高等学校计算机及其应用系列

网络信息安全

主　编/于莉莉　闫文刚　刘　义
主　审/刘景顺

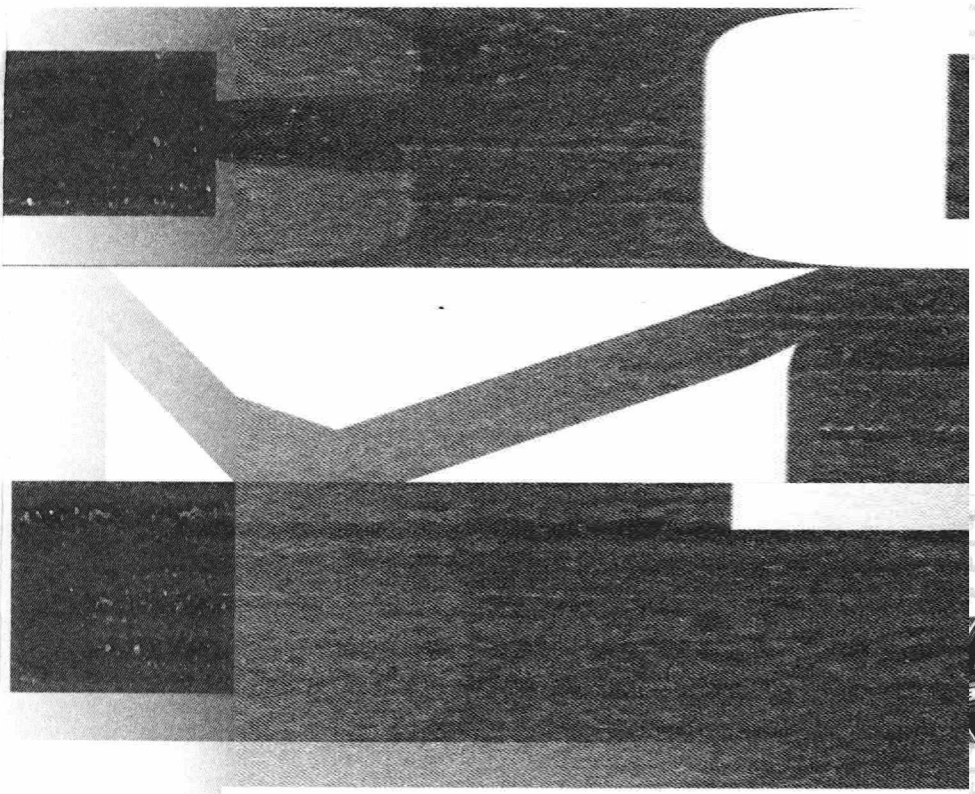
重点规划教材

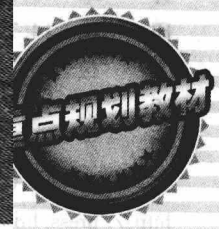
HEUP 哈尔滨工程大学出版社
Harbin Engineering University Press

高等学校计算机及其应用系列

网络信息安全

主　编/于莉莉　闫文刚　刘　义
副主编/孟凡波　王　安　丁晓迪
主　审/刘景顺





HEUP 哈尔滨工程大学出版社
Harbin Engineering University Press

内容简介

本书是一本关于网络信息安全的专业书籍，比较全面地介绍了信息安全的基础理论和技术原理。由网络安全的基本概念、网络信息安全模型和标准、网络安全协议、密码技术、防火墙技术、入侵检测技术、数据库系统安全技术、VPN技术、入侵检测技术、无线网络安全、网络信息对抗与入侵技术、网络信息安全测试工具及其应用技术组成。

本书取材广泛，内容系统，理论与实际相结合，不仅可作为高等院校计算机专业本科教材，也适合广大读者自学使用。

图书在版编目(CIP)数据

网络信息安全／于莉莉，阎文刚，刘义主编. —哈尔滨：哈尔滨工程大学出版社，2011.3
ISBN 978-7-5661-0041-2

Ⅰ. ①网… Ⅱ. ①于… ②阎… ③刘… Ⅲ. ①计算机网络-安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 020094 号

