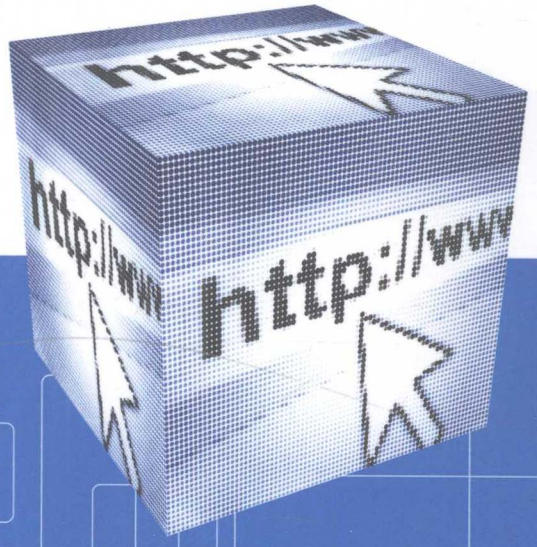
WANG LUO XIN XI AN QUAN LI LUN YU JI SHU

网络信息安全理论与技术

莫兴德　余棉水　贾青平　◎　主编

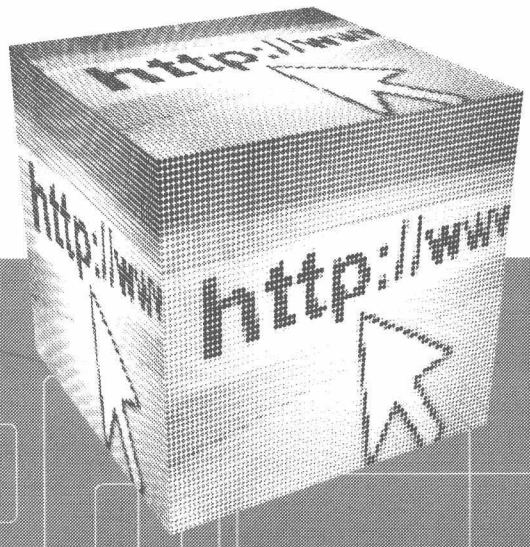


东北师范大学出版社
NORTHEAST NORMAL UNIVERSITY PRESS

WANG LUO XIN XI AN QUAN LI LUN YU JI SHU

网络信息安全理论与技术

主编 ◎ 莫兴德 余棉水 贾青平
副主编 ◎ 苏 锦 郭永利 余远波
李志芳 李晓玲



东北师范大学出版社
NORTHEAST NORMAL UNIVERSITY PRESS

图书在版编目（CIP）数据

网络信息安全理论与技术／莫兴德，余棉水，贾青平主编．—长春：东北师范大学出版社，2012.6

ISBN 978-7-5602-8387-6

Ⅰ.①网… Ⅱ.①莫… ②余… ③贾 Ⅲ.①计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2012）第 114913 号

□责任编辑：李敬东 □封面设计：韩瑞瑞

□责任校对：肖 迪 □责任印制：张 力

东北师范大学出版社出版发行

长春净月经济开发区金宝街 118 号（邮政编码：130117）

电话：0431—84568091

传真：0431—85605102

网址：http//www.nenup.com

电子函件：sdcbs@mail.jl.cn

三河市国英印务有限公司印装

2012 年 6 月第 1 版 2012 年 6 月第 1 次印刷

幅面尺寸：185 mm×260 mm 印张：26.125 字数：653 千

定价：52.00 元

前 言

随着社会的发展和科技的进步，计算机网络应用得到了迅猛发展和普及，给人们的生活与学习方式、生产方式和思维方式带来了巨大的变化，将人类带入到信息化与网络化时代，而网络信息安全的重要性日益突出。网络信息安全不仅影响到网络信息社会的个人生活，而且也影响到电子商务、电子现金支付、数字货币、网络银行、网上证券、电子政务等政治和经济活动。针对这种情况，大多数高等院校都开设了网络信息安全方面的课程。面对市场上众多的计算机网络信息安全的教材，我们该选哪一本来作为学生的教学用书已成为了教师和学者们普遍关注的问题。针对这种情况，我们编写了此书，希望它的出版发行，能解答学生的疑惑。

全书共分十二章，前五章可视为理论基础部分，第六章至第十章可视为实践部分，最后两章可视为案例分析。理论部分是学习网络信息安全的基础，是学生认识网络信息的入门课程，它的作用在于学生们通过这部分的学习，能对网络信息有一个初步的认识，掌握一些基本的术语，同时也为下面的技术学习奠定一定的基础。实践部分是全书的重点，这部分内容主要包括黑客入侵技术、病毒原理与反病毒技术、防火墙技术、入侵检测技术和信息隐藏技术，针对不同地区高校的教学要求和篇幅关系，我们有选择性地讲解了几个比较重要的方面来讲。这部分知识的作用在于掌握一定的技术来解决实际问题，这既巩固了理论知识又增加了技能。案例分析主要讲述信息安全协议，通过这部分内容的讲解可以做到理论与实践的结合，能使学生们更加容易地理解理论知识和实践技能。

