普通高等教育"十一五"国家级规划教材

高职高专计算机系列规划教材

网络安全技术

（第2版）

钟乐海　王朝斌　李艳梅　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

普通高等教育“十一五”国家级规划教材

高职高专计算机系列规划教材

网络安全技术（第2版）

钟乐海　王朝斌　李艳梅　编著

電子工業出版社
Publishing House of Electronics Industry
北京・BEIJING

内 容 简 介

本书全面系统地讲解了计算机网络安全的基础知识和基本技术，包括计算机网络安全的基本定义，计算机安全等级，计算机访问控制，网络协议，网络操作系统，数据加密技术和电子商务安全，计算机病毒和防火墙技术等网络安全知识与实现方法。本书内容新颖，各章重点、难点突出，原理、技术和方法的阐述融于实例之中。书中安排有习题、实验，使于教学和自学。

图书在版编目（CIP）数据

网络安全技术 / 钟乐海编著. 2 版. —北京：电子工业出版社，2007.2
（高职高专计算机系列规划教材）
普通高等教育“十一五”国家级规划教材
ISBN 7-121-02863-8

Ⅰ. 网… Ⅱ. 钟… 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（2006）第 129178 号

责任编辑：吕 迈（lumai@phei.com.cn）
印 刷：
装 订：北京市铁成印刷厂
出版发行：电子工业出版社
北京市海淀区万寿路 173 信箱 邮编 100036
开 本：787×1 092 1/16 印张：13 字数：333 千字
印 次：2007 年 2 月第 1 次印刷
印 数：4 000 册 定价：17.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系电话：（010）68279077；邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前　言

随着计算机网络技术的广泛应用和飞速发展，计算机安全问题也随之日益突出，计算机病毒扩散、网络黑客攻击、计算机网络犯罪等违法事件的数量迅速增长，安全问题已成为人们普遍关注的问题。

随着网络的开放性、共享性、互联程度的扩大和 Internet/Intranet 的发展，对整个社会带来了巨大的推动与冲击，同时也给我们带来了许多挑战。Internet/Intranet 信息安全是一项综合的系统工程，需要大家在网络安全技术的研究和应用领域做长期的、不懈的努力。事实上，信息资源共享和信息安全历来是一对矛盾。近年来，随着 Internet 的飞速发展，计算机网络信息资源共享得到了进一步加强，随之而来的安全问题也日益突出。随着网络上电子商务、电子现金、数字货币、网络银行等业务的兴起以及各种专用网（如金融网）的建设，网络与信息系统的安全与保密问题显得越来越重要。

伴随着信息产业发展而产生的互联网和网络信息的安全问题，已成为各国政府有关部门、各大行业和企事业领导人关注的热点问题。目前，全世界每年由于信息系统的脆弱性而导致的经济损失逐年上升，安全问题日益严重。

本书共 8 章。第 1 章介绍网络安全概要，包括网络信息安全概况、计算机网络安全的定义、网络安全基本概念、网络安全威胁和黑客与网络安全等；第 2 章介绍计算机系统的安全及访问控制，包括计算机系统安全级别、系统访问控制、文件和资源的访问控制、选择性访问控制和强制性访问控制等；第 3 章介绍系统安全性规划及管理，包括风险分析和评估、制定安全策略、日常的系统维护和网络安全教育等；第 4 章介绍计算机网络通信协议与安全，包括 TCP/IP 协议、网络通信不安全的原因分析、网络协议存在的安全问题、IPv6 及安全问题、WWW 的安全和 Modem 的安全等；第 5 章介绍 Windows 2000 系统的安全问题，包括 Windows 2000 系统及其安全、Windows 2000 系统的安全漏洞和解决办法、Linux 系统安全性、Windows XP 系统安全性和 Windows 2000 的安全性评估和监测工具等；第 6 章介绍计算机病毒防范技术，包括计算机病毒简介、计算机病毒的种类、计算机病毒的工作原理、计算机病毒实例、计算机病毒的预防、计算机病毒的检测和计算机病毒的清除等；第 7 章介绍防火墙技术，包括防火墙概述、防火墙的体系结构、防火墙的安全标准、实用防火墙技术、防火墙产品、第四代防火墙和防火墙技术展望等；第 8 章介绍电子商务与电子政务的安全性，包括电子商务的基本概念、电子商务的安全性要求、电子支付系统的安全性、电子现金系统和电子政务及安全等。为了配合教学，本书在每章后都附有思考题、习题和实验，以巩固学习效果。

