的表现形式随着硬件技术的不断发展，也在不断地进化。这里将一些典型的危害网络安全的行为总结如表 1-1 所示。

表 1-1 威胁的主要表现形式

威胁	描述
授权侵犯	为某一特定目的被授权使用某个系统的人，将该系统用作其他未授权的目的
旁路控制	攻击者发掘系统的缺陷或安全弱点，从而渗入系统
拒绝服务	合法访问被无条件拒绝和推迟
窃听	在监视通信的过程中获得信息
电磁泄漏	从设备发出的电磁辐射中泄漏信息
非法使用	资源被某个未授权的人或以未授权的方式使用
信息泄露	信息泄露给未授权实体
完整性破坏	对数据的未授权创建、修改或破坏造成数据一致性损害
假冒	一个实体假装成另一个实体
物理侵入	入侵者绕过物理控制而获得对系统的访问权
重放	出于非法目的而重新发送截获的合法通信数据的拷贝
否认	参与通信的一方事后否认曾经发生过此次通信
资源耗尽	某一资源被故意超负荷使用，导致其他用户的服务被中断
业务流分析	通过对业务流模式进行观察（有、无、数量、方向、频率），而使信息泄露给未授权实体
特洛伊木马	含有觉察不出或无害程序段的软件，当它被运行时，会损害用户的安全
陷门	在某个系统或文件中预先设置的“机关”，使得当提供特定的输入时，允许违反安全策略
人员疏忽	一个授权的人出于某种动机或由于粗心将信息泄露给未授权的人

1.2.4 网络出现安全威胁的原因

引起网络的安全问题的原因，可以归纳为以下几种。

1. 薄弱的认证环节

网络上的认证通常是使用口令来实现的，但口令有公认的薄弱性。网上口令可以通过许多方法破译，其中最常用的两种方法是把加密的口令解密和通过信道窃取口令。例如，UNIX 操作系统通常把加密的口令保存在一个文件中，而该文件普通用户即可读取。该口令文件可以通过简单的拷贝或其他方法得到。一旦口令文件被闯入者得到，他们就可以使用解密程序对口令进行解密，然后用它来获取对系统的访问权。

2. 系统的易被监视性

用户使用 Telnet 或 FTP 连接他在远程主机上的账户，在网上传的口令是没有加密的。入侵者可以通过监视携带用户名和口令的 IP 包获取它们，然后使用这些用户名和口令通过正常

渠道登录到系统。如果被截获的是管理员的口令，那么获取特权级访问就变得更容易了。成千上万的系统就是被这种方式侵入的。

3. 易欺骗性

TCP 或 UDP 服务相信主机的地址。如果使用“IP Source Routing”，那么攻击者的主机就可以冒充一个被信任的主机或客户。使用“IP Source Routing”，采用以下操作可把攻击者的系统假扮成某一特定服务器的可信任的客户。

4. 有缺陷的局域网服务和相互信任的主机

主机的安全管理既困难又费时。为了降低管理要求并增强局域网，一些站点使用了诸如 NIS 和 NFS 之类的服务。这些服务通过允许一些数据库（如口令文件）以分布式方式管理以及允许系统共享文件和数据，在很大程度上减轻了过多的管理工作量。但这些服务带来了不安全因素，可以被有经验闯入者利用以获得访问权。如果一个中央服务器遭受到损失，那么其他信任该系统的系统会更容易遭受损害。

5. 复杂的设置和控制

主机系统的访问控制配置复杂且难以验证，因此偶然的配置错误会使闯入者获取访问权。一些主要的 UNIX 经销商仍然把 UNIX 配置成具有最大访问权的系统，这将导致未经许可的访问。

许多网上的安全事故原因是由于入侵者发现的弱点造成的。由于目前大部分的 UNIX 系统都是从 BSD 获得网络部分的代码，而 BSD 的源代码又可以轻易获得，所以闯入者可以通过研究其中可利用的缺陷来侵入系统。存在缺陷的部分原因是因为软件的复杂性，而没有能力在各种环境中进行测试。有时候缺陷很容易被发现和修改，而另一些时候除了重写软件外几乎不能做什么（如 Sendmail）。