出版发行 哈尔滨工程大学出版社
社　　址 哈尔滨市南岗区东大直街 124 号
邮政编码 150001
发行电话 0451-82519328
传　　真 0451-82519699
经　　销 新华书店
印　　刷 黑龙江省教育厅印刷厂
开　　本 787mm×1 092mm 1/16
印　　张 14.75
字　　数 351 千字
版　　次 2011 年 3 月第 1 版
印　　次 2011 年 3 月第 1 次印刷
定　　价 28.00 元
http://press.hrbeu.edu.cn
E-mail:heupress@hrbeu.edu.cn

前　言

伴随着网络技术的高速发展，网络与信息系统的基础性、全局性作用不断增强，全社会对计算机网络的依赖越来越大。网络系统如果遭到破坏，不仅会带来经济损失，还会引起社会混乱。网络安全已经成为国家安全的重要组成部分。加快网络安全保障体系的建设、培养高素质的网络安全人才队伍，已经成为我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务。

网络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，不因偶然的或者恶意的原因而遭受到更改、破坏或泄露，保证系统连续可靠地运行，网络服务不中断。网络安全是一门涉及计算机科学、网络技术、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综合性学科。本书共分13章，比较全面地论述了信息安全的基础理论和技术原理。分别介绍了网络安全的基本概念、网络信息安全模型和标准、网络安全协议、密码技术、防火墙技术、入侵检测技术、数据库系统安全技术、数字签名与认证技术、VPN技术、入侵检测技术、无线网络安全、网络信息对抗与入侵技术、网络信息安全测试工具及其应用技术等。

本书由佳木斯大学的于莉莉、闫文刚、刘义任主编，孟凡波、王安、丁晓迪任副主编。由于莉莉编写第4章、第6章、第13章；闫文刚编写第1章、第8章；刘义编写第9章、第10章、第11章；孟凡波编写第2章、第5章、第7章；王安编写第3章；丁晓迪编写第12章。

本书在编写过程中参考并引用了国内外一些专家学者的改著，同时得到了刘景顺教授的指导和审阅，在此表示衷心的感谢，同时也感谢佳木斯大学国际学院广大师生的大力支持。官祥龙同学在本书的编写过程中付出了宝贵的时间，在此一并致谢。由于编者水平有限，书中定有不当之处，望广大读者提出意见和建议。

编　者

2011年1月

目　录

第 1 章　网络安全概论 …… 1

1.1　网络安全概念 …… 1
1.2　网络安全所产生的威胁 …… 2
1.3　网络安全组件 …… 6
1.4　安全策略的制定与实施 …… 7
1.5　计算机网络发展趋势 …… 8
1.6　本章小结 …… 8

第 2 章　网络信息安全模型和标准 …… 9

2.1　OSI 概述 …… 9
2.2　协议安全分析 …… 17
2.3　网络安全标准 …… 18
2.4　本章小结 …… 21

第 3 章　网络安全协议 …… 22

3.1　Internet 常见协议介绍 …… 22
3.2　TCP/IP 协议 …… 26
3.3　网络层协议报头结构 …… 28
3.4　传输层协议报头结构 …… 31
3.5　TCP 会话安全 …… 35
3.4　本章小结 …… 35

第 4 章　密码技术 …… 36

4.1　密码技术概述 …… 36
4.2　IDEA 加密算法 …… 37
4.3　高级加密标准 AES …… 49
4.4　分组密码的工作模式 …… 65
4.5　本章小结 …… 68

第 5 章　防火墙技术 …… 69

5.1　防火墙功能及分类 …… 70
5.2　防火墙结构 …… 74
5.3　Linux 中的防火墙 …… 76
5.4　本章小结 …… 80

第 6 章　入侵检测系统 …… 81

6.1　入侵检测系统概述 …… 81

6.2 入侵检测系统结构 …… 82
6.3 入侵检测系统分类 …… 82
6.4 入侵检测系统工具与产品介绍 …… 85
6.5 入侵检测系统的发展及研究方向 …… 95
6.6 提高 IDS 的性能 …… 98
6.7 数据采集 …… 106
6.8 本章小结 …… 113
第 7 章 数据库安全系统 …… 114
7.1 数据库安全概述 …… 114
7.2 ACCESS 数据库的安全配置 …… 115
7.3 MySQL 数据库安全配置 …… 118
7.4 Sql server 数据库安全配置 …… 122
7.5 oracle 数据库安全配置 …… 125
7.6 本章小结 …… 129
第 8 章 数字签名与认证技术 …… 130
8.1 引言 …… 130
8.2 PKI 的信任模型和交叉认证 …… 133
8.3 双证书和 SSL/TLS 安全 …… 149
8.4 ECIA:一个高效 CRL 发布机制 …… 153
8.5 无线 PKI(WPKI) …… 155
8.6 本章小结 …… 163
第 9 章 VPN 技术 …… 164
9.1 VPN 的基本概念 …… 164
9.2 VPN 的系统特性 …… 164
9.3 VPN 的原理与协议 …… 166
9.4 构建 VPN 的解决方案与相关设备 …… 180
9.5 本章小结 …… 182
第 10 章 计算机病毒 …… 183
10.1 病毒的定义 …… 183
10.2 计算机病毒简史 …… 183
10.3 计算机病毒的发展及分类 …… 183
10.4 计算机病毒原理 …… 188
10.5 计算机病毒的检测及清除 …… 193
10.6 本章小结 …… 195
第 11 章 无线网络安全 …… 196
11.1 WLAN 的应用现状 …… 196