本书由西华师范大学计算机学院钟乐海教授编写第 1 章、第 2 章、第 3 章、第 4 章和附录 A；西华师范大学计算机学院教师王朝斌编写第 5 章、第 6 章和第 7 章；西华师范大学计算机学院教师李艳梅编写第 8 章。全书由钟乐海教授统稿、定稿。

在本书的编纂过程中，桂林电子科技大学网络中心王任主勇博士提供了宝贵的资料并提出了宝贵的意见和建议，同时也得到了西华师范大学教务处、科研处的支持和帮助，得到了西华师范大学计算机学院全体同仁的关心和帮助，得到了编著者家属的支持。本书大纲得

到中国计算机学会高职高专教育学组的审定，高职高专计算机教材编审委员会给予了指导与帮助，在此对所有关心和支持本书编写和出版的人表示衷心的感谢！

作者曾以善意的眼光寻找他人著作中的缺陷与不足，作者也真诚期待同仁的批评指正，衷心期待读者提供使用本书的宝贵意见。由于作者水平有限，时间仓促，书中难免会有错误和不妥之处，恳请读者批评指正。作者信箱：lehaizhong@163.com。

作　者

2006 年 6 月于西华师范大学

目　录

第 1 章　网络安全概要

1.1　网络信息安全概况

Internet 已遍及世界 180 多个国家，容纳了 60 多万个网络，为 1 亿多用户提供了多样化的网络与信息服务。在 Internet 上，除了原来的电子邮件、新闻论坛等文本信息的交流与传播之外，网上电话、网上传真、静态图像及视频等通信技术都在不断地发展与完善。在信息化社会中，网络信息系统将在政治、军事、金融、商业、交通、电信、文教等方面发挥越来越大的作用。社会对网络信息系统的依赖也日益增强。另一方面，这些网络信息系统都依靠计算机网络接收和处理信息，实现其相互间的联系和对目标的管理、控制。以网络方式获得信息和交流信息已成为现代信息社会的一个重要特征。网络正在逐步改变人们的工作方式和生活方式，成为当今社会发展的一个主题。

随着网络的开放性、共享性和互联程度的扩大，特别是 Internet 的出现，网络的重要性和对社会的影响也越来越大。随着网络上电子商务、电子现金、数字货币和网络银行等业务的兴起以及各种专用网（如金融网）的建设，网络与信息系统的安全与保密问题显得越来越重要。

伴随着信息产业发展而产生的 Internet 和网络信息的安全问题，也已成为各国政府有关部门、各大行业和企事业领导人关注的热点问题。目前，全世界每年由于信息系统的脆弱性而导致的经济损失逐年上升，安全问题日益严重。面对这种现实，各国政府有关部门和企业非常重视网络的安全问题。

国际标准化机构在信息系统安全方面从事了大量的工作，1985 年，DoD 5200.28-STD，即可信计算机系统评测标准（TCSEC）（美国国防部橙皮书，以下简称 DoD 85 评测标准），为计算机安全产品的评测提供了测试方法，指导信息安全产品的制造和应用。1987 年，美国国家计算机安全中心（NCSC）为 TCSEC 橙皮书提出可依赖网络解释，通常被称做红皮书。1991 年，美国国家计算机安全中心为 TCSEC 橙皮书提出可依赖数据库管理系统解释（TDI）。

世界上 IT 业界的各大公司，特别是一些大的跨国公司在信息和信息系统安全方面推出了相应的技术和产品。如 HP 公司 1996 年 3 月领导发布的 X/Open Security Branding 计划，推出了 ICF（国际密码架构）战略。DEC 公司推出安全级别为 C2 级的操作系统 Digital UNIX 和 OpenVMS，推出的 B1 级/CMW 级的操作系统 SEVMS 和 Digital MLS+。Sun 公司也有高安全级（B1 级）的 Solaris 操作系统。Oracle 公司的安全数据库 Trusted Oracle，是 B2 产品，在美国是用于军方的产品。Sybase 公司的安全数据库是 Secure SQL Server，其安全级别为 B1 级，也是美国军方使用的产品，曾在海湾战争中使用过。

