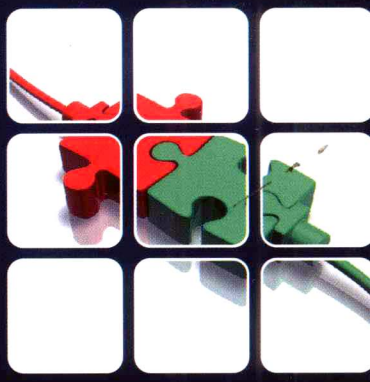
21st CENTURY
实用规划教材

21世纪全国高职高专
计算机系列实用规划教材

全新推出第2版

网络安全基础教程与实训（第2版）

主　编　尹少平



COMPUTER

内容特点：

- 扩充了应用案例和实训项目
- 增加了网络安全新技术内容

赠送 教学参考资料 www.pup6.com

北京大学出版社
PEKING UNIVERSITY PRESS

21 世纪全国高职高专计算机系列实用规划教材

网络安全基础教程与实训
（第 2 版）

主　编　尹少平
参　编　张平华

北京大学出版社
PEKING UNIVERSITY PRESS

内 容 简 介

本书是《网络安全基础教程与实训》的第2版，各章都进行了修整，扩充了应用案例和实训项目，删除了较为陈旧的示例，增加了网络安全新技术内容，更加全面和系统，基本能够涵盖高职高专学生对于网络安全技术应当掌握和了解的知识和方法。

本书共分11章，主要内容包括：网络安全概论、网络监听与TCP/IP协议分析、密码技术、操作系统安全、病毒分析与防御、Internet应用服务安全、防火墙、入侵检测系统、网络攻击与防范、VPN技术、和综合实训。

本书注重实践技能的培养，以实训为依托，深入浅出地讲解理论知识，因此既可作为高职高专院校计算机及相关专业的学生教材，也可作为计算机网络安全类的技术参考书或培训教材。

图书在版编目(CIP)数据

网络安全基础教程与实训/尹少平主编.—2版.—北京：北京大学出版社，2010.2

(21世纪全国高职高专计算机系列实用规划教材)

ISBN 978-7-301-16877-6

Ⅰ. 网… Ⅱ. 尹… Ⅲ. 计算机网络—安全技术—高等学校：技术学校—教材 Ⅳ. TP393.08

中国版本图书馆CIP数据核字(2010)第017158号

书　　名：网络安全基础教程与实训（第2版）

著作责任者：尹少平　主编

责 任 编 辑：李彦红

标 准 书 号：ISBN 978-7-301-16877-6/TP·1081

出 版 者：北京大学出版社

地　　址：北京市海淀区成府路205号　100871

网　　址：http://www.pup.cn　http://www.pup6.com

电　　话：邮购部62752015　发行部62750672　编辑部62750667　出版部62754962

电 子 邮 箱：pup_6@163.com

印 刷 者：三河市北燕印装有限公司

发 行 者：北京大学出版社

经 销 者：新华书店

787毫米×1092毫米　16开本　18.75印张　432千字

2005年9月第1版　2010年2月第2版　2010年2月第1次印刷

定　　价：30.00元

第 2 版　前言

第 2 版在第 1 版基础上做了较大修整，扩充了应用案例和实训项目，删除了较为陈旧的示例，增加了网络安全新技术内容，内容更加全面和系统，表述更为规范和准确，基本能够涵盖高职高专学生对于网络安全技术应当掌握和了解的知识和方法。针对第 1 版的改动如下。

第 1 章对网络安全内涵的阐述前后重复的部分做了删减；第 2 章标题做了修改，原内容做了精简，增加了应用案例；第 3 章为本书的重点，内容做了较大扩充，增加了成熟的密码学应用案例 PGP 和 SET 的讲述，并增加了 PGP 的实训项目，另外还修改了 DSA 算法描述中的错误；第 4 章修改了标题，增加了最新操作系统 Windows Server 2008 和常用操作系统 Linux 的安全性阐述；第 5 章删减了原书中的病毒示例，增加了比较新的梅勒斯病毒分析，增加了 2009 年最新防杀病毒软件的新技术应用案例，修改和补充了实训项目；第 9 章删减了较陈旧的内容，如木马示例，增加了 Web 安全一节；增加了第 11 章综合实训；第 6 章、第 7 章、第 8 章和第 10 章内容做了适当的改动，在此不一一赘述。