11.2 WLAN 面临的安全问题 …… 196
11.3 WLAN 业界的安全技术 …… 197
11.4 企业/校园无线网安全解决方案 …… 202
11.5 本章小结 …… 203
第 12 章 网络信息对抗及其相关技术 …… 204
12.1 国内外信息对抗理论与技术研究现状及发展趋势 …… 204
12.2 常用攻击方法及原理 …… 205
12.3 扫描程序 …… 209
12.4 网络攻击的趋势 …… 213
12.5 口令安全 …… 215
12.6 本章小结 …… 217
第 13 章 网络信息安全测试工具及其应用 …… 218
13.1 如何评估和使用测试工具 …… 218
13.2 评估测试工具性能的标准 …… 219
13.3 使用渗透测试工具的四个注意事项 …… 219
13.4 常见网络安全测试工具 …… 220
13.5 本章小结 …… 224
参考文献 …… 225

第1章　网络安全概论

21世纪是知识经济时代，信息化、网络化已成为现代社会的一个重要特征。在这个新时代里，网络信息与我们息息相关。网络信息安全是一个涉及网络技术、通信技术、密码技术、信息安全技术、计算机科学、应用数学、信息论等多种学科的边缘性综合学科。网络信息安全在国民经济建设、社会发展、国防和科学研究等领域的作用日益重要，是国家安全的重要基础。实际上，网络的快速普及与发展、用户端软件多媒体化、协同计算、资源共享与开放、远程管理化、电子商务、金融电子化等已成为网络时代必不可少的产物。

网络信息安全至关重要，没有网络信息的安全就谈不上网络信息的应用。当今，计算机互联网络迅速发展和广泛应用，打破了传统的时间与空间的局限性，极大地改变了人们的工作方式和生活方式，成了经济和社会发展的最活跃因素。然而，任何事物的发展都具有两面性，计算机互联网络国际化、社会化、开放化、个性化的特点，使得它在向人们提供网络信息共享、资源共享和技术共享的同时，也带来了不安全的隐患。对互联网络的非法侵入或任何的故意破坏，都会轻而易举地改变互联网络上的应用系统或导致网络瘫痪，给网络用户在军事、经济、政治上带来无法弥补的巨大损失。因此，很早就有人提出了“信息战”的概念，并将信息武器列为继原子武器、生物武器和化学武器之后的第四大武器。

网络信息的泄漏、篡改、假冒和重传，黑客入侵，非法访问，计算机犯罪，计算机病毒传播等对网络信息安会已构成重大威胁。如果这些问题不解决，国家安全就会受到威胁，电子政务、电子商务、网络银行、网络科技、远程教育和远程医疗等都将无法正常开展，个人隐私也得不到保障。因此，网络信息安全是我们亟待解决的问题。

1.1　网络安全概念

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，它可以来自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)自由性意味着网络最初对用户的使用并没有任何的技术约束，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。如何使内部机密信息不受黑客和间谍的窃取，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。

1.1.1 网络安全的概念

网络安全包括五个属性：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，凡是涉及到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。

1.1.2 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。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网络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是矛盾的，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是非授权访问,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。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. 泄漏或丢失信息

泄漏或丢失信息指敏感数据被有意泄漏出去或丢失,通常包括:信息在传输中丢失或泄漏(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

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

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,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,即可以制订"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 公司的 Solaris 中也引入公共密钥结构(PKI)、基于 IP Security 的虚拟私有网络(VPN)和内置的防火墙。这些措施都极大地改善了主机的网络安全状况。不过它们都是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验证。

(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 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。