还有一些专门从事信息系统安全工作的公司，例如 RSA 公司，是以色列在美国注册的安全技术公司，面向多平台，提供各类安全软、硬件系统。ISS 公司，是一个做网络与服务器安全系统的公司，1996 年 ISS 的一种安全产品获美国大奖及最佳创意奖，它是一个网络

安全的测试软件，非常受用户欢迎。其产品有 Web Security Scanner，System Security Scanner，RealSecure，Firewall Scanner，Internet Scanner，Intranet Scanner 等产品，目前 ISS 公司还在安全测试和监控领域处在领导地位。

在国内，信息系统安全方面的建设可以追溯到“七五”与“八五”期间，我国在信息加密、解密、密钥芯片、密钥管理等方面有所研究，到了 20 世纪 90 年代，在信息安全的传统思路上，中国科学院成立了信息安全技术工程研究中心，主要从事加密与解密的研究工作。从“七五”开始到“九五”期间，信息产业部 15 所在网络安全方面进行了科研工作，自主开发了 B1 级安全级别的 UNIX 操作系统。

近年来，我国有关部门逐步重视网络信息安全问题，并建立了相应的机构，发布了有关的法规，以加强对网络信息安全的管理。2000 年 1 月，国家保密局发布的《计算机信息系统国际联网保密管理规定》已开始实施。2000 年 3 月，中国国家信息安全测评认证中心计算机测评中心宣告成立。2000 年 4 月，公安部发布了《计算机病毒防治管理办法》。2000 年 7 月，我国第一个国家信息安全产业基地在四川省成都市高新技术产业开发区奠基。2000 年 10 月，信息产业部成立了网络安全应急协调小组，国家计算机网络与信息安全管理工作办公室主办了“计算机网络应急工作企业级研讨会”。这一切都反映出我国对计算机网络与信息安全的高度重视；表明了我国努力推动信息安全产业发展，提高我国信息安全技术水平的决心。

近两年安全软件的市场一直保持着较大幅度的增长率，1999 年国内安全软件的销售额达到 4.55 亿元，与 1998 年相比市场增长率为 33.8%，其增长速度明显高于软件整体市场的增长率。2000 年下半年起，安全产品市场快速启动。据统计，2000 年，我国网络安全软件市场保持了良好的增长态势，销售总额达 7.1 亿元，比 1999 年增长 56%，远远高于软件总体市场 30.7%的增长率。从产品结构看，杀病毒软件和防火墙是 2000 年网络安全软件市场中主要的安全产品，二者占据了网络安全软件市场份额的 70.4%，而安全认证、信息加密等产品的市场份额相对较小，但随着今后各行业信息化建设对于网络安全整体解决方案需求的增加，将会有较大的增长。据统计，2001 年，网络安全产品市场销售额达到了 11 亿元左右。

目前，在网络安全产品的研制和开发方面，一些知名的 IT 公司开始研究和开发安全产品，例如东软集团、联想、高阳信安、紫光、中科网威、天网、天融信、实达、海信等都有了自己开发的防火墙。国外网络安全厂商也纷纷涌入我国，并采取各种手段，以扩大在我国的市场份额。

与国内产品相比，国外防火墙产品优势在于技术成熟、知名度高，因此在高端防火墙市场中，国外产品始终占据优势。金融、电信、大型 ISP 等，除特殊部门外的大部分行业用户一般都选用了国外防火墙产品。但近年来国内防火墙厂商也有着相当大的发展机会，并在市场上异军突起，形成了自己的品牌。

在网络入侵检测领域，国外早已开展了早期预警系统及入侵检测技术的研究，在一些重要的政治、军事和经济网络上，对非法入侵实施监控，同时，还可以动态地调整防火墙的防护策略，使得防火墙成为一个动态的智能的防护体系。这些系统在保障网络安全、尽早发现入侵攻击迹象、分析入侵攻击的技术手段方面发挥着重要的作用。我国在这些技术上起步相对较晚，1999 年从事入侵检测的厂家还不多，随着 2000 年网络安全事件的风起云涌，出现了很多开发扫描器和入侵检测软件的公司。目前国外厂商在市场上占据了较大优势。