与以往教材相比，本书具有以下特点：

首先，更加注重理论与实践的结合，倡导在科学的理论指导下，通过动手实践学到知识，用学到的知识去解决现实中的问题，例如黑客入侵、病毒原理与反病毒技术等。其次，逻辑性较强。本书按照先易后难，由浅入深的教学方法层层进行讲解和论述的，这既符合人们学习知识的认知过程，又符合教学大纲的要求。

本书主编由莫兴德（广西大学）、余棉水（广东工贸职业技术学院）、贾青平（甘肃政法学院）担任，副主编由苏锦（南阳理工学院）、郭永利（南阳广播电视大学）、余远波（海南医学院）、李志芳（海南医学院）担任，具体分工如下：

第3章～第5章、第8章第4节：莫兴德（广西大学）；

第1章、第2章、第12章：余棉水（广东工贸职业技术学院）；

第6章、第11章第1节～第2节：贾青平（甘肃政法学院）；

第10章、第7章第1节～第3节：苏锦（南阳理工学院）；

第9章、第8章第1节～第3节：郭永利（南阳广播电视大学）；

第8章第5节～第7节：余远波（海南医学院）；

第11章第3节～第6节：李志芳（海南医学院）；

第7章第4节～第5节：李晓玲（海南医学院）。

在本书的策划和编写过程中，曾参阅了国内外有关的大量文献和资料，从其中得到启示；同时也得到了有关领导、同事、朋友及学生的大力支持与帮助。在此致以衷心的感谢！

由于网络信息安全的技术发展非常快，本书的选材和编写还有一些不尽如人意的地方，加上编者学识水平和时间所限，书中难免存在缺点和谬误，敬请同行专家及读者指正，以便进一步完善提高。

编者

2012 年 4 月

目 录

第1章 网络信息安全概论

1.1 网络信息安全体系架构

信息是资源的抽象，可以被用来进行处理、存储和传输，也可以用来表达资源。例如，学生档案信息是对学生的抽象，它由专门人员进行登记，用电子数据文件对这些资源进行存储，并通过网络媒介进行传输。

1.1.1 网络信息系统中的资源

一般将网络信息系统中的资源分为三种：

第一种：人：信息系统的决策者、使用者和管理者。

第二种：应用：由一些业务逻辑组件及界面组件组成。

第三种：支撑：为开发应用组件而提供技术上支撑的资源，包括网络设施、操作系统软件等。人类资源主要提供智力的服务以及体力的服务。

每个人都是由某些生理组织系统组成的，结构上差别不大，但他们所能提供的智力服务和体力服务是大不相同的，这是由于他们各自的知识体系不同造成的。同时由于人类是高智能的系统，具有更为复杂的社会关系，这些都将是社会工程所需要研究的内容。在目前以技术为主的网络信息系统中，将人按角色与权限进行划分，其实也从某种角度上提出了对相应人类资源的知识和社会职责的要求。

所谓应用是指面向业务的技术资源。这些技术组成一个处理与人类业务相关的信息。应用虽然也表现为软件或硬件组件，但我们一般更加看中的是它能为人类解决什么样的问题。甚至可以说，应用是将一部分人类执行业务的逻辑或智能用技术的形式进行了实现，随着人工智能技术不断的发展，这些技术中所体现的智能将越来越高，面向的业务范围也越来越广。计算机和网络技术最早是由一些科学家使用，那时的业务像是一些技术领域的业务，后来将业务扩展到商务等实际应用领域。目前，我们的业务应用虽然还处于相对初级的阶段，但它的扩展是未来发展的主要方向，且将会更个性和智能。

支撑类资源更多的是一些具体的技术，为应用类资源的实现提供服务。这类资源有它们自己要处理的信息，例如，路由技术就需要处理路由资源等。支撑类资源种类很多，但在信息系统中，它们通常包括一系列的物理设施、电子设施、网络技术、操作系统等。应用和支撑之间主要的区别在于：应用资源是以逻辑驱动技术，而支撑资源是以技术驱动逻辑。