学完本书，学生将具备网络协议分析、操作系统安全配置、密码技术应用、防病毒软件的应用、防火墙的安装与使用、入侵检测系统和 VPN 系统的配置等方面的能力，能胜任初中级的网络安全管理和安全系统集成的工作。

建议学时安排如下。

章名	课堂讲授学时	实训学时	章名	课堂讲授学时	实训学时
第 1 章	2		第 7 章	2	2
第 2 章	2	2	第 8 章	2	2
第 3 章	6	4	第 9 章	4	6
第 4 章	4	2	第 10 章	4	4
第 5 章	2	2	第 11 章		4
第 6 章	2	2			

本书第 1 版由常州信息职业技术学院杨诚编写第 1 章，石家庄计算机职业学院的李磊编写第 2 章，石家庄职业技术学院的张恒杰编写第 3 章，石家庄职业技术学院的张军编写第 5 章，辽东学院信息技术学院的刘华谱编写第 4、6 章，太原电力高等专科学校的尹少平编写第 7、8、9、10 章。杨诚、尹少平担任主编，刘华谱、张恒杰担任副主编。

第 2 版由太原电力高等专科学校的尹少平主编。第 2 章由万博科技职业学院张平华编写，其他章节由尹少平统一编写和修订。

由于编者水平有限，时间仓促，书中不妥之处在所难免，恳请广大读者批评指正。

编　者

2009 年 12 月

目　录

第 1 章　网络安全概论

教学目标

通过对本章的学习，能够理解网络安全的基本概念，初步了解网络安全的问题、目标、网络安全组件、体系结构和管理策略。

教学要求

知识要点	能力要求	相关知识
网络安全定义	掌握网络安全定义和属性	
网络安全标准	熟悉网络安全国际标准规范要点	
网络安全策略	了解网络安全策略的 3 个方面和实施要点	

引例

所谓“网络安全”，其实质就是计算机网络环境中的信息安全。网络安全与传统纸质方式的信息安全的不同之处简要列举如下。

传统方式下，复制品与原件存在不同；用手写体签名或者图章来表明文件的真实性和有效性，而模仿的签名与原始的签名有差异并且可以鉴别；用铅封来防止文件在传送中被非法阅读或篡改；用保险柜来防止文件在保管中被盗窃、毁坏、非法阅读或篡改；信息安全依赖于物理手段与行政管理。

计算机网络环境中，复制后的文件跟原始文件没有差别；无法像传统方式一样在文件上直接签名或盖章；只能用密码技术和访问控制技术防止文件在传输和存储过程中被盗窃、非法阅读或篡改；信息安全不能完全依赖于物理手段与行政管理。

随着网络技术及其应用的深入和普及，电子商务、电子政务的开展、实施和应用，网络安全已经不再仅仅为科学研究人员和少数黑客所涉足，日益庞大的网络用户群同样需要掌握网络安全知识。只有这样，才有可能构筑属于全社会的信息安全体系。

1.1　网络安全简介

以 Internet 为代表的全球性信息化浪潮所带来的影响日益深刻，信息网络技术的应用正日益普及，应用层次正在深入，应用领域从传统的、小型业务系统逐渐向大型的、关键业务系统扩展，典型的如党政部门信息系统、金融业务系统、企业商务系统等。伴随网络的普及，安全日益成为影响网络效能的重要因素，而 Internet 所具有的开放性、国际性和自由性在增加应用自由度的同时，对安全提出了更高的要求，这主要表现在以下两个方面。

(1) 开放性的网络，导致网络的技术是全开放的，任何组织和个人都可能获得，因而网络所面临的破坏和攻击可能是多方面的。例如：任何具有不良企图的黑客都可以对物理传输线路实施攻击，也可以对网络通信协议实施攻击，可以对软件实施攻击，也可以对硬件实施攻击。网络的国际化还意味着网络的攻击不仅仅来自本地网络用户，还可以来自 Internet 上的任何一台主机，也就是说，网络安全所面临的是一个国际化的挑战。

(2) 自由意味着网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。用户只对自己的行为负责，而不受任何的法律限制。

开放的、自由的、国际化的 Internet 的发展给政府机构、企事业单位带来了革命性的改革和开放，使得人们能够利用 Internet 提高办事效率和市场反应能力，以便更具竞争力，同时人们又要面对网络开放带来的数据安全的新挑战和新危险。如何保护内部机密信息不受黑客和工业间谍的入侵，已成为政府机构、企事业单位信息化健康发展所必须考虑的重要事情之一。

