★ 信息安全丛书　国家十五规划重点图书

★ 国家863计划信息安全技术发展战略研究专家组

★ 中国信息安全产品测评认证中心

信息安全技术概览及探索

XINXIANQUAN JISHUGAILAN JITANSUO

曲成义 陈若兰/编著

贵州科技出版社

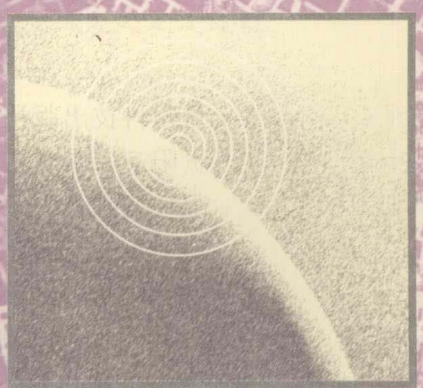
信息安全技术概览及探索

XINXIANQUAN

曲成义 陈若兰/编著

JISHUGAILAN

JITANSUO



贵州科技出版社

图书在版编目(CIP)数据

信息安全技术概览及探索/曲成义,陈若兰编著.
贵阳:贵州科技出版社,2004.5
(信息安全丛书/何德全主编)
ISBN 7-80662-308-6

Ⅰ.信... Ⅱ.①曲...②陈... Ⅲ.计算机网络—安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2004)第 029357 号

贵州科技出版社出版发行
贵阳市中华北路 289 号
邮政编码:550004
出 版 人:丁聪
印　　刷:贵州云商印务有限公司
经　　销:贵州省新华书店经销
760 mm×1092mm 16 开本 18 印张 430 千字
2004 年 5 月第 1 版 第 1 次印刷
定　　价:36.00 元

《信息安全丛书》编著单位

国家863计划信息安全技术发展战略研究专家组

中国信息安全产品测评认证中心

《信息安全丛书》编辑员会

总　　序

人类社会进入21世纪，以互联网为标志的信息时代的社会轮廓日益明晰。在这个新时代所蕴育的新世界里，人、网、环境相耦合构成了一个复杂巨系统。通过互联网的协同交流，人的智能和计算机的运算能力融合重构，涌现出社会生产力发展的崭新内涵，极大地提高了人类和环境协调发展的能力，同时，也深刻地改变着人类自身经济、社会、文化的结构和运行方式。

正如马克思所说，人的本质是“一切社会关系的总和”。在这个复杂巨系统中，“人”以资源使用者的身份出现，是系统的主体，处于主导地位，而系统资源（包括通讯网、计算机软硬件、数据和信息内容等）则是客体，它是为主体即“人”服务的。与此相适应，信息安全的主体也是“人”，其目的主要是保证主体对网络资源的控制。由此可见，提高“人”的信息安全意识，加强“人”的信息安全教育，已成为我们开展信息安全工作，构建信息安全保障体系的关键问题。

在国家科技部的直接领导下，在社会各界的大力支持下，我们在开展国家863计划信息安全技术应急项目、国家信息安全应用示范工程（上海S219工程）、国家信息安全产业化基地建设等项工作的同时，组织编写了这套《信息安全丛书》，力图集成国内信息安全专家们的智慧，较为全面地阐释多年来从事信息安全理论与实践工作的体会。

丛书的编写得取了天虹信科技资询中心、中国科学院信息安全国家重点实验室、天融信网络安全技术有限公司、启明星辰信息技术有限公司、北京江南科友科技有限公司等社会各界的大力支持与帮助，并被国家新闻出版总署列入国家“十五”重点图书规划，在此谨对各位作者及各个方面的努力表示衷心感谢。

信息安全是一个蓬勃发展的新兴领域，本套丛书的缺点和不足在所难免，希望大家多提宝贵意见，与时俱进，共同为提高全民族的信息安全意识，推动我国信息安全科技发展，促进我国信息安全保障体系建设作出贡献。

编　者

2004年5月

前　言

当前信息化浪潮席卷全球，信息技术应用正直接深入经济、政治、军事和文化等各领域，成为推动社会发展和进步的重要动力。因此，构建信息安全保障体系和发展信息安全技术和产业就成为推动信息化进程健康发展的重要保障。