从网络经济发展对网络安全产品带来的需求看，防火墙、杀病毒、信息加密、入侵检

测、安全认证等产品将具有巨大的市场前景，其中防火墙和高端的杀毒软件将占据市场的主要份额。同时，现有的对网络进行被动防守的做法，将逐渐向网络主动检测和防御的技术方向发展。入侵监测系统则是适应这种发展趋势的一种主动的网络安全防护措施，因此预计其需求量将呈快速增长趋势。

近年来，我国还出现了一些专门做信息安全服务的厂商，我国网络安全产品市场已进入激烈的竞争阶段，各厂商竞争的主要手段已覆盖了产品、技术、价格、渠道、服务等各个方面，其目的都是为了将产品从单一扩展到全面，这已经成了网络安全厂商谋求长期发展的一种重要策略，信息安全产品的产业化已经有了一个良好的开端。

1.2 什么是计算机网络安全

1.2.1 计算机网络安全的内涵

计算机网络安全主要是指计算机及其网络系统资源免受破坏、替换、盗窃和丢失，这些资源包括计算机及其网络设备、存储介质、通信介质、软件和计算机信息等。计算机网络安全包括广泛的策略和解决方案，主要包括如下 8 个方面。

1．访问控制

访问控制也称为授权，它是对人们访问计算机系统进行控制，只允许合法的用户使用计算机系统资源，而把非法用户拒之门外，这就像守在大楼门口的门卫一样，对进出大楼的人员进行安全检查。通过对用户和组授权，访问控制表（Access Control List，ACL）允许配置整个门户网站内网络资源的访问权。在用户被授权访问资源前，必须成功通过认证。除了要求成功认证，授权要独立于应用程序服务器或任何定制认证代理服务器。

2．选择性访问控制

选择性访问控制（Discretionary Access Controls，DAC）用来决定用户是否有权访问数据的权限，对不同的合法用户授予不同的权力，使他们有不同的计算机系统资源的访问权限，如一个非正式用户就不能访问系统的关键数据和敏感数据，而系统的拥有者，即系统管理员对系统具有全面的控制权限。

3．计算机病毒和计算机“野生动物”

计算机病毒（Computer Virus）在《中华人民共和国计算机信息系统安全保护条例》中被明确定义为“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或者破坏数据，影响计算机使用并且能够自我拷贝的一组计算机指令或者程序代码”。计算机“野生动物”也称为寄生型病毒，是指一些特殊类型的破坏性程序，如蠕虫、特洛伊木马等，计算机病毒和计算机“野生动物”对计算机系统具有很大的破坏性，这也是计算机系统安全长期要面对的问题。

4．加密

信息的保密性是信息安全的一个重要方面，加密是实现信息保密性的一种重要手段。加密就是为隐藏信息、防止对信息篡改或防止非法使用信息而转换数据的功能或方法。它是将数据信息转为一种不易解读的模式来保护信息，除非有解密密钥才能阅读信息，这可以保

证只有经过授权的人才能阅读该信息。加密技术是信息的主要安全保密措施，是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）。加密技术包括算法和密钥。算法是将普通的文本（或者可以理解的信息）与一串数字（密钥）的结合，产生不可理解的密文的步骤，密钥是用来对数据进行编码和解码的一种算法。在安全保密中，可通过适当的密钥加密技术和管理机制来保证网络的信息通信安全。

5．系统计划和管理

系统计划和管理就是计划、组织和管理计算机系统设备，并根据系统和用户要求制定安全策略并实施的过程。就像企业管理一样，具有十分重要的意义。

6．物理安全

物理安全就是保证计算机系统装置和设备的安全，防止非法人员进入机房对计算机系统设备进行破坏，或直接窃取机密信息。

7．生物统计学

根据生物统计学原理，用生物唯一性特征来识别用户，如指纹、视网膜和声音等特征来作为识别用户的信息。

8．网络和通信的安全

计算机网络和通信安全是计算机安全中很重要的一个部分，网络入侵、窃听等都属于这个范畴。计算机安全在现代企业中有着极其重要的地位，但它常常被人们忽略，并在灾难发生后追悔莫及。近年来，很多商业计算机网站被黑客入侵，并受到攻击和破坏，导致网站不能正常工作，网站服务被迫关闭，造成了很大的社会影响和巨大的经济损失。如一个公司的投标计划被竞争对手窃取，该公司就可能失去一次绝好的商业机会。一个企业的计算机系统遭到破坏，或自然灾害，如水灾、火灾等，企业财务数据被损坏，如果该企业对数据没有很好的保护手段和备份措施，这可能引起企业的巨大损失，甚至不能开业了。