1.1.2 网络与信息安全的任务

网络安全的任务是保障各种网络资源（局域网资源、边界资源和网络基础设施）的稳定、可靠地运行和受控、合法地使用。信息安全的任务是保障信息在存储、传输、处理等过

程中的安全。具体的有：

（1）机密性（confidentiality）：是指防止非授权用户获得有用信息的特性。

（2）完整性（integrity）：是指数据没有任何遭到非授权的更改和破坏。

（3）不可抵赖性（non-repudiation）：是指实体不能抵赖其发送、接受某信息或参与某活动事实的特性。

（4）可用性（availability）：是指保证授权用户对资源合法使用的特性。

1.1.3 网络信息安全机制

网络信息安全一般是由一系列安全机制来实现的。所谓安全机制，是将安全技术实现逻辑抽象而成的一系列的模式。

在网络信息安全领域，人们提出的高层机制主要有六种：预警、防护、检测、响应、恢复、反击。它们的关系如图 1－1 所示。

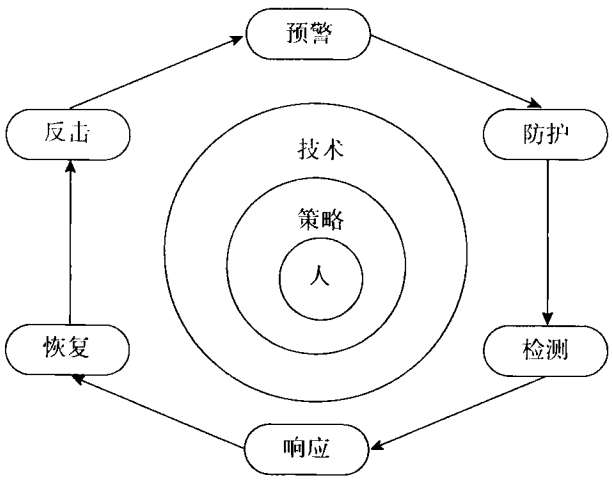


图 1－1 安全机制之间的关系

网络信息安全中层机制有：身份认证、授权、加密、网络隔离、高可用性、内容分析等。

网络信息安全基础应用域包括：网络基础设施安全、边界安全和局域网安全。网络信息安全具体应用域有：防火墙应用、入侵检测、反病毒软件、文件共享安全应用等。

网络信息安全系统的三要素：安全服务（安全任务）、安全机制和安全应用域，它们的关系可用一个三维坐标进行表述，如图 1－2 所示。

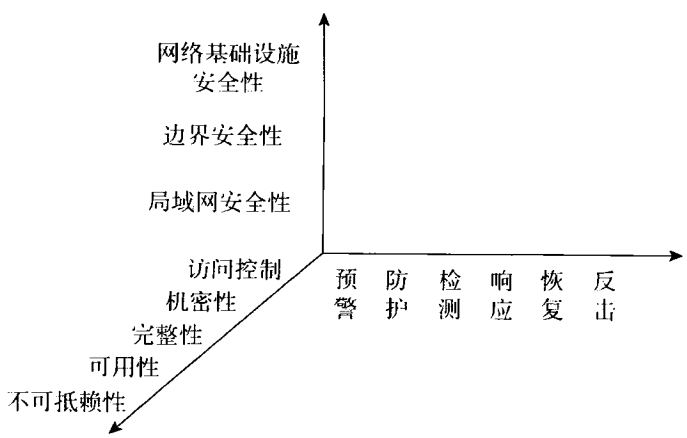


图 1－2 安全服务、安全机制和安全应用域之间的关系

1.1.4　网络安全防范体系框架结构

为了有效地了解用户的安全需求，选择各种安全产品和策略，有必要建立一些系统的方法来进行网络安全防范。网络安全防范体系的科学性、可行性是其可以顺利实施的保障。图1-3给出了基于DISSP扩展的一个三维安全防范技术体系框架结构。第一维是安全服务，给出了八种安全属性（ITU-T REC-X.800-199103-I）。第二维是系统单元，给出了信息网络系统的组成。第三维是结构层次，给出并扩展了国际标准化组织ISO的开放系统互联（OSI）模型。

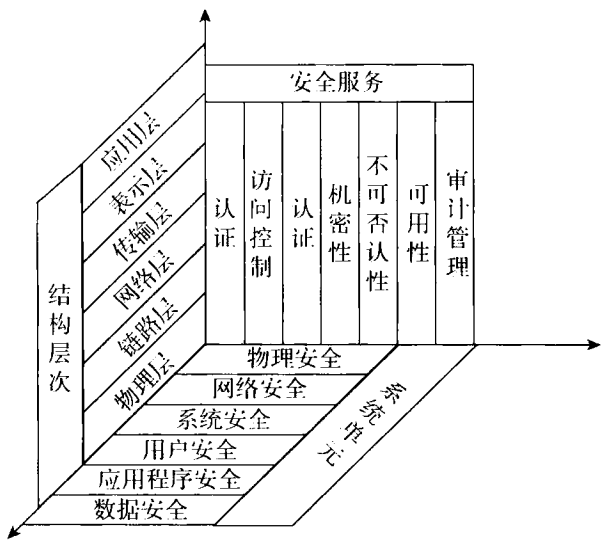


图1-3　安全防范技术体系框架结构

1.2　网络信息安全与泄露

1.2.1　网络信息安全的主要内容

现代网络技术的发明与广泛应用极大地提高了人类活动的质量与效率，但是如同许多新技术的应用一样，网络技术也是人类为自己锻造的一柄双刃剑，善意的应用能够造福人类，恶意的应用会给社会带来危害。所以，在考虑网络信息安全的保障总体规划上，不仅要在网络信息安全技术上进行统筹计划，还要强调网络信息保障研究跨学科的性质；更重要的是加强网络信息安全教育和管理，强调其系统规划与责任，重视对网络信息系统使用的法律与道德规范问题，将法律、法规和各种规章制度融入到网络信息安全解决方案之中。总之，网络信息安全保障和安全的本质在于思想观念上不是被动保护而是主动防御。

1. 网络信息的物理安全

保证计算机网络信息系统中各种设备的物理安全是整个网络信息系统安全的前提。网络信息物理安全就是指以物理方法对网络信息系统的设备和线路采取安全措施与保密，即保护计算机网络设备、设施和其他媒体免遭地震、水灾、火灾等环境事故，以及人为操作失误或