《信息安全技术概览及探索》一书是“863信息安全战略专家组”组织编写的信息安全系列丛书中的首部。本书主要从信息安全保障体系中安全技术层面上论述了物理安全、系统与应用安全、网络安全和数据安全，以及密码技术、恶意代码防范技术、攻击与取证技术等重要的关键技术。本书力求将信息安全技术发展的简况和重要技术给出一个综述，并对最新的进展作一点探索，以便为信息安全研究人员、信息安全产业开发人员和信息应用系统构建人员提供一些借鉴。本书编写者都是从事信息安全科研和生产各部门的第一线人员，能够融合理论与实际，博取众家所长，但因出自多人之笔，难免有协调不当之处。

该书的具体编写者分别为：陈若兰（第1、4章），李伟斌、王志强（第2章），张明德（第3章），崔宗军（第6章），刘宝旭、刘闻欢、李路、吴鲁加、陈爱锋、郭志峰、刘光明（第5、7、8、9章）。

信息安全技术浩大精深，因编写者水平和时间所限，书中难免有错误、疏漏和不完善之处，敬请读者批评、指正。

曲成义　陈若兰

2003年6月

目　录

第 1 章 安全服务、机制和协议

1.1 信息安全概念和内涵

当今人类社会正在迈向信息时代，信息资源已成为最能代表综合国力的战略资源。我国的信息化是在经济、科技全球化的大环境下进行的，信息安全面临巨大风险和挑战。我们必须把信息安全问题放在全球战略的高度加以考虑，不失时机地努力增强我国包括信息安全保障能力在内的综合实力。

信息安全技术是伴随着信息技术的发展和应用而兴起的，随着信息技术在全球经济中地位日益增强，发达国家将信息安全领域的技术创新视为增强其国际竞争力的重要手段。在过去 10 年内，信息安全技术和产品在发达国家中迅速发展。如美国一直将信息安全技术列为国防科研和政府资助科研计划的重点项目，目前已形成包括政策、法规、技术、情报、产品、产业和基础设施等的完整体系。并采取了一系列重要措施：加大信息安全的研究和开发力度，投入大量经费用于信息系统安全的建设；建立了较大规模的信息系统安全产业，具有一定规模的信息安全产品厂家约 800 家，产品 2 000 余种；建立起信息安全基础设施，大力推广信息安全产品的应用。从 20 世纪 70 年代以来，美国先后推广防电磁辐射安全产品、安全计算机技术、网络安全技术，包括防火墙、安全操作系统、安全协议及与 PDR（保护、检测与监控、响应与恢复）相关的系列产品。美国已形成了相当规模的信息安全产业，不仅能为其国内信息与网络应用领域提供多种安全产品，而且还将自己可控的安全技术和产品向国外推销。其他国家和地区，如欧洲各国、日本、加拿大、澳大利亚等在近 5 年内也大幅度增加信息安全技术的投入，资助和推动国家级的研究和标准化

部门，成为信息安全技术研究开发的主力军。

“信息安全”的内涵可以理解为：“保证信息内容在存取、处理、传输和服务的保密性（机密性）、完整性和可用性以及信息系统主体的可控性和真实性等特征的系统辨别、控制、策略和过程”。保密性主要是指信息只能在所授权的时间、地点暴露给所授权的实体，即利用密码技术对信息进行加密处理，以防止信息泄漏。完整性是指信息在获取、传输、存储和使用的过程中是完整的、准确的和合法的，防止信息被非法删改、复制和破坏，也包括数据摘要、备份等。可用性是指信息与其相关的服务在正当需要时是可以访问和使用的。可控性是指信息系统主体可以全程控制信息的流程和服务（如检测、监控、应急、审计和跟踪）。真实性是指信息系统主体身份（如人、设备、程序）的真实合法（如鉴别、抗否认）。

信息系统本身存在着脆弱性，常被非授权用户利用，他们对计算机系统进行非法访问，这种非法访问使系统中存储信息的完整性受到威胁，导致信息被破坏而不能继续使用，更为严重的是系统中有价值的信息被非法篡改、伪造、窃取或删除而不留任何痕迹。另外，计算机还易受各种自然灾害和各种误操作的破坏。对系统中下列特征：如存储密度高、数据可访问性、信息聚生性、保密困难性、介质剩磁效应、电磁泄漏性、通信网络的弱点等等也要给予足够重视。