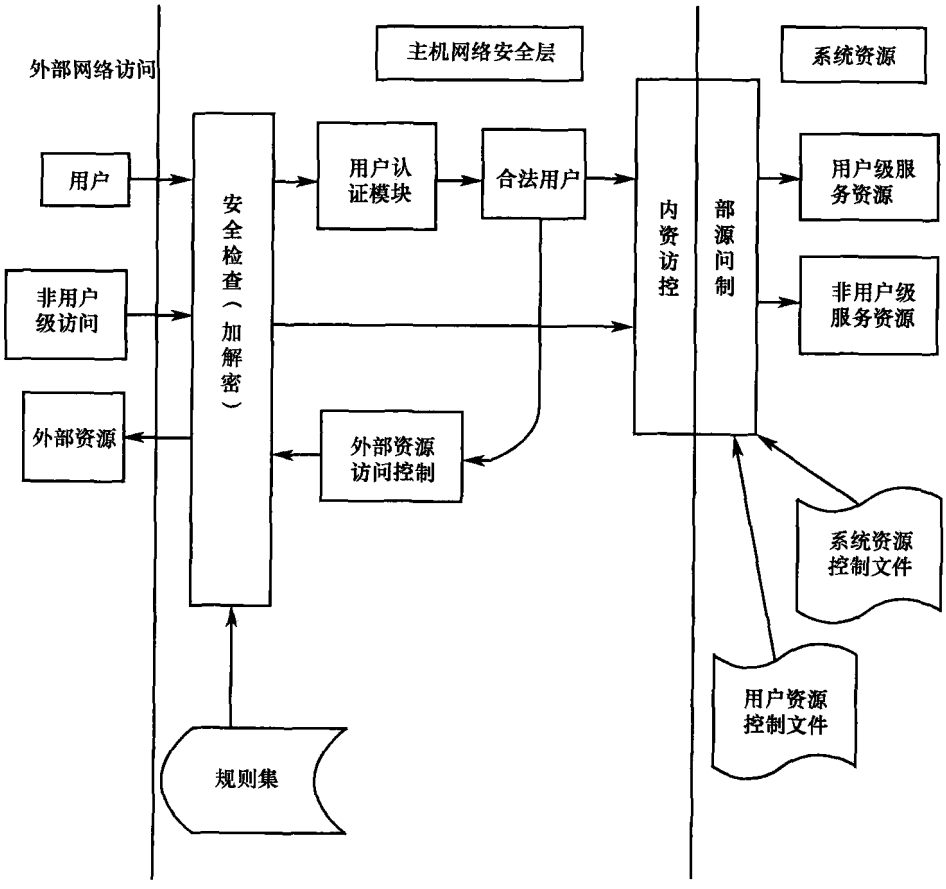


图 1.1　主机网络安全系统结构模型

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 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、信息审查、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. 安全审查系统

安全审查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 上可以得到圆满的解决。

5. IDS

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。IDS 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，我们可以得出这样一个结论：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。

1.4　安全策略的制定与实施

安全的基石是社会法律、法规与手段，即通过建立与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。先进的安全技术是信息安全的根本保障，用户可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。各网络使用机构、企业和单位应建立相应的信息安全管理办法，加强内部管理，建立审查和跟踪体系，提高整体信息安全意识。

安全策略是指在某个特定的环境中，为达到一定级别的安全保护需求所必须遵守的诸多规则和条例。安全策略包括三个重要组成部分：安全立法、安全管理、安全技术。安全立法是第一层，有关网络安全的法律法规可以分为社会规范和技术规范；安全管理是第二层，主要指一般的行政管理措施；安全技术是第三层，它是网络安全的物质技术基础。

网络安全策略可以从以下几方面制定和实施。

(1)重要的商务信息和软件的备份应当存储在受保护、限制访问且距离源地点足够远的地方，这样备份数据就能逃脱本地的灾害。因此需要将关键的生产数据安全地存储在相应的位置。

这一策略要求将最新的备份介质存放在距离资料地较远的地方。同样，规定只有被授权的人才有权限访问存放在远程的备份文件。在某些情况下，为了确保只有被授权的人可以访问备份文件中的信息，需要对备份文件进行加密。

(2)需要给网络环境中的系统软件打上最新的补丁。各公司的联网系统应当具备一套可供全体员工使用的方法，以方便定期检查最新的系统软件补丁、漏洞修复程序和升级版本。当需要时，此方法必须能够为连接 Internet 和其他公用网络的计算机迅速安装这些新的补丁、漏洞修复程序和升级版本。