错误而导致的破坏。物理安全历来备受重视，国内外已经制定了许多标准和规范。物理安全所涉及的内容相当广泛，主要包括以下四个方面。

（1）环境安全

环境安全是对计算机网络信息系统所在环境的安全保护。例如，灾难保护和区域保护等，具体要求请参见国家标准 GB50173—93《电子计算机机房设计规范》、GB2887—89《计算站场地技术条件》和 GB9361—88《计算站场地安全要求》。

（2）媒体安全

媒体安全指对媒体的安全保管（包括媒体的防盗、防毁、防霉和防砸等），包括媒体数据的安全和媒体本身的安全，目的是保护存储在媒体上的信息。

（3）设备安全

设备安全是对计算机网络信息系统设备的安全保护，如防电磁信息辐射泄漏、防止线路截获、防盗、防毁、抗电磁干扰，以及电源保护等。

（4）计算机网络临界点安全

计算机网络临界点安全主要包括内外网络互联的设备、防火墙、无线网络设备、VPN 设备等。近年来，因特网安全性问题已成为人们越来越重视的问题。为了提高安全性，人们做了大量研究，提出了各种各样的方案，如数据加密、数字签名、身份认证、防火墙、内容过滤等，但收到的效果都不是很大。总体来讲，因特网不安全因素主要来自三个方面：外在不安全环境、缺乏系统安全标准和因特网内在不可忽视的特性。上述三方面中最重要的是第三个方面，因为因特网设计最初的目的是提供广泛互联、互操作、资源共享，侧重点并不是安全，所以它是威胁网络安全、导致网络不可信任的根本原因。

2. 网络信息密码技术

密码是网络信息安全的基础，密码技术是研究计算机信息加密、解密及其变换的科学，是数学和计算机交叉的一门新兴的学科。随着计算机网络和计算机通信技术的兴起与发展，网络信息密码技术得到前所未有的重视并迅速地普及起来。密码历史悠久，作为运用于军事与政治斗争的一种技术，无论是在古希腊时代还是在现代都发挥了非常重要的作用。现代密码学不仅用于解决信息的保密性，而且还可以用于解决信息的完整性、可用性、可控性和不可抵赖性等方面。可以说，密码是保护网络信息安全最有效的方式，密码技术也是保护网络信息安全最为关键的技术。过去密码的研制、生产、使用和管理都是在封闭的环境下进行的。20 世纪 70 年代以来，随着经济、社会和信息技术的发展和进步，密码应用范围越来越广泛，社会对密码的需求愈加迫切，密码研究领域不断拓展，密码研究也从专门机构扩展到民间，密码技术得到了空前繁荣与发展。

保障信息安全的最基本、最核心的技术措施和理论基础是密码技术。密码技术不仅在保护国家秘密信息中具有不可忽视、不可代替的作用，而且广泛应用于诸如电子邮件、政府信息上网、网上招生录取、网上购物、网络银行、数字化网络电视、网络远程教育、远程合作诊断等各个领域中。到目前为止，已经公开发表的各种加密算法多达数百种。若以密钥为分类标准，可以将密码系统分为对称密码（又叫单钥密码或私钥密码）系统和非对称密码（又叫双钥密码或公钥密码）系统；若以密码算法对明文的处理方式为标准，则可以将密码系统分为序列密码系统和分组密码系统。在私钥密码体制中，发送方和接收方可以同时使用一个秘密密钥，即加密密钥和解密密钥是相同或等价的。除了以代换密码和转轮密码为代表

的古典密码之外，比较著名的私钥密码系统主要有：美国的 DES（Data Encryption Standard）及其各种变形 Triple DES、GDES、NewDES，欧洲的 IDEA，日本的 FEAL－N、LOKl－91、Skipjack、RC4、RC5 等。

在公钥密码体制中，接收方和发送方使用的密钥是互不相同的，即加密密钥和解密密钥不相同，加密密钥公开而解密密钥保密，而且几乎不可能由加密密钥推导出解密密钥。比较著名的公钥密码系统主要有：RSA 密码系统、椭圆曲线密码系统 ECC、背包密码系统、McEliece 密码系统、Diffe－Hellman 密码系统、零知识证明的密码体制和 ELGamal 密码等。

密码管一理是指密码的生成、空间、发送、验证、更新、存储密钥的管理机制。其中密码的生成是算法安全性的基础；非线性密钥空间可假定能将选择的算法加入到防窜改模块中，要求有特殊保密形式的密钥，从而让可以偶然碰到正确密钥的可能性降低；在密钥发送时需要分成很多不同的部分，然后用不同的信道发送，即使截获者可以收集到密钥，仍可以保证密钥安全性；密钥验证要根据信道类型判断是发送者传送或是其他人伪装发送者传送；密钥更新可以采用从旧密钥中产生新密钥的方法改变加密数据链路的密钥。

3. 数字签名与认证技术

随着 Internet 的发展和应用的普及，一方面除了需要保护用户通信的私有性和秘密性，使非法用户不能获取、读懂通信双方的私有信息和秘密信息之外；另一方面，在许多应用中还需要保证通信双方的不可抵赖性和信息在公共信道上传输的完整性。数字签名（Digital Signatures，DS）、身份认证和信息认证等技术都可以解决这些问题。