信息系统安全威胁的分类目前还无法统一，但可以简单地分成自然威胁和人为威胁两种。其中自然威胁是指因自然力造成的地震、水灾、风暴、雷击等，它可以破坏计算机系统实体，也可以破坏信息，自然威胁可以分为自然灾害、自然损坏、环境干扰等。各种自然灾害造成的事故和损失如表 1-1 所示。

表 1-1　　各种自然灾害造成的事故概率和损失

不安全因素	发生事故的概率	损失范围（万元）
失　　火	0.50	1~300
地震灾害	0.01	50~300
风暴灾害	0.20	50~300
洪水灾害	0.10	50~300
雷击灾害	0.01	1~100
静　　电	0.18	0.2~2

自然损坏是由系统本身的脆弱性而造成的，例如，元器件失效、设备（包括计算机、外围设备、通信及网络、供电设备、空调设备等）故障、软件故障（含系统软件和应用软件）、设计不合理、保护功能差和整个系统不协调等。

第1章 安全服务、机制和协议

环境干扰是如高低温冲击、电压降低、过压或过载、振动冲击、电磁波干扰和辐射干扰等环境因素对计算机系统造成的破坏。

人为威胁分为无意和有意两种。无意威胁是过失性的，例如操作失误、错误理解无意造成的信息泄漏或破坏。有意威胁是指攻击，如直接破坏建筑设施或设备、盗窃资料及信息、非法使用资源、施放病毒或使系统功能改变等，这是应该引起特别注意的。有意威胁又可分成被动和主动两类。被动攻击包括只对信息进行监听而不修改，主动攻击包括对信息进行篡改等。

主要的威胁包括渗入式威胁（内部威胁、假冒、旁路等）和植入式威胁（特洛伊木马、逻辑炸弹、后门等）。另外，人员的疏忽、窃听、业务流分析等潜在威胁也很重要。

信息安全既是一个理论问题，又是一个工程实践问题；信息安全也是一个完整的系统概念。单一的信息安全机制、技术和服务及其简单组合，不能保证网络信息系统的安全、有序和有效地运行。

忽视信息系统运行、应用和变更对信息安全的影响而制定的安全策略，无法获得对信息系统及其应用发生变化所出现的新的安全脆弱性和威胁的认识，这样的安全策略是不完整的，只有充分考虑并认识到信息系统运行、应用和变更可能产生新的安全风险和风险变化，由此制定的安全策略才是完整的，这就是信息安全的相关性问题。

安全策略必须能根据风险变化进行及时调整。一成不变的静态策略，在信息系统的脆弱性以及威胁技术发生变化时将变得毫无安全作用，因此安全策略以及实现安全策略的安全技术和安全服务，必须具有“风险检测→实时响应→策略调整→风险降低”的良性循环能力，这就是信息安全的动态性问题。

信息安全策略的完整实现，完全依赖技术并不现实，而且有害。因为信息安全与网络拓扑、信息资源配置、网络设备、安全设备配置、应用业务，用户及管理员的技术水平、道德素养、职业习惯等变化性因素联系密切。因此，强调完整可控的安全策略实现必须依靠管理和技术的结合，这样才符合信息安全自身规律。必要时以牺牲使用方便性、灵活性或性能来换取信息系统整体安全是值得的，同时再完善的信息安全方案也有可能出现意想不到的安全问题，这就是信息安全的相对性问题。只有经过对网络进行安全规划，对信息进行保护优先级的分类，对信息系统的安全脆弱性（包括漏洞）进行分析，对来自内外部威胁带来的风险进行评估，建立起PP-DRR（策略、保护、检测、响应和恢复）的安全模型，形成人员安全意识、安全政策

法律环境、安全管理和技术的安全框架，才是符合信息系统自身实际的科学合理的信息安全体系，这就是信息安全的系统性问题。

信息系统从单机时代经局域网、广域网发展到信息高速公路，这一高度分布、边界模糊、层次欠清、动态演化，而用户又在其中扮演主角的复杂而又巨大的系统引发了多重信息安全关系：如安全策略与实施过程、基于产品与基于过程、静态防护与动态自适应、风险规避与风险化解、可信与保障、集中与分治、信息基础设施与内容安全、技术属性与社会属性等，对立面“度”的把握十分困难，软件和人又极其复杂，这就是信息安全的复杂性问题。