1. 网络安全的概念

网络安全包括 5 个属性：机密性、完整性、可用性、可控性和可审查性。机密性指确保信息不暴露给未授权的实体或进程。完整性则意味着只有得到授权的实体才能修改数据，并且能够判别出数据是否已被篡改。可用性说明得到授权的实体在需要时可访问数据，即攻击者不能占用所有的资源而阻碍授权者的工作。可控性表示可以控制授权范围内的信息流向及行为方式。可审查性指对出现的网络安全问题提供调查的依据和手段。

网络安全的定义从狭义的保护角度来看，是指计算机及其网络系统资源和信息资源不受自然和人为有害因素的威胁和危害，从广义来说，凡是涉及计算机网络上信息的机密性、完整性、可用性、可控性、可审查性的相关技术和理论都是计算机网络安全的研究领域。

2. 网络安全的现状

现在全球普遍存在缺乏网络安全意识的状况。人们在组建一个网络的时候，并没有意识到网络安全的重要性。这导致大多数网络存在着先天性的安全漏洞和安全威胁。

国际上也存在着信息安全管理规范和标准不统一的问题。美国是西方国家中对信息安全着力较多的国家之一，同样存在着规范和标准跟不上技术进步发展的问题。西欧国家则另有一套信息安全标准，虽然在原理和结构上同美国有相同的部分，但是不同的部分也相当多。

在信息安全的发展过程中，企业和政府的要求有一致的地方，也有不一致的地方。企业更注重于信息和网络安全的可靠性，政府更注重信息和网络安全的可管性和可控性。由美国政府组织的 KRS 系统，就是由于企业不欢迎而无法推广。在发展中国家，对信息安全的投入还满足不了信息安全的需求，同时投入也常常被挪用和借用。

但不可忽视的现象是信息和安全的技术仍然在发展过程中。

同样在国内，网络安全产品的“假、大、空”现象在一定程度上普遍存在，防火墙变成了网络安全的全部。产生这种情况的原因是重技术、轻管理，以及网络安全知识的普及程度不够。

1.2　网络安全所产生的威胁

使用 TCP/IP 协议的网络所提供的网络服务都包含许多不安全的因素，存在着许多漏洞。同时，网络的普及使信息共享达到了一个新的层次，信息被暴露的机会大大增多，特别是 Internet 就是一个不设防的开放大系统。另外，数据处理的可访问性和资源共享的目的性之间是一对矛盾，这些都给网络带来了威胁。

1.2.1　网络中存在的威胁

目前网络中存在的威胁主要表现在以下几个方面。

1. 非授权访问

没有预先经过同意就使用网络或计算机资源被看作非授权访问，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，或擅自扩大权限，越权访问信息等。非授权访问主要包括以下几种形式：假冒、身份攻击、非法用户进入网络系统进行违法操作、合法用户以未授权方式进行操作等。

2. 泄露或丢失信息

泄露或丢失信息指敏感数据被有意泄露出去或丢失，通常包括信息在传输中丢失或泄露(如“黑客”们利用电磁泄漏或搭线窃听等方式截获机密信息，或通过对信息流向、流量、通信频度和长度等参数的分析，得到用户密码、账号等重要信息)，信息在存储介质中丢失或泄漏，敏感信息被隐蔽隧道窃取等。

3. 破坏数据完整性

破坏数据完整性指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等。

4. 拒绝服务攻击

拒绝服务攻击指通过不断对网络服务系统进行干扰，改变其正常的作业流程，执行无关程序响应来减慢甚至使网络服务瘫痪，影响正常用户的使用，导致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等。

5. 利用网络传播病毒

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。

1.2.2 主机网络安全

由于主机安全和网络安全的技术手段难以有机地结合，因此容易被入侵者各个击破。并且由于它们在保护计算机和信息的安全上各自为政，因此很难解决系统安全性和使用方便性之间的矛盾。举一个简单的例子，从严密保护主机安全来说应该禁止用户的远程登录，但是这将给用户的使用带来极大的不便，对 Internet 上绝大多数 UNIX 主机来说是不可以接受的。而一旦允许用户远程登录，却无法区分用户的远程登录是合法的还是非法的，也就控制不了非法用户的入侵，并且系统一旦被入侵，入侵者就拥有合法用户的全部权力，危害极大。对于防火墙系统来说也有同样的问题，防火墙可以禁止外部主机对于内部主机的访问(安全但不方便)，但是一旦允许用户经防火墙授权认证后进入内部主机，就无法控制其在内部主机上的行为(方便但不安全)。