数字签名的概念最早在 1976 年由 Whitfield Diffie 和 Martin Hellman 提出，其目的是让签名者对电子文件也能进行签名且无法否认，验证者没有任何办法篡改文件。简单地说，所谓数字签名就是附加在数据单元上的一些数据，或是对数据单元所做的密码变换。这种数据或变换允许数据单元的接收者用以确认数据单元的来源和数据单元的完整性并保护数据，防止被人（如接收者）进行伪造。它是对电子形式的消息进行签名的方法之一，一个签名消息可以在一个通信网络中传输。

基于公钥密码体制和私钥密码体制都能获得数字签名，目前常见的主要是基于公钥密码体制的数字签名，包括普通数字签名和特殊数字签名。普通数字签名算法主要有 RSA、ElGamal、Fiat-Shamir、Guillou-Quisquarter、Schnorr、Ong-Schnorr-Shamir 数字签名算法、DES/DSA、椭圆曲线数字签名算法和有限自动机数字签名算法等。特殊数字签名主要有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息恢复功能的签名等，它与具体应用环境是密切相关的。显然，数字签名的应用一定会涉及法律问题，美国联邦政府基于有限域上的离散对数问题制定了自己的数字签名标准（Digital Signature Standard，DSS）。

数字签名技术是在网络系统虚拟环境中确认身份的重要技术，完全能代替现实过程中的“亲笔签字”，在技术和法律上有保证。在公钥与私钥管理方面，数字签名应用与加密邮件 PGP（Prettv Good Privacy）技术正好是相反的。在数字签名应用中，发送者的公钥能十分方便地得到，但发送者的私钥则需要严格的保密。

数字签名通过一套标准化、规范化的软硬结合的系统，使得持章者能在电子文件上完成签字、盖章，与传统的手写签名、盖章等完全相同的功能。数字签名主要解决电子文件的签字盖章问题，用于辨识电子文件签署者的身份，保证文件的完整性，确保文件的真实性、可

靠性和不可抵赖性。同时根据《电子签名法》，所签属文档具有同等法律效力，极大地提高了在电子商务、电子政务中的办事效率与安全性，同时也为实现无纸化办公扫除了障碍，极大地节省办公耗材等各种资源。

在现代生活中，当人们在住宿、求职、银行存款时，一般要出示自己的身份证来证明自己的身份。但是，如果警察要求你出示身份证来证明身份，按照规定，首先警察必须先出示自己的证件来证明自身的身份。前者是一方要向另一方证明身份，而后者则是对等双方相互证明自己的身份。网络信息认证技术是网络信息安全技术的重要方面之一，它用于保证通信双方的不可抵赖性和信息的完整性。在因特网络深入发展和普遍应用的时代，网络信息认证显得极为重要。例如，在网络银行、电子商务等实际应用中，对于所发生的业务或交易，人们可能并不需要保密交易的具体内容，但是交易双方一定要能确认是对方发送（接收）了这些信息，同时接收方还可以确认接收的信息是完整的，即在通信过程中没被修改或替换。

一般情况下，网络身份认证可以分为用户与主机之间的认证和主机与主机之间的认证两种。用户与主机之间的认证可以基于如下一个或几个因素：①用户所知道的东西，如口令、密码等；②用户拥有的东西，如印章、智能卡（如信用卡等）；③用户所具有的生物特征，如指纹、声音、视网膜、签字和笔迹等。

为解决因特网的安全问题，各个国家对其进行了很多年的研究，初步形成了一套完整的因特网安全解决方案，目前被广泛采用的有 PKI（Public Key Infrastructure，公钥基础设施）。PKI 是一种遵循标准的利用公钥加密技术为电子商务的开展提供一套安全基础平台的技术与规范。它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系。用户可以利用 PKl 平台提供的服务进行安全的电子交易、通信和互联网上的各种活动。PKI 技术采用证书管理公钥，通过第三方的可信任机构—CA（Certificate Authority，证书授权）认证中心将用户的公钥和用户的其他标识信息捆绑在一起，在互联网上验证用户的身份。目前，通用的办法是采用建立在 PKI 基础之上的数字证书，通过把要传输的数字信息进行加密与签名，保证信息传输的机密性、真实性、完整性和不可否认性，从而保证信息的安全传输。PKI 是创建、颁发、管理、注销公钥证书所涉及的所有软件、硬件的集合体，其核心元素是数字证书，核心执行者是 CA 认证机构。

PMI（Privilege Management Infrastructure，授权管理基础设施）以资源管理为核心，对资源的访问控制权统一交由授权机构进行处理，即由资源的所有者来进行访问控制。PMI 是一个由属性证书、属性权威、属性证书库等部件构成的综合系统，它用来实现权限和证书的产生、管理、存储、分发和撤销等一系列功能。PMI 实际提出了一个新的信息保护基础设施，可以与 PKI 和目录服务紧密地集成，并系统地建立起对认可用户的特定授权，对权限管理进行了系统的定义和描述，完整地提供了授权服务所需的过程。PKI 证明用户是谁，而 PMI 证明这个用户有什么样权限，能干什么，而且 PMI 需要 PKI 为其提供身份认证。