1.2 信息安全参考模型

信息安全服务、机制和协议有机地统一于信息安全体系结构中，一起综合叙述比较容易理解。它们都基于网络的参考模型之上，故先简单介绍网络参考模型。目前主要流行的网络参考模型是 OSI 参考模型和 TCP/IP 参考模型。

1.2.1 OSI 参考模型

OSI(Open System Interconnection——开放系统互连)参考模型是 ISO（国际标准化组织）为解决异种机互连而制定的开放式计算机网络层次结构模型，即我国国家标准《信息处理-开放系统互连-基本参考模型 第二部分：安全体系结构》（GB/T 9387.2—1995）。它涵盖了任何类型的开放式网络环境的层次结构，优势在于将服务、接口和协议这 3 个概念明确区分，各层之间相对独立，加上其早于相关协议栈而不依赖于任何具体协议，因此普适性很强，非常适合于用来描述各种网络。

OIS 参考模型分为 7 层，由低到高依次为物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。其中物理层的作用是在物理媒介上传输原始的数据比特流；数据链路层的作用就是通过一定的手段使网络层无需了解物理层的具体物理特性而进行透明可靠的数据传输；网络层的作用是将数据分成一定长度的分组，将分组穿过通信子网从信源（发信方）传送到信宿（接收方），当分组需跨越多个网络才能到达目的时，网络层还需解决网络互连的问题；传输层是第一个端-端层，也称为主机-主机层，它为上层用户提供不依赖于具体网络的高效、经济、透明的端对端数据传输服务；会话层是进程-进程层，它组织和管理不同于主机上各进程间的对话，功能是 7 层中最少的；表示层为上层用户提供数据或信息语法的表示

转换，它实现的功能都与数据表示有关；应用层是 OSI 参考模型的最高层，它的作用是为应用进程提供访问 OSI 环境的方法。7 层中只有最低 3 层涉及通过通信子网的数据传输，因而通信子网只包括 3 层的功能。

1.2.2 TCP/IP 协议集模型

TCP/IP 协议作为因特网的骨架，是目前业界公认的事实工业标准。专门用来描述 TCP/IP 的协议栈的 TCP/IP 协议集模型（简称 TCP/IP 模型），在工业上得到了广泛的应用，但它没有明确区分开服务、接口和协议的概念，较之 OSI 参考模型一般性差。

TCP/IP 模型从下至上分作 4 层：物理层、网络层、传输层和应用层。物理层在功能上等价于 OSI 的子网络技术功能层，包括 OSI 模型网络层中与子网有关的下部子层、数据链路层和物理层，其负责将 IP 分组封装成适合在物理网络上传输的帧格式并传输，或将从物理网络接收到的帧解封，取出 IP 分组交给网络层；网络层在功能上等价于 OSI 网络层中与子网无关的部分，是此模型的关键，这一层上的协议称为 IP，它提供了数据在源和目的主机之间通过子网的路由功能，它同时也能提供网络与传输控制协议（TCP 协议）或用户数据报协议（UDP）协议之间的数据全双传输；传输层在功能上等同于 OSI 的传输层，该层上主要定义了提供流量控制和重传机制以保证用户数据可靠传到目的地的面向连接协议 TCP 和不保证数据报的可靠传送的无连接协议 UDP；应用层将 OSI 模型的应用层、表示层和会话层的功能集合为一层，此层常见协议有文件传输协议（FTP）、远程终端协议（TELNET）、简单电子邮件传输协议（SMTP）、域名系统（DNS）、简单网络管理协议（SNMP）和超文本传输协议（HTTP）等。