为了解决这些问题，一种结合主机安全和网络安全的边缘安全技术开始兴起，这就是主机网络安全技术。主机网络安全技术是一种主动防御的安全技术，它结合网络访问的网络特性和操作系统特性来设置安全策略，用户可以根据网络访问的访问者及访问发生的时间、地点和行为来决定是否允许访问继续进行，以使同一用户在不同场所拥有不同的权限，从而保证合法用户的权限不被非法侵占。主机网络安全技术考虑的元素有 IP 地址、端口号、协议、MAC 地址等网络特性和用户、资源权限以及访问时间等操作系统特性，并通过对这些特性的综合考虑，来达到用户网络访问的细粒度控制。

与网络安全采用安全防火墙、安全路由器等在被保护主机之外的技术手段不同，主机网络安全所采用的技术手段通常在被保护的主机内实现，并且一般为软件形式。因为只有在被保护主机之上运行的软件，才能同时获得外部访问的网络特性以及所访问资源的操作系统特性。在当前广泛使用的计算机安全产品中，已经有一些软件在主机网络安全技术方面做了一些探索。

这类产品中，应用最为广泛的当属 Wietse Venema 开发的共享软件 TCP Wrapper。TCP Wrapper 是一种对进入的网络服务请求进行监视与过滤的工具，它可以截获 systat、finger、ftp、telnet、rlogin、rsh、exec、tftp、talk 等网络服务请求，并根据系统管理员设置的服务访问策略来禁止或允许服务请求。一般情况下，其策略主要考虑的是外部主机的域名(或 IP 地址)和请求的服务类型。通过扩充，还可以将请求访问的用户名和访问时间包括进来，即可以制定“在某时间允许/禁止某用户从外部某主机对某服务的访问”这样的策略。

另外，现在一些操作系统厂商已经或即将在操作系统中提供主机网络安全产品，如 IBM 公司在 AIX4.3.1 中引入了强制访问控制、控制访问的多级目录管理，并可内置 Check Point 公司的 Firewall-1/VPN-14.0；SUN 公司即将发布的 Solaris 中也将引入公共密钥结构(PKI)、基于 IP Security 的虚拟私有网络(VPN)和内置的防火墙。这些措施都将极大地改善主机的网络安全状况。不过它们都侧重于从访问的网络特性方面考虑，对于访问的操作系统特性考虑不够，因此对于冒充合法用户之类的攻击缺乏有效的办法。

1.2.3 主机网络安全系统体系结构

主机网络安全系统是为了解决主机安全性与访问方便性之间的矛盾，将用户访问时表现的网络特性和操作系统特性综合起来考虑，因此，这样的系统必须建立在被保护的主机上，并且贯穿于网络体系结构中的应用层、传输层、网络层之中。在不同的层次中，可以实现不同的安全策略，具体内容如下。

(1) 应用层：是网络访问的网络特性和操作系统特性的最佳结合点。通过对主机所提供服务的应用协议的分析，可以知道网络访问的行为，并根据用户设置的策略判断在当前环境下是否允许该行为；另外，还要附加更严格的身份论证。

(2) 传输层：是实现加密传输的首选层。对于使用了相同安全系统的主机之间的通信，可以实现透明的加密传输，而对于没有加密措施的通用客户软件之间的通信，仍可以使用不加密方式，并且加密与否对于用户来说是透明的。

(3) 网络层：是实现访问控制的首选层。通过对 IP 地址、协议、端口号的识别，能方便地实现包过滤功能。

当然，更复杂的设计可以在更多的层实现更多的安全功能，下面就前面的设想提出一个可行的主机网络安全系统的结构模型，如图 1.1 所示。

在图 1.1 所示的结构模型中，安全检查承担了防火墙的任务，它对进出的数据包按照系统设置的安全规则进行过滤，另外，在该模块中还可以实现加密/解密。对用户的访问进行细粒度控制是主机网络安全系统最为重要的特点，它包括两个方面：内部资源访问控制和外部资源访问控制。