6. 无法估计主机的安全性

主机系统的安全性无法很好的估计。随着一个站点主机数量的增加，确保每台主机的安全性都处在高水平的能力却在下降。只用管理一台系统的能力来管理如此多的系统就容易犯错误。另外，系统管理的作用经常变换并行动迟缓，这导致一些系统的安全性比另一些要低。这些系统将成为薄弱环节，最终将破坏这个安全链。

1.3　网络安全措施

1.3.1　安全技术手段

1. 物理措施

例如，保护网络关键设备（如交换机、大型计算机等），制定严格的网络安全规章制度，采取防辐射、防火及安装不间断电源（UPS）等措施。

2. 访问控制

对用户访问网络资源的权限进行严格的认证和控制。例如，进行用户身份认证，对口令加密、更新和鉴别，设置用户访问目录和文件的权限，控制网络设备配置的权限等。

3. 数据加密

加密是保护数据安全的重要手段。加密的作用是保障信息被人截获后不能读懂其含义。防止计算机网络病毒，安装网络防病毒系统。

4. 网络隔离

网络隔离有两种方式：一种是采用隔离卡来实现的；另一种是采用网络安全隔离网闸实现的。隔离卡主要用于对单台机器的隔离，网闸主要用于对于整个网络的隔离。

5. 其他措施

其他措施包括信息过滤、容错、数据镜像、数据备份和审计等。近年来，围绕网络安全问题提出了许多解决办法，如数据加密技术和防火墙技术等。数据加密是对网络中传输的数据进行加密，到达目的地后再解密还原为原始数据，目的是防止非法用户截获后盗用信息。防火墙技术是通过对网络的隔离和限制访问等方法来控制网络的访问权限。

1.3.2 安全防范意识

拥有网络安全意识是保证网络安全的重要前提。许多网络安全事件的发生都和缺乏安全防范意识有关。对于网络用户来说，提高网络安全防范意识是解决安全问题的根本。具体地说，凡是来自于网上的东西都要持谨慎态度。

1.3.3 主机安全检查

要保证网络安全，进行网络安全建设，第一步首先要全面了解系统，评估系统安全性，认识到自己的风险所在，从而迅速、准确地解决内网安全问题。由安天实验室自主研发的国内首款创新型自动主机安全检查工具，彻底颠覆传统系统保密检查和系统风险评测工具操作的繁冗性，一键操作即可对内网计算机进行全面的安全保密检查及精准的安全等级判定，并对评测系统进行强有力的分析处置和修复。

1.4 网络安全标准与体系

安全服务是由网络安全设备提供的，它为保护网络安全提供服务。保护信息安全所采用的手段称为安全机制。安全服务和安全机制对安全系统设计者有不同的含义，但对安全分析来说其含义是相同的。所有的安全机制都是针对某些安全攻击威胁而设计的，它们可以按不同的方式单独使用，也可组合使用。合理地使用安全机制，会在有限的投入下最大限度地降低安全风险。

1.4.1 可信计算机系统评价准则简介

为实现对网络安全的定性评价，美国国防部所属的国家计算机安全中心（NCSC）在 20 世纪 90 年代提出了网络安全性标准（DoD5200.28-STD），即可信任计算机标准评估准则（Trusted Computer Standards Evaluation Criteria），也叫橘皮书（Orange Book），认为要使系统免受攻击，对应不同的安全级别，硬件、软件和存储的信息应实施不同的安全保护。安全级别对不同类型的物理安全、用户身份验证（Authentication）、操作系统软件的可信任性和用户应用程序进行了安全描述，标准限制了可连接到你的主机系统的系统类型。

网络安全性标准将网络安全性等级划分为 A、B、C、D 四类，其中，A 类安全等级最高，D 类安全等级最低。

1.4.2 国际安全标准简介

数据加密的标准化工作在国外很早就开始了。比如，1976 年美国国家标准局就颁布了“数