4. 网络安全协议

计算机网络安全以保证其自身的安全为目的，主要内容包括网络设备安全、网络系统安全和数据库安全等。网络协议是网络上所有设备（网络服务器、计算机及交换机、路由器、防火墙等）之间通信规则的集合，它定义了通信时信息一定要采用的格式和这些格式的意义。大多数网络都会采用分层的体系结构，每一层都建立在它的下层之上，向它的上一层提供一定的服务，如把如何实现这一服务的细节对上一层加以屏蔽。一台设备上的第 n 层与另

一台设备上的第 n 层进行通信的规则就是第 n 层协议。在网络的各层中存在着很多的协议，接收方和发送方同层的协议必须是一致的，否则一方将没有办法识别另一方发出的信息。网络协议使网络上各种设备可以相互交换信息。

网络安全协议是在协议中采用了加密技术、认证技术以保证信息安全交换的安全网络协议。它运行在计算机通信网或分布式系统中，为安全需求的各方提供一系列步骤和方法。具体来讲，就是建立在密码体系上的一种互通协议，为需要安全的各方提供一系列的加密管理、身份认证及信息保密措施，以保证通信或者电子交易的安全完成。为了保证计算机网络环境中信息传递的安全性，促进网络交易的繁荣与发展，各种网络信息安全标准及协议应运而生，为网络信息交换提供了极为强大的安全保护。

常用的安全协议主要有安全外壳协议（SSH）、安全套接字层协议（SSL）、安全电子交易（SET）、网际安全协议（IPSec）和公钥基础实施（PKI）等。

5. 无线网络安全机制

无线网络是利用无线电波作为信息传输的媒介构成的无线局域网（WLAN）。它与有线网络的用途十分相似，最大的不同在于传输媒介的不同，利用无线电技术来取代网线，和有线网络相互备份。无线局域网能应用于区域覆盖和点对点传输，其中又以区域覆盖应用占绝大多数。

计算机无线联网方式是有线联网方式的一种补充，它是在有线网的基础上发展起来的，使联网的计算机能自由移动，可以快速、方便地解决以有线方式不易实现的信道连接问题。然而，由于无线网络采用空间传播的电磁波作为信息的载体，因此与有线网络是不同的，辅以专业设备，任何人都有条件窃听或干扰信息。因此，无线网络中网络安全是极为重要的。

目前，无线网络按照应用规模大致可以分为以下四种类型：①无线个人网。拥有多台计算机的家庭是十分普遍的，此类用户通常会使用集成无线功能的宽带路由器。典型距离覆盖几米到十几米，能与计算机同步传输文件，访问本地外围设备，如打印机等；②无线局域网。这类用户的无线网络大部分都是由自己或系统集成商搭建，网络规模差异很大，网络的设计水平和安全状况也是参差不齐的。典型距离覆盖几十米至上百米；③无线 LAN-to-LAN 网桥。主要是用于大楼之间的联网通信，典型距离为几千米，很多的无线网桥采用 802.11b 技术；④无线城域网和广域网。为提升城市形象或出于 ISP 之间的竞争，目前涌现了大批的机场覆盖、无线社区、无线高校，甚至无线城市，这类大型网络通常是由各大运营商进行部署的，从设计到实施都较为系统化。覆盖城域和广域环境，主要用于因特网访问。

在无线网络领域，常见的是 IEEE 802.11 标准。IEEE 802.11 是 IEEE 最初制定的一个无线网络标准，主要用于解决办公室局域网和校园网、用户与用户终端的无线接入。非法接入、带宽盗用、假冒 AP、WEP 破解工具等，这些安全问题一直伴随着无线网络，关于无线网络的安全问题，也是一个讨论很长时间的话题，但是似乎大部分的目光都集中在了硬件厂商及行业组织身上，大家多数讨论的是诸如 WEP 存在漏洞、802.11 标准尚待统一等话题。无线网络的安全问题可以分为两方面来关注：硬件厂商和行业组织固然应该致力于新技术的推出和新标准的统一，但是另一方面，用户的安全意识比最健壮的加密算法更为关键。

无线连接和无线设备的管理比有线系统要复杂很多。一旦企业忽视了无线安全问题，攻击者将能堂而皇之地进入企业内部大肆破坏，同时企业建构在有线系统上的安全设施将形同虚设。这意味着无线安全防范已成为信息安全领域新的课题，每个使用无线的用户都要认识

并解决它。

对不同的无线网络技术，有着不同的安全级别要求。通常来说，可以分为四级。第一级，扩频、跳频无线传输技术本身使盗听者难以捕捉到有用的数据。第二级，采取网络隔离及网络认证措施。第三级，设置严密的用户口令及认证措施，防止非法用户入侵。第四级，设置附加的第三方数据加密方案，即使信号被盗听也难以理解其中的内容。

针对无线网络相关的安全问题，采取的常见措施有：①运用服务区标识符（SSID）；②运用扩展服务集标识号（ESSID）；③物理地址（MAC）过滤；④连线对等保密（WEP）；⑤虚拟专用网络（VPN）；⑥端口访问控制技术（802.1x）。