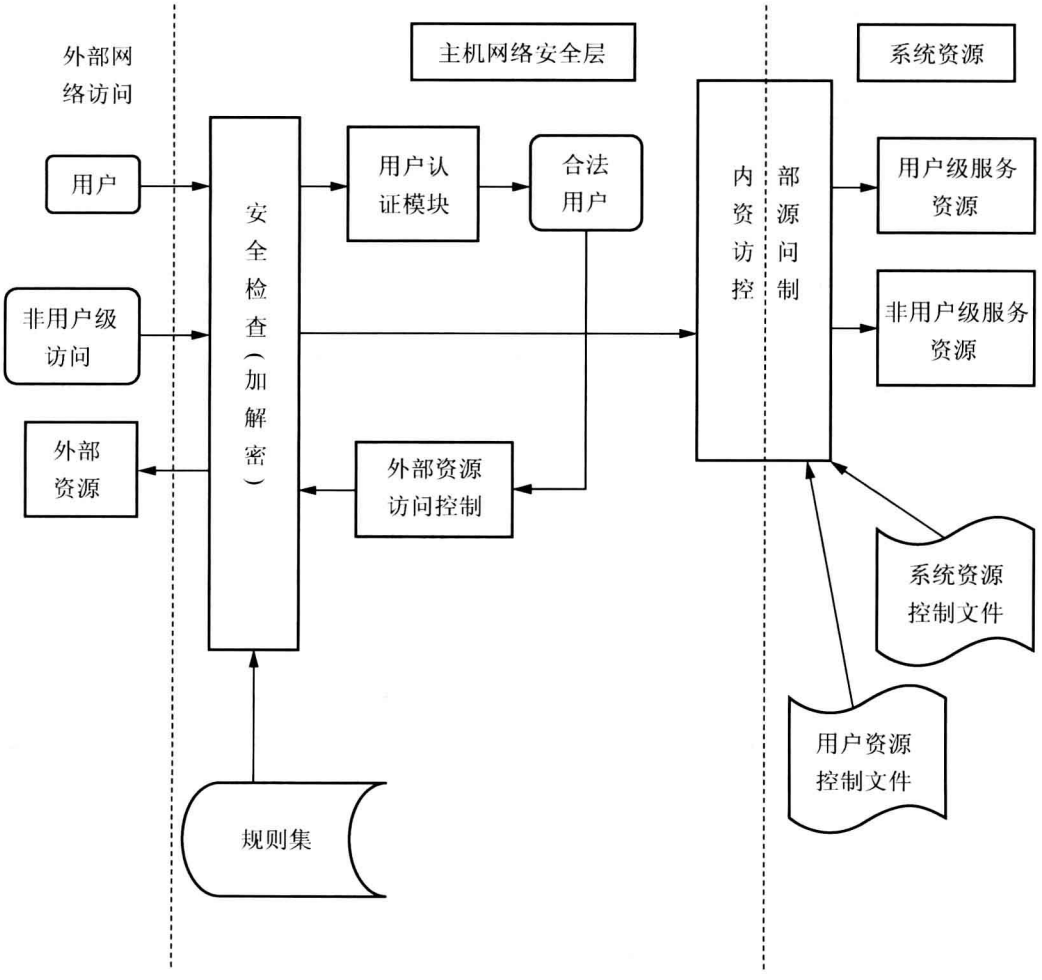


图 1.1　主机网络安全系统结构模型

内部资源访问控制主要是对网络用户(不管是合法用户还是入侵者)的权限进行控制，对用户的权限进行细致的分类控制、跟踪并及时阻止非法行为，防止用户利用系统的安全漏洞进行攻击。内部资源访问控制根据系统资源控制文件(全局作用)和用户资源控制文件(局部作用)来控制用户的行为。如系统资源控制文件可以设置“如果网络用户获取到ROOT权限(不管是使用系统命令获得还是利用系统漏洞取得)，则切断其连接”这样的规则，从而阻止入侵者获得超级权限严重威胁系统安全。又如用户资源控制文件可以设置“在某某时间某某地点(如日常工作场所)可以远程登录，其他情况下禁止远程登录”，这样的规则使用户既有系统之外的方便性又保证了系统的安全性。

外部资源访问控制是控制用户对系统之外网络资源的访问，如阻止网络用户通过本主机远程登录外部主机，即不允许将本地主机当作跳板(这是黑客最常见的行为)。

1.3　协议安全分析

计算机网络的运行机制基于网络协议，不同结点之间的信息交换按照事先约定的固定机制通过协议数据单元来完成。目前，TCP/IP 协议在 Internet 上一统天下。正是由于它的广泛使用性，使得 TCP/IP 的任何安全漏洞都会产生巨大的影响。TCP/IP 协议在设计初期并没有考虑到安全性问题，而是注重异构网的互联，而且用户和网络管理员没有足够的精力专注于网络安全控制，再加上操作系统越来越复杂，开发人员不可能测试出所有的安全漏洞，连接到网络上的计算机系统就可能受到外界的恶意攻击和窃取。