总之，计算机安全就是一个组织机构本身的安全，保证计算机系统安全对组织有着重要的意义。

1.2.2 数据保密性

数据保密性就是保证只有授权用户可以访问数据，而限制其他人对数据的访问。数据保密性分为网络传输保密性和数据存储保密性。

就像电话可以被窃听一样，网络传输也可以被窃听，解决这个问题的办法就是对传输数据进行加密，数据加密现在已经大量应用在网络传输过程中。

数据保密性主要是通过访问控制来实现的，系统管理员把数据分类，分成敏感型数据、机密型数据、私有型数据和公用型数据，对这些数据的访问可以有不同的访问控制，如领导可以访问所有数据，部分人员可以访问敏感型数据和机密型数据，一般人员只能访问私有型数据和公用型数据。这种访问控制是不难实现的，许多操作系统都能实现，如 UNIX、Windows NT/2000/XP 等操作系统，而 Windows 98/95 和 DOS 等操作系统不具有这种功能。

保证数据安全性另一个重要的也是最容易被人们忽略的环节是人的安全意识，一个有

经验的黑客可能会收买一个职员或欺骗一个无知的职员，从而获得机密数据，这是一种常见的攻击方式，被称为社会工程（Social Engineering）。

数据保密性在国家机关、商业、军事等领域是十分重要的，如果一个商业计划、军事秘密或国家机关机密、财政机密等被泄露或被人窃取，那将会产生严重的后果或重大损失。

1.2.3 数据的完整性和真实性

完整性是指“一种未受损的状态”或“保持完整或未被分割的品质或状态”。数据的完整性的目的就是保证计算机系统上的数据和信息处于一种完整和未受损的状态，数据完整性的丧失会直接影响到数据的可用性。

影响数据完整性的因素很多，有人为的蓄意破坏和无意破坏，有计算机系统软件、硬件的失效，还有自然灾害等不可抗拒的因素，等等；但不管怎样，人们可以通过访问控制、数据备份和冗余设置等来实现和保证数据的完整性。

典型的蓄意破坏就是被解雇的职员或黑客入侵到企业的内部网络，并肆意删除一些重要文件。为了破坏一个计算机网络站点，入侵者可能会利用系统缺陷、软件缺陷或网络病毒等对网络实行攻击，并删除或篡改系统重要文件，使系统无法正常工作。这种破坏的目的很多，有的是为了显示自己的计算机水平和能力，有的是为了报复，而有的可能是一种恶作剧。

无意破坏则主要来自操作失误，比如一个对计算机系统操作不熟练的人可能会无意中删除他人的文件，这种错误对于一些安全性好的操作系统是不容易出现的，如 UNIX、Windows NT 等操作系统，在这些系统中可以对操作者的操纵严格控制，从而减少错误的发生，而在 Windows 95/98 和 DOS 这样的系统中，误操作的可能性就很大。为了防止这种错误操作对系统的影响，对于 Windows 95/98 和 DOS 系统，用户可以对一些重要文件和数据做一个备份。对于 UNIX 和 Windows NT 系统，可以为用户划分不同的目录，并限制用户的访问权限，把用户的访问权限限制在他自己的目录中，对自己的目录才有改写的权限，对其他目录无写权限等。

计算机系统硬件和软件失效也是造成数据破坏的一个重要原因，磁盘损坏就是一种典型的硬件失效，软盘是一种极易损坏的存储介质，人们经常随身携带软盘，这样很容易造成软盘的物理损坏，加上软盘质量的问题，因此，使用软盘应多做几份备份以防止软盘不能读写。硬盘是计算机系统中最常用的存储介质，几乎系统中的系统文件和数据文件都保存在硬盘上，硬盘虽然比软盘的可靠性高得多，但硬盘仍然是计算机系统易损坏的部件，对于重要的信息，如关键数据、军事信息、商业信息和财务数据等都应有保护措施，因此，硬盘的备份也是十分重要和必要的。现在很多服务器都采用硬盘阵列结构，可以通过硬盘镜像等方式提供冗余备份，以保证服务器数据信息的安全。硬件失效也可能是计算机硬件本身的问题引起的，如 1994 年 Intel 公司的 Pentium 芯片被披露存在除法错误，一时间在业界引起了轩然大波。软件失效是因为计算机系统软件或应用软件存在的漏洞而产生的错误，软件越大，功能越强大，其缺陷可能就越多。人们经常听到一些软件开发商提供一些补丁程序，而且是一个补丁接一个补丁，这就是在软件使用过程中发现了错误或漏洞，为弥补软件中的问题提供的修补程序。