各种无线网络的运用一定会越来越普遍，所以只要有资料信号在无线中传送，安全的保护机制将是人们首先要面对的问题，唯有确保万无一失的数据传输，才能满足人们在一定区域内实现不间断移动办公的要求，创造一个安全自由的空间，这也将为服务商带来无限的机会与商机。

6. 访问控制与防火墙技术

信息安全的门户是访问控制与防火墙技术。访问控制技术过去主要是用于单机状态，但如今随着网络技术的发展，此项技术也得到了长足的进步；而防火墙技术则是用于网络安全的关键技术之一。只要网络世界存在着利益之争，那么就一定要自立门户，即拥有自己的网络防火墙。

访问控制是通过一个参考监视器来进行的。每次用户对系统内目标进行访问时，都由它来进行调节。当用户对系统进行访问时，参考监视器查看授权数据库，以确定准备进行操作的用户是否确实得到了可以进行此项操作的许可。而数据库的授权则是由一个安全管理器负责管理与维护的，管理器以组织的安全策略为基准来设置这些授权。访问控制策略一般包括自由访问控制策略、强制性策略、角色策略。自由访问控制策略和强制性策略都十分有用，但并不能满足很多实际需求。角色策略成功地替代了严格的传统的强制性控制并提供了自由控制中的一些灵活性。有效的分散式授权行政管理还能使用改进的一些技术。

将计算机和网络安全更加紧密地统一联系起来，发展信息安全是十分必需的。访问控制策略尽管在这方面已经取得了很大进步，却还在发展之中。为此，必须引入防火墙技术。

通常来讲，安全防范体系具体实施的第一项内容就是在内网和外网之间构筑一道防线，以抵御来自外部的某些攻击，完成这项任务的网络边防产品称为防火墙。下面介绍防火墙的发展现状和未来发展趋势。

（1）防火墙的现状

自从1986年美国Digital公司在Internet上安装了全球第一个商用防火墙系统之后，提出了防火墙的概念，防火墙技术得到了飞速的进步与发展。第二代防火墙，也称为代理服务器，它用来提供网络服务级的控制，起到外部网络向被保护的内部网络申请服务时中间转接作用，这种方法能有效地防止对内部网络的直接攻击，安全性较高。第三代防火墙有效地提高了防火墙的安全性，称为状态监控功能防火墙，它能对每一层的数据包进行检测和监控。随着网络攻击手段和信息安全技术的发展，新一代的功能更加强大、安全性更加强的防火墙已经问世，这个阶段的防火墙已超出了原来传统意义上防火墙的范畴，已经演变成一个全方位的安全技术集成系统，人们称为第四代防火墙，它能抵御目前常见的网络攻击手段，如IP地址欺骗、特洛伊木马攻击、Internet蠕虫、口令探寻攻击、邮件攻击等。

在目前采用的网络安全的防范体系中，防火墙发挥着举足轻重的作用，因此市场对防火墙的设备需求和技术要求都在不断发展与提升。

（2）防火墙的发展趋势

①高速化。目前防火墙的一个很大的局限性是速度不够。实现高速防火墙的主要方法是应用 ASIC、FPGA 和网络处理器，其中以采用网络处理器最优。实现高速防火墙，算法也是极为关键的，因为网络处理器中集成了很多硬件协处理单元，因此极为容易实现高速。对于采用纯 CPU 的防火墙，就必须有算法支撑，如 ACL 算法。

②多功能化。防火墙的发展方向之一是多功能，鉴于目前路由器和防火墙价格都较为高，组网环境也越来越复杂，通常用户总希望防火墙能支持更多的功能，满足组网和节省投资的需要。

③更安全。未来防火墙的操作系统会更加安全。随着算法和芯片技术不断的发展，防火墙会更多地参与应用层分析，为应用提供更安全的保障。

7. 入侵检测技术

随着网络应用范围的不断扩大，对网络的各类攻击与侵害也与日俱增。无论政府、商务，还是金融、媒体的网站都在不同程度上受到入侵和侵害。网络安全已经成为国家与国防安全的重要组成部分，同时也是国家网络经济发展的关键。据数据信息统计，信息窃贼在过去 5 年中以 250% 的速度增长，99% 的大公司都发生过大的入侵事件。世界著名的商业网站，如 Yahoo，Buy，EBay，Amazon 和 CNN 都曾被黑客入侵，造成了巨大的经济损失，甚至连专门从事网络安全的 RSA 网站也曾经受到黑客的攻击。

入侵是对任何企图危及资源的完整性、机密性和可用性的活动。入侵检测（Intrusion Detection），顾名思义，就是对入侵行为的发觉，通过对计算机网络或计算机系统中的若干关键点收集信息并对收集到的信息进行整理与分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。入侵检测系统所采用的技术可以分为特征检测与异常检测两种。

特征检测，又称为 Misuse detection，这一检测假设入侵者活动可以用一种模式来表示，系统的目标是检测主体活动是否符合这些模式。它可以将已经有的入侵方法检查出来，但对新的入侵方法是无能为力的。其难点在于如何设计模式既能表达“入侵”现象，又不会将正常的活动包含进来。