1. 物理层安全

物理层安全威胁主要指网络周边环境和物理特性引起的网络设备和线路的不可用而造成的网络系统的不可用，如设备老化、设备被盗、意外故障、设备损毁等。由于以太局域网中采用广播方式，因此，在某个广播域中利用嗅探器可以在设定的侦听端口侦听到所有的信息包，并且对信息包进行分析，那么本广播域的信息传递都会暴露无遗，所以需将两个网络从物理上隔断，同时保证在逻辑上两个网络能够连通。

2. 网络层安全

网络层的安全威胁主要有两类：IP 欺骗和 ICMP 攻击。

IP 欺骗技术的一种实现方法是把源 IP 地址改成一个错误的 IP 地址，而接收主机不能判断源 IP 地址的正确性，由此形成欺骗。另外一种方法是利用源路由 IP 数据包，让它仅仅被用于一个特殊的路径中传输，这种数据包被用于攻击防火墙。

Internet 控制信息协议(ICMP)在 IP 层检查错误和其他条件。ICMP 信息对于判断网络状况非常有用，例如，当 ping 一台主机想看它是否运行时，就产生了一条 ICMP 信息。远程主机将用它自己的 ICMP 信息对 ping 请求作出回应，这种过程在网络中普遍存在。然而，ICMP 信息能够被用于攻击远程网络或主机，利用 ICMP 来消耗带宽从而有效地摧毁站点。

3. 传输层安全

具体的传输层安全措施要取决于具体的协议。传输层安全协议 TLS 在 TCP 的顶部提供了如身份验证、完整性检验以及机密性保证这样的安全服务。TLS 需要为一个连接维持相应的场景，它是基于可靠的传输协议 TCP 的。由于安全机制与特定的传输协议有关，所以

像密钥管理这样的安全服务可为每种传输协议重复使用。

在 Internet 中提供安全服务的一个最初想法便是强化它的 IPC(广义的进程间通信)界面，具体做法包括双端实体的认证，数据加密密钥的交换等。Netscape 通信公司遵循了这个思路，制定了建立在可靠的传输服务基础上的安全套接层协议(SSL)“Secure Sockets Layer”，，它是 Netscape 公司提出的基于 Web 应用的安全协议。SSL 是一种在 Web 服务协议(HTTP)和 TCP/IP 之间提供数据连接安全性的协议。它为 TCP/IP 连接提供数据加密、用户和服务器身份验证以及消息完整性验证。SSL 被视为因特网上 Web 浏览器和服务器的安全标准。。SSL 版本 3(SSL v3)主要包含以下两个协议：SSL 记录协议和 SSL 握手协议。

4. 应用层安全

现在，应用层安全已经被分解成网络层、操作系统、数据库的安全，由于应用系统复杂多样，不存在一种安全技术能够完全解决一些特殊应用系统的安全问题。但对一些通用的应用程序，如 Web Server 程序、FTP 服务程序、E-mail 服务程序、浏览器、MS Office 办公软件等，可以通过互联网扫描服务和系统扫描服务检查应用程序自身的安全漏洞和由于配置不当造成的安全漏洞，在最大程度上避免安全隐患。

1.4　网络安全标准

针对日益严峻的网络安全形势，许多国家和标准化组织纷纷出台了相关的安全标准，我国也制定了相应的安全标准，这些标准既有很多相同的部分，也有各自的特点。其中以美国国防部制定的可信计算机安全标准(TCSEC)应用最为广泛。

1.4.1　网络安全主要国际标准

国际性的标准化组织主要有国际标准化组织(ISO)、国际电器技术委员会(IEC)及国际电信联盟(ITU)所属的电信标准化组织(ITU-TS)。ISO 是总体标准化组织，而 IEC 在电工与电子技术领域里相当于 ISO 的位置。1987 年，ISO 的 TC97 和 IEC 的 TCS47B/83 合并成为 ISO/IEU 联合技术委员会(JTC1)。ITU-TS 是联合缔约组织。这些组织在安全需求服务分析指导、安全技术研制开发、安全评估标准等方面制定了一些标准草案，但尚未正式执行。另外还有众多的标准化组织，它们也制定了不少安全标准，如 IETF 就有 9 个功能组：认证防火墙测试组(AFT)、公共认证技术组(CAT)、域名安全组(DNSSEC)、IP 安全协议组(IPSEC)、一次性密码认证组(OTP)、公开密钥结构组(PKIX)、安全界面组(SECSH)、简单公开密钥结构组(SPKI)、传输层安全组(TLS)和 Web 安全组(WTS)等，它们都制定了相关的标准。