此策略的目的是确保系统管理员和其他用户快速更新、升级连接 Internet 等公用网的计算机系统软件。如果系统软件更新不及时，入侵者可能运用漏洞识别软件判断系统是否存在已知漏洞。这意味着恐怖分子、黑客、工业间谍和其他图谋不轨的人使用计算机识别可以进行破坏的系统。如果与网络连接的系统没有安装带有安全性错误的修复程序、安全补丁和更新的软件，短时间内这些系统的漏洞就会被识别并被渗透。在未来几年，借助一些分布在系统中的自动执行软件，这一方法的执行将逐渐不需要人工干预。

(3)安装入侵检测系统并实施监视。为了让企业能快速响应攻击，所有与 Internet 连接的、设置多用户的计算机必须运行一套信息安全部门认可的入侵检测系统。

入侵检测系统不同于漏洞识别系统，前者在防御措施遭受破坏时向工作人员发出警报，后者是告诉工作人员有哪些漏洞需要修复以支撑防御系统。通常入侵检测系统会通过一个网络管理系统或其他通知手段实时向负责人员报警并采取应对措施。例如，计算机紧急响应小组

(CERT)的成员可根据入侵检测系统的 BP 机报警采取行动。这一策略的目的是确保内部网络外围设备上的所有系统都具备适当的入侵检测系统。

(4)启动最小级别的系统事件日志。计算机系统在处理一些敏感、有价值或关键的信息时必须可靠地记录下重要的、与安全有关的事件。与安全有关的事件包括:企业猜测密码、使用未经授权的权限、修改应用软件以及系统软件。

此策略可被所有生产系统采用,而不只是那些需要处理敏感的价值高的或关键信息的系统。不管怎样,企业实施此策略可确保此类日志被记录下来,并在一段时期内保存在一个安全的地方。在许多情况下会运用哈希算法或数字签名来判断系统日志记录之后是否被改变过。

1.5 计算机网络发展趋势

第一代:Internet,实现了计算机硬件的连通;

第二代:Web,实现了网页的连通;

第三代:Grid,试图实现 Internet 上所有资源的全面连通,包括计算资源、存储资源、通信资源、软件资源、信息资源和知识资源等。

网格的定义为:用高速的计算机网络集成超级计算机、大型数据库、数据存储设备、先进的显示设备和科学仪器(电子显微镜、雷达阵列、粒子加速器、天文望远镜等),形成了网络虚拟超级计算机或称之为超级计算机 (Meta Computer),从而有可能构造各种网格(Grid)。网格的种类包括计算网格、数据网格、对象网格、知识网格、服务网格、信息网格和各种代理网格等。

1.6 本章小结

本章讲述了网络安全的定义和基本属性,包括机密性、完整性、可用性、可控性和可审查性;简要介绍了网络威胁的几种类型;介绍了网络安全基本组件,网络安全策略的构成及计算机网络发展趋势。

第2章　网络信息安全模型和标准

2.1　OSI概述

2.1.1　ISO－OSI模型

计算机网络是计算机技术和通信技术相结合的产物。自从1946年第一台电子计算机ENIVAC问世以来，由于计算机网络技术和软件技术的不断发展，人们使用计算机的方式有了根本的改变，由多人通过终端使用一台计算机变为现在一人通过计算机网络使用多台计算机。

计算机网络是由多个独立的计算机通过通信线路和通信设备互连起来的系统，以实现彼此交换信息和共享资源的目的。

计算机网络具有以下功能：

(1)数据通信。网络系统中各相连的计算机能够相互传送数据信息，使相距很远的用户之间能够直接交换数据。

(2)资源共享。网络中的软件、硬件资源，如外部设备、文件系统和数据等可被多个用户所共享。

(3)进行并行和分布式处理。在计算机网络中，用户可根据问题的性质和要求选择网内最合适的资源来处理。对于综合性的大问题，可以采用合适的算法，将任务分散到不同的计算机上进行分布和并行处理。

(4)能提高可靠性。由于控制、数据、软件和硬件的分散性(不存在集中环节)，资源冗余以及结构上可动态重组提高了可靠性。

(5)可扩充性好。随着用户需求的增长，包括性能方面和功能方面的增长，只需增加新节点数，而不必替换整个系统。可扩充性可以避免较大的初始投资，另外使用多个微小型机代替一个大型主机，可以获得很好的性能价格比。