自然灾害是无法预测的，如水灾、火灾等原因，破坏了通信线路，造成信息在传输过程中丢失，也可能是磁盘设备被毁坏，造成全部数据信息破坏等。这只有通过磁盘备份来恢

复系统或数据，因此，备份是非常重要的安全手段。

对于这些破坏方式，人们可以以不变应万变，最好的办法就是对系统和数据进行备份。对简单的单机系统，重要数据不多，可以采用软盘人工备份，因为软盘可靠性差，一般需要多备份几份。对于大型计算机系统或计算机网络系统，如银行交易网络系统，需要安装先进的网络自动备份系统，使系统定时或随时进行自动备份。

1.2.4 数据的可用性

数据的可用性就是要保证数据可用，保证数据可用，首先要保证数据是完整的，其次还要保证系统是正常运转的，在计算机系统或网络上不会出现严重的拥塞，以免用户请求数据时，数据不能被及时地传过来。“拒绝服务”是一种常见的恶作剧式的攻击方式，它是使服务器忙于处理一些杂乱的任务，消耗大量的处理时间，以至于服务器无暇顾及用户的数据请求，造成系统或网络处于瘫痪状态。如网络上的蠕虫病毒就是一个典型的“拒绝服务”攻击的例子，它依靠网络在网上大量拷贝并传播，占用大量的 CPU 处理时间，用户的正常数据请求不能得到处理，导致系统越来越慢，直至网络发生崩溃。

数据不可用也可能是由于软件臭虫的原因引起的，软件臭虫导致网络失效，使用户不能登录到服务器上。在某大学的开放实验室就发生过这样的事情，有一次，有人在实验室上机，突然网络发生故障，想登录的人不能登录到网络，想退出的人也不能退出网络，一时间开放实验室里乱糟糟的，后来经过检查才发现是服务器的登录软件存在软件臭虫，致使它不能处理大量用户同时登录和退出的情况。

1.3 基本概念

1.3.1 信任

信任（Trust）是指对系统的预期运作与实际相符的信心，信任的级别与预期和实际运作关联的信心级别相对应。协同运作的系统元件通过对其他元件充分的信任假设来达到这个目的。在这些假设被证实缺乏根据的情况下，就会存在漏洞，而威胁也将随之出现。

为信任关联做出评定，相当于划出一个安全的界线，从而限定了相关的安全区域。这个方法在每个结合点对信任关联进行系统的评估，对系统的可信度做出更深入的洞察解析。

保护系统的信息安全不可能是绝对的，而是多种约束条件下的折中选择。对信息防护不应是消极的，它与信息攻击相辅相成。当称一个系统是可信任的时候，应当有一个边界，以区分内部和外部，边界有物理的和逻辑的边界。无论将系统的安全界限划到什么位置，都要注意信任所引起的问题。在系统的安全界线内，必须信任系统管理员和系统用户不会滥用他们的特权，还必须信任系统放置的物理环境可以保护系统不受物理损害。

对于外界的防范，重心在于对于边界的守卫和对授权的外部人员及程序通过边界后是否超越权限的把握、限制和控制上。就时效而言，内部人员大多数在系统边界的内部一侧，当外出时，可通过公共网络对其所连接的内部网络进行授权访问，他们拥有机构所分配的岗位和工作以及在这样的岗位上需要的权限。具有职业道德和职业技能的工作人员，是由人机共同构成的 IT 系统中不可缺少的组成部分，要求内部人员对系统不允许有违规、违法的行为。

总之，一个信任系统是指该系统拥有足够的硬件和软件，以保证准许同时进行敏感和分类信息的使用。因此，信任系统被设计成准许军用和智能组织在同一台计算机上放置符合