1. 美国 TCSEC(橘皮书)

该标准是美国国防部制定的。它将安全分为 4 个方面：安全政策、可说明性、安全保障和文档。这 4 个方面又分为 7 个安全级别，从低到高依次为 D1、C1、C2、B1、B2、B3 和 A1 级。

2. 欧洲 ITSEC

ITSEC 与 TCSEC 不同，它并不把保密措施直接与计算机功能相联系，而是只叙述技术安全的要求，把保密作为安全增强功能。另外，TCSEC 把保密作为安全的重点，而 ITSEC

则把完整性、可用性与保密性作为同等重要的因素。ITSEC 定义了从 E0 级(不满足品质)到 E6 级(形式化验证)的 7 个安全等级，对于每个系统，安全功能可分别定义。ITSEC 预定义了 10 种功能，其中前 5 种与橘皮书中的 C1～B3 级非常相似。

3. 加拿大 CTCPEC

该标准将安全需求分为 4 个层次：机密性、完整性、可靠性和可说明性。

4. 美国联邦准则(FC)

该标准参照了 CTCPEC 及 TCSEC，其目的是提供 TCSEC 的升级版本，同时保护已有投资。FC 是一个过渡标准，后来结合 ITSEC 发展为联合公共准则。

5. 联合通用准则(CC)

该标准的目的是把已有的安全准则结合成一个统一的标准。该项计划从 1993 年开始执行，1996 年推出第一版，但目前仍未付诸实施。CC 结合了 FC 及 ITSEC 的主要特征，它强调将安全的功能与保障分离，并将功能需求分为 9 类 63 族，将保障分为 7 类 29 族。

6. ISO 安全体系结构标准

在安全体系结构方面，ISO 制定了国际标准 ISO7498-2-1989《信息处理系统·开放系统互联、基本模型第 2 部分安全体系结构》。该标准为开放系统标准建立了一个框架。其任务是提供安全服务与有关机制的一般描述，确定在参考模型内部可以提供这些服务与机制的位置。

近 20 年来，人们一直在努力发展安全标准，并将安全功能与安全保障分离，制定了复杂而详细的条款。但真正实用、在实践中相对易于掌握的还是 TCSEC 及其改进版本。在现实中，安全技术人员也一直将 TCSEC 的 7 级安全划分当作默认标准。

1.4.2　ISO7498-2 安全标准

ISO7498 从体系结构的角度描述了 ISO 基本参考模型之间的安全通信必须提供的安全服务及安全机制，并说明了安全服务及其相应机制在安全体系结构中的关系，从而建立了开放互连系统的安全体系结构框架。

ISO7498-2 提供了以下 5 种可选择的安全服务。

1. 身份认证

身份认证是访问控制的基础。身份认证必须做到准确无误地将对方辨别出来，同时还应该提供双向的认证，即互相证明自己的身份。网络环境下的身份认证更加复杂，主要是要考虑到验证身份的双方一般都是通过网络交互而非直接交互，像指纹认证等手段就无法应用。同时大量的黑客随时都可能尝试向网络渗透，截获合法用户密码冒名顶替，因此必须利用高强度的密码技术来进行身份认证，比较著名的有 KERTESOS、PGP 等方法。

2. 访问控制

访问控制是控制不同用户对信息资源的访问权限，对访问控制的要求主要有以下几方面。

(1) 一致性，也就是对信息资源的控制没有二义性，各种定义之间不冲突。

(2) 统一性，对所有信息资源进行集中管理，安全政策统一贯彻。

(3) 审计功能，对所有授权有记录并可以核查。

(4) 尽可能地提供细粒度的控制。目前很多系统的访问控制实际上还是基于 UNIX 文件系统的模式，不能很好地满足安全需求。

3. 数据加密

数据加密是大家所熟知的保证安全通信的手段。由于计算机技术的发展，传统通信加密算法被不断破译，促使更高强度的加密算法问世。目前加密技术主要有两大类：一类是基于对称密钥加密的算法，也称私钥算法；另一类是基于非对称密钥的加密算法，也称公钥算法。这两种加密算法都已经达到一个很高的强度。具体到加密手段，一般分软件加密和硬件加密两种，软件加密成本低而且使用灵活，更换也方便；硬件加密效率高，本身安全性高。用户可以根据不同需要采用不同的方法。密钥管理包括密钥产生、分发、更换等，是数据保密的重要一环。目前如何实现密钥完全自动管理还有待于进一步研究。