随着计算机网络的日益普及，它已经应用在各个领域中，我们在日常生活中常见的采用计算机的服务项目，如银行的提款机、销售点的终端、支票和发票的核实等都依赖于计算机网络。下面是计算机网络应用的一些典型领域。

服务业：通过计算机网络系统进行酒店和航空公司的在线订票、订房，远程购物等。

金融服务业：现在的金融服务都依赖于计算机网络，如外汇汇兑、投资服务、电子资金转账服务等。

企业管理：通过网络信息系统对企业生产、销售、财务等方面进行管理。

制造业：计算机网络在制造业的多个方面包括制造过程本身，都有应用。如计算机辅助设计(CAD)和计算机辅助制造(CAM)，这两种业务都允许同时有多个用户在同一个项目上工作。

电子信息传递:最广泛的应用如电子邮件。

信息服务:如电子公告板和 WWW 站点。

实时信息传递:如音频和视频会议,视频点播,远程教学等。

总之,计算机网络的应用已经深入到社会和经济生活的各个方面。随着计算机网络应用的不断推广和普及,网络软件的设计和开发越来越流行,目前绝大多数系统软件(如 UNIX, Linux, Windows 系列等操作系统)和应用软件都是网络版的。掌握网络安全的原理和方法对于设计和开发网络应用程序是十分重要的。

计算机网络要完成数据处理和数据通信两大功能。相应地,网络结构可以分成两大部分:负责数据处理的计算机和终端;负责数据通信的通信控制处理机 CPP(Communication Control Processor)、通信线路。计算机网络从逻辑功能上可以分为两个子网:资源子网和通信子网,其结构如图 2.1 所示。

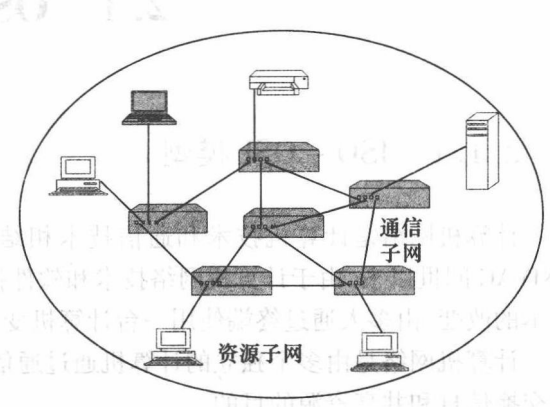


图 2.1 资源子网和通信子网

计算机网络由若干个相互连接的节点组成,在这些节点之间要不断地进行数据交换。要进行正确的数据传输,每个节点就必须遵守一些事先约定好的规则,这些规则就是网络协议。网络协议是在主机与主机之间、主机与通信子网之间或子网中各通信节点之间的通信中使用的,是通信双方必须遵守的,事先约定好的规则、标准或约定。

一个网络协议主要由以下三个要素组成。

(1)语法:即数据与控制信息的结构或格式。如数据格式、信号电平等规定。

(2)语义:即需要发出何种控制信息,完成何种动作,以及做出何种应答。包括用于调整和进行差错处理的控制信息。

(3)时序(同步):即事件实现顺序的详细说明,包括速度匹配和顺序。

为了减少网络设计的复杂性,大多数网络在设计上都是分成不同功能的多个层次的。图 2.2 是国际标准化组织 ISO - OSI 网络参考模型,图 2.3 以报文传输的形式演示了图 2.2 中的通信过程。

各层协议是通信双方在通信过程中的约定,规定有关部件在通信过程中的操作以保证正确地进行通信。各层的主要功能如下。

(1)物理层:规定在一个节点内如何把计算机连接到通信介质上,规定了机械的、电气的功能;该层负责建立、保持和拆除物理链路;规定如何在此链路上传送原始比特流;比特如何编码,使用的电平、极性,连接插头插座的插脚如何分配等。所以在物理层数据的传送单位是比特(bit)。

(2)数据链路层:它把相邻两个节点间不可靠的物理链路变成可靠的无差错的逻辑链路,包括把原始比特流分帧、排序、设置检错、确认、重发、流控等功能;数据链路层传输信息的单位是帧(frame),每帧包括一定数量的数据和一些必要的控制信息,在每帧的控制信息中,包括同步信息、地址信息、差错控制信息、流量控制信息等;同物理层相似,数据链路层负责建立、维护