OSI 参考模型与 TCP/IP 模型的对应关系大致如表 1-2 所示。

表 1-2　　OSI 参考模型与 TCP/IP 模型的对应关系

OSI 参考模型	TCP/IP 协议集模型
应用层	应用层
表示层	
会话层	
传输层	传输层
网络层	网络层
数据链路层	物理层
物理层	

图 1-1 为 TCP/IP 模型各层次上对应的 TCP/IP 协议及其相互关系。

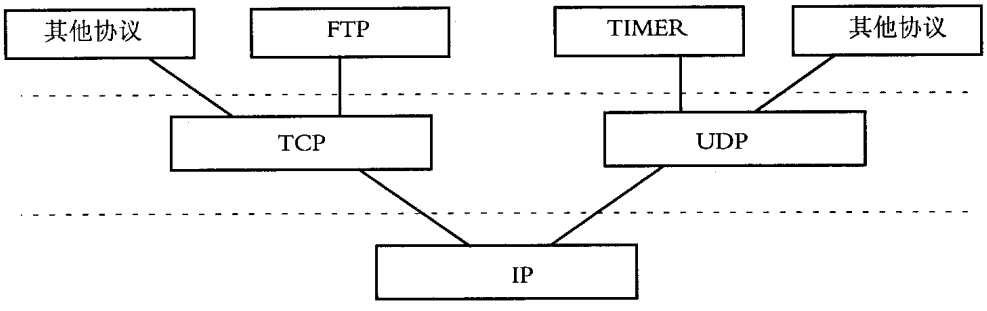


图 1-1 TCP/IP 各层协议及相互关系

1.3 安全体系结构与安全服务、机制的分层配置

安全服务（也叫安全功能）即主要的安全防护措施。安全机制是具体的安全规则，也是实现安全服务的具体方法。

如何在分层的安全体系结构中配置安全服务和安全机制是重要的策略。协议分层导致了数据项嵌在数据项之中，连接之中有连接，潜在地形成多重层嵌套。因此，我们必须对每一层应该对哪些数据项或连接提供保护做出决策。在此只提供典型安全体系结构中安全服务、机制的分层配置，供大家参考。

1.3.1 OSI 安全体系结构与分层配置

首先陈述安全服务的分层配置的正式标准是 OSI 安全体系结构标准——ISO 7498-2，颁布于 1989 年 2 月 15 日。作为国际标准，它确立了基于 OSI 参考模型 7 层协议之上的信息安全体系结构，对具体网络环境的信息安全体系结构有重要指导意义。它的核心是为了保证异构计算机进程与进程之间远距离交换信息的安全，定义了该系统 5 大类安全服务、提供这些服务的 8 类安全机制及相应的 OSI 安全管理，并可根据具体系统适当地放置在 OSI 模型的 7 层协议中。它虽然说明了哪一层适合于提供哪些安全服务，但并没有确定具体系统如何将放置每一项安全服务。ISO 7498-2 中规定的网络中的 5 类安全服务（主要的安全防护措施）是 ：

（1）鉴别服务（也叫认证服务）：提供某个实体（人或系统）的身份的保证，包括对等实体鉴别和数据源鉴别。

（2）访问控制服务：保护资源以免对其进行非法使用和操纵。

（3）机密性服务：保护信息不被泄漏或暴露给未授权的实体，包括：连接机密性、无连接机密性、选择字段机密性和业务流保密。

（4）完整性服务：保护数据以防止未授权的改变、删除或替代，包括：具有恢复功能的连接完整性、没有恢复功能的连接完整性、选择字段连接完整性、无连接完整性、选择字段无连接完整性。

（5）抗否认服务（也叫抗抵赖服务）：防止参与某次通信交换的一方事后否认本次交换曾经发生过，包括：源发方抗否认、接收方抗否认。

以上安全服务与 OSI 各层次的对应关系如表 1-3 所示。

表 1-3　　与网络各层相关的 ISO / OSI 安全服务

	协　议　层						
安　全　服　务	1	2	3	4	5	6	7★
对等实体鉴别	–	–	Y	Y	–	–	Y
数据源鉴别	–	–	Y	Y	–	–	Y
访问控制服务	–	–	Y	Y	–	–	Y
连接机密性	Y	Y	Y	Y	–	Y	Y
无连接机密性	–	Y	Y	Y	–	Y	Y
选择字段机密性	–	–	–	–	–	Y	Y
流量机密性	Y	–	Y	–	–	–	Y
有恢复功能的连接完整性	–	–	–	Y	–	–	Y
无恢复功能的连接完整性	–	–	Y	Y	–	–	Y
选择字段连接	–	–	–	–	–	–	Y
完整性无连接完整性	–	–	Y	Y	–	–	Y
选择字段非连接完整性	–	–	–	–	–	–	Y
源发方抗否认	–	–	–	–	–	–	Y
接收方抗否认	–	–	–	–	–	–	Y