4. 数据完整性

数据完整性是指信息在存储、传输和使用中不被篡改和泄密。显然，金融信息网络传输的信息对传输、存储和使用的完整性要求很高，需采用相应的安全措施，来保障数据的传输安全，以防被篡改或泄密。

5. 防止抵赖

接收方要对方保证自己收到的信息是发送方发出的信息而不是被中间人冒名、篡改过的信息。发送方要求对方不能否认已经收到的信息。对金融电子化系统来说，电子签名的主要目的就是防止抵赖，给仲裁提供证据。

1.4.3　BS7799(ISO17799: 2000)标准

ISO17799 于 2000 年 12 月出版，它适用于所有的组织，目前已成为强制性的安全标准。ISO17799 是一个详细的安全标准，包括安全内容的所有准则，具体由以下 10 个独立的部分组成，其中每一部分都覆盖不同的主题和区域。

(1) 信息安全方针：为信息安全提供管理方向和支持。

(2) 组织安全：建立组织内的信息安全管理体系，以便实施安全管理。

(3) 财产分类和控制：维护组织资产的适当保护系统。

(4) 人员安全：减少误操作、入侵、盗用等人为造成的风险。

(5) 物理和环境安全：防止电子商务和信息的未经许可的介入、损伤和干扰。

(6) 计算机通信和操作管理：保证通信和操作设备的正确使用和安全维护。

(7) 访问控制：控制对信息的访问。

(8) 系统开发与维护：保证在信息系统中建立安全设置。

(9) 商务持续性管理：防止商务活动中断及保护关键商务过程不受重大失误或灾难事故的影响。

(10) 符合性：避免任何违反法令、法规、合同约定及其他安全要求的行为。

1.5 网络安全组件

网络的整体安全是由安全操作系统、应用系统、防火墙、网络监控、安全扫描、信息审计、通信加密、灾难恢复、网络反病毒等多个安全组件共同组成的，每一个单独的组件只能完成其中部分功能，而不能完成全部功能。

1. 防火墙

防火墙是指在两个网络之间加强访问控制的一整套装置，是软件和硬件的组合体，通常被比喻为网络安全的大门，用来鉴别什么样的数据包可以进出企业内部网。在内部网(可信任的)和外部网(不可信任的)之间构造一个保护层。防火墙可以阻止基于 IP 包头的攻击和非信任地址的访问，但无法阻止基于数据内容的黑客攻击和病毒入侵，同时也无法控制内部网络之间的攻击行为。

2. 扫描器

扫描器是一种自动检测远程或本地主机安全性弱点的程序，通过使用扫描器可以自动发现系统的安全缺陷。扫描器可以分为主机扫描器和网络扫描器。但是，扫描器无法发现正在进行的入侵行为，而且它也可以被攻击者加以利用。

3. 防毒软件

防毒软件可以实时检测、清除各种已知病毒，具有一定的对未知病毒的预测能力，利用代码分析等手段能够检查出最新病毒。在应对网络入侵方面，它可以查杀特洛伊木马和蠕虫等病毒程序，但不能有效阻止基于网络的攻击行为。

4. 安全审计系统

安全审计系统对网络行为和主机操作提供全面详实的记录，其目的是测试安全策略是否完善，证实安全策略的一致性，方便用户分析与审查事故原因，协助攻击的分析，收集证据以用于起诉攻击者。

前 4 种安全组件对正在进行的外部入侵和网络内部攻击缺乏检测和实时响应功能。所有这些在 IDS 上得到了圆满的解决。

5. IDS

由于防火墙所暴露出来的不足和弱点，引发了人们对 IDS(入侵检测系统)技术的研究和开发。它被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。

综观上述网络安全组件的特点，可以得出结论：由于每个网络安全组件自身的限制，不可能把入侵检测和防护做到一应俱全。所以不能指望通过使用某一种网络安全产品实现绝对的安全。只有根据具体的网络环境，有机整合这些网络安全组件才能最大限度地满足用户的安全需求。