异常检测（Anomaly detection）的假设是入侵者活动异常于正常主体的活动。根据这一理念建立主体正常活动的“活动简档”，将当前主体的活动状况与“活动简档”相比较，当违反其统计规律时，认为此活动可能出现是“入侵”行为。异常检测的难点在于如何建立“活动简档”，以及如何设计统计算法，从而不把正常的操作当做“入侵”或忽略真正的“入侵”行为。

随着科学技术的发展，入侵的手段与技术也有了飞速的发展，如入侵的综合化、分布化和主体间接化等，这对入侵检测技术提出了更高的要求。从此以后，入侵检测技术朝着智能化、分布化等方向发展。所谓的智能化就是利用现阶段常用的专家系统神经网络、模糊技术、遗传算法等方法，加强入侵检测的辨识能力，如现有的专家系统，尤其是具有自学习能力的专家系统，实现了知识库的不断更新和扩展，让设计的入侵检测系统的防范能力不断增强，应具有更广泛的应用前景。应用智能体的概念来进行入侵检测的尝试也已经有相关的报道。较为一致的解决方案应为高效常规意义下的入侵检测系统与具有智能检测功能的检测软

件或模块的相结合使用。

8. 网络数据库安全与备份技术

网络数据库应用系统是数据库技术与网络技术相结合进行信息处理的系统。这种结合一方面极大地提高了网络功能，另一方面也把数据库应用延伸到网络上，发挥数据库强大的数据管理作用。网络数据库应用系统正在以惊人的速度应用于社会各个方面。在国外，数据库生产已经形成一定的规模，并走向产业化和商业化，这就使得网络数据库的整体发展呈现出以下特点：数据量大，增长迅速，更新速度快；品种齐全，内容丰富；数据标准、规范、多元；检索功能强；检索结果的显示与输出灵活、多样；数据库系统有扩展整合功能等。因此，网络数据库访问的查询速度和安全控制等问题的研究已经成为新的热点与难题。

网络数据库安全的基本要求可以归纳为：数据库的完整性（物理上的完整性、逻辑上的完整性和库中元素的完整性）、数据库的保密性（用户身份识别、访问控制和可审计性）和数据库的可用性（用户界面友好，在授权范围内用户可以简便地访问数据）。当前，实现数据库安全的方案有用户身份认证、访问控制机制和数据库加密等。在大多数的数据库系统中，第一层安全部件就是用户身份认证。每个需要访问数据库的用户都一定要创建一个用户账号。用户账号管理是整个数据库安全的基础，它由数据库管理员创建与维护。在创建账号时，数据库管理员指定新用户以何种方式进行身份验证，以及用户可以使用哪些系统资源。当用户需要连接数据库时，他们一定要向服务器验证身份，服务器用预先指定的验证方法验证用户的身份。当前的主流商品化数据库管理系统都支持多种验证方案，主要有基于密码的验证、基于主机的验证、基于公钥基础设 PKI 的验证，以及其他基于第三方组件的验证方案。

访问控制策略是所有数据库管理系统实现的主要安全机制，它基于特权的概念。一个主体只有在被赋予了相应数据库对象访问权限的时候才可以访问此对象。访问控制是许多安全方案实现的基础，能可能通过创建特殊视图和存储过程来限制对数据库表内容的访问。目前，网络数据库管理系统访问控制具体分为以下四类：①任意访问控制模型。它主要采用的身份验证方案有消极验证、基于角色和任务的验证和基于时间域的验证；②强制访问控制模型。它基于信息分类方法，通过使用复杂的安全方案确保数据库免受非法入侵；③基于高级数据库管理系统的验证模型。对象数据模型包括继承、组合对象、版本和方法等概念。因此，基于关系数据库管理系统的自由和强制访问控制模型一定要经过适当的扩展才可以处理这类新增加的概念；④基于高级数据库管理系统及应用（如万维网与数字图书馆）的访问控制模型。万维网是一个动态更新、高度分布的巨型网络。基于万维网的访问控制模型带来一些新的问题，如用户认证证书、安全数据浏览、匿名访问、分布式授权和验证管理等。基于数字图书馆的访问控制模型不仅需要解决通信保密问题，而且还要解决基于数据内容的验证和保证数据完整性问题，此外，也必须要实现分布式授权访问、验证及密钥管理。

当网络用户最初听到“备份”这个词的时候，感觉就像如同老百姓最初听到“保险”这个词，熟悉之极，又陌生之极。保险的优势，只有发生意外的人才可以体会到；备份亦然。因为，现在使用网络系统处理日常业务提高工作效率的同时，系统与数据安全的问题也日益突出。一旦系统崩溃或数据丢失，用户或企业就会陷入困境。客户资料、技术文件、财务账目等数据就可能被破坏得面目全非，严重时会导致系统和数据无法恢复，其结果是不堪设想的。

解决上述问题的最佳方案是进行数据备份，备份技术的主要目的是若系统崩溃或数据一旦丢失，就可以用备份的系统和数据进行及时的恢复，让损失减少到最小。现代备份技术涉