说明：Y=服务应作为选项并入该层的标准之中

–=不提供

★ 第 7 层应用本身可能提供安全服务

ISO 7498-2 出现较早，随着信息安全的发展，后来安全界又提出了审计安全服务。

ISO 7498-2 中规定网络中的 8 类安全机制（具体的安全规则）是：加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、业务流填充机制、路由控制机制、公证机制。以上 8 种安全机制与它们所能提供的 5 大类安全服务对应关系如表 1-4 所示。

需要指出的是，一种安全服务可以通过某种安全机制单独提供，也可以通过多种安全机制联合提供；一种安全机制可用于提供一种安全服务，也可以用于提供多种安全服务。在 OSI7 层协议层中除第 5 层（会话层）外，每 1 层均规定有相应的安全服务，实际上安全服务最适宜配置于物理层、网络层（或传输层）和应用层。

根据 ISO 7498-2，可以整合以上两表为图 1-2 所示的三维安全空间图。

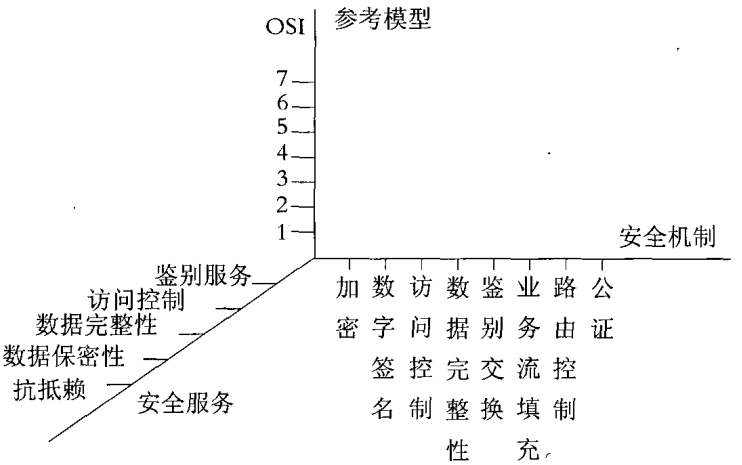


图 1-2 ISO 7498-2 三维安全空间图

1.3.2 TCP/IP 模型与分层配置

因为 OSI 参考模型与 TCP/IP 模型之间存在对应关系，就可以根据 ISO7498-2 的安全体系结构框架，将各种安全机制和安全服务映射到 TCP/IP 的协议集中，从而形成一个基于 TCP/IP 协议的网络安全体系结构，如表 1-5 所示。

表 1-5 TCP / IP 协议模型中提供的安全服务

安全服务	TCP/IP 协 议 层			
	物理层	网络层	传输层	应用层
对等实体鉴别	-	Y	Y	Y
数据源鉴别	-	Y	Y	Y
访问控制服务	-	Y	Y	Y
连接机密性	Y	Y	Y	Y
无连接机密性	Y	Y	Y	Y
选择字段机密性	-	-	-	Y
流量保密性	Y	Y	-	Y
具有恢复功能的连接完整性	-	-	Y	Y
没有恢复功能的连接完整性	-	Y	Y	Y
选择字段连接完整性	-	-	-	Y
无连接完整性	-	Y	Y	Y
选择字段非连接完整性	-	-	-	Y
源发方抗否认	-	-	-	Y
接收方抗否认	-	-	-	Y

说明：Y=服务应作为选项并入该层的标准之中

-=不提供

基于网络安全体系结构的指导，近年来国内外许多网络安全研究机构和生产厂商针对各层次上的安全隐患，不断推出新的安全协议、标准和产品，这反过来又使网络安全体系结构的理论不断充实与完善，两方面互相促进着向前发展。

1.4 安全机制

安全服务体现于安全体系结构配置层上的协议中或嵌入协议中，但协议中的安全服务仅是安全服务输入和输出参数，并不作内部处理，所有处理由安全机制具体完成，独立于协议的安全机制完成安全服务的实现和处理，是安全服务的基础，只有有了安全的安全机制，才可能有可靠的安全服务，因此，安全机制也是信息系统获得安全的基础。

根据 GB/T 9387.2—1995，安全机制包括：加密机制、数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、业务流填充机制、路由控制机制、抗否认