黄元飞 陈 麟 唐三平 编著

# 信息安全与加密解密

## 核心技术

Xinxi Anquan Yu Jiami Jiemi

**Hexin Jishu**


浦东电子出版社
PeP Pudong ePress

# 信息安全与加密解密核心技术

黄元飞　陈麟　唐三平 编著

浦东电子出版社
PEP Pudong ePress

# 内容简介

《信息安全与加密解密核心技术》围绕信息安全，特别是信息安全技术的核心技术——密码技术，就“基础知识”、“密码技术”、“应用技术”和“安全管理”等方面作了较系统和深入的介绍。其中，第 1 章至 3 章为第一部分，介绍信息安全和密码学基础知识；第 4 至 10 章为第二部分，介绍密码技术；第 11 章至 16 章为第三部分，介绍应用技术；第 17、18 章为第四部分，介绍信息安全管理；附录部分包括术语、参考文献、与安全相关的 RFC 目录等方面内容。

《信息安全与加密解密核心技术》对各级政府上网工程、基于网络的信息服务系统（如网上证券系统）的开发者，以及从事网络信息系统安全科研、教学和管理的人员，都具有参考价值。

多媒体光盘中含有与 AES 相关的原始资料和与 RFC 相关的文本，并提供了大量与加密解密算法有关的 C 语言代码和源文件。

书　　名：信息安全与加密解密核心技术
文本著作者：黄元飞　陈　麟　唐三平
CD 制 作 者：海搏多媒体制作中心
责 任 编 辑：舒红梅
出版、发行者：浦东电子出版社
地　　址：上海浦东郭守敬路 498 号上海浦东软件园内　201203
　　电话：021-38954510，38953321，38953323（发行部）
经　　销：各地新华书店、软件连锁店
排　　版：四川中外科技文化交流中心排版制作中心
CD 生 产 者：东方光盘制造有限公司
文本印刷者：郫县犀浦印刷厂
开本/规格：787×1092 毫米　16 开本　17.25 印张　310 千字
版次/印次：2001 年 7 月第一版　2001 年 7 月第一次印刷
印　　数：0001——8000 册
本 版 号：ISBN 7-900335-67-6
定　　价：36.00 元

# 前　言

随着全球信息化的发展，信息技术已经成为应用面最广，渗透性最强的战略性技术。Internet 的日益普及，极大地推动了国家信息化的步伐，给我国带来了难得的发展机遇。Internet 固有的广泛互联性和跨国性质，在给我国带来信息共享、易于交流的便利的同时，也带来了一系列的安全问题，如大量色情信息在网上自由传播，不少黑客利用网络互联攻击信息系统，不法分子利用网络传播谣言，敌特机构利用网络秘密勾结、截取情报等。

90 年代计算机网络技术迅速发展与应用，信息安全的概念已从面向数据，即强调信息的保密性、完整性和可用性，发展到面向连接、面向用户（主体——个人、企业、单位和首长等），以及“人”与环境的结合，从而突出了保证主体对信息资源（客体——包括硬件、软件、通信网、数据即信息内容等）的控制。所谓信息安全，是以确保信息在传输、存取和处理过程中，保持其保密性、完整性和可用性，并实现鉴别、授权、访问控制、抗否认性及可服务性等安全功能。这些安全问题需要依靠密码、数字签名、身份鉴别技术、防火墙、安全审计、灾难恢复、防病毒、防黑客侵入等安全机制综合加以解决。其中密码技术和管理是信息安全的核心；安全标准和系统评估是信息安全的基础。

对于信息安全，国家有关部门非常重视，自 1995 年以来，先后颁布了一系列法律、法规和政策规定；国家质量技术监督局为配合国家信息安全工作建设，先后制定了 GB/T15277-94《信息处理—64 位块加密算法操作方式》，GB/T9387-95《信息处理系统　开放系统互联基本参考模型　第二部分：安全体系结构》等十多项信息技术安全标准。上述管理文件和技术标准，是我国深入推进信息安全工作的法律保证和技术基础。

《信息安全与加密解密核心技术》围绕信息安全，特别是信息安全技术的核心技术——密码技术，就“基础知识”、“密码技术”、“应用技术”和“安全管理”等方面较系统和深入的介绍。其中，第 1 章至 3 章介绍信息安全和密码学基础知识；第 4 至 10 章为第二部分，介绍密码技术；第 11 章至 16 章为第三部分，介绍应用技术；第 17、18 章为第四部分，介绍信息安全管理；附录部分包括术语、参考文献、安全相关 RFC 目录等方面内容。它对各级政府上网工程、基于网络的信息服务系统（如网上证券系统）的开发者，以及从事网络信息系统安全科研、教学和管理的人员，都具有参考价值。

本作品由黄元飞、唐三平和陈麟合作撰写，其中唐三平主笔撰写第 9 章和第 13 章，陈麟主笔撰写第 14 章、15 章、16 章，其余部分由黄元飞主笔撰写。整个作品由黄元飞统稿，金丽萍参与了部分文字录入和校订工作。该作品的编写得到四川大学信息安全研究所、川大能士信息技术有限公司、中国国家信息安全测评认证中心的支持和帮助，在此表示感谢！

《信息安全与加密解密核心技术》涉及的内容新，技术复杂，部分内容还正处于研究阶段，加上编写时间较为仓促，尽管作者尽了自己的努力，限于作者的水平和知识，工作中难免出现不足之处，敬请读者指正。

多媒体光盘中包含与 AES 相关的原始资料和与 RFC 相关的文本,并提供了大量与加密解密算法有关的 C 语言代码和头文件。

**黄元飞　博士**

# 目　录

# 第1章 介绍

以 Internet 为代表的全球性信息化浪潮日益深刻，信息网络技术的应用正日益普及和广泛，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、关键业务系统扩展，典型的如党政机关信息系统、金融业务系统、证券业务系统、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问题，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：

- 开放性的网络导致网络的技术是全开放的，任何一个人、团体都可能获得，因而网络所面临的破坏和攻击可能是多方面的，例如：可能是来自物理传输线路的攻击，也可以对网络通信协议和实现实施攻击；可以是对软件实施攻击，也可以对硬件实施攻击。
- 国际性的网络还意味着网络受到的攻击不仅仅来自本地网络的用户，它可以来自 Internet 上的任何一个机器，也就是说网络安全所面临的是一个国际化的挑战。
- 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，而没有任何的法律限制。

尽管开放的、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，使得它们能够利用 Internet 提高办事效率和市场反应能力，以便更具竞争力。通过 Internet，它们可以从异地取回重要数据，同时又要面对 Internet 的开放性带来的数据安全的新挑战和新危险。如何保护企业的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要考虑的重要事情之一。

## 1.1 信息安全的基本概念

究竟什么是信息，目前在理论界尚无定论，据《牛津字典》中解释："信息就是谈论的事情、新闻和知识"。《韦氏字典》中解释："信息就是观察或研究过程中获得的数据、新闻和知识"。前苏联学者卢什科夫把信息定义为"物质和能量在空间和时间分布不均的测度"，意大利学者朗格提出"信息是事物间的差异"，我国信息论专家钟义信教授把信息定义为"事物运动的状态和方式"，还有人认为信息是"客观事物可传递的差异性"，更有人认为信息是"事物的运动状态和关于事物动态过程的各种陈述"，或是"对客观事物属性和相互联系特征的表达"。在我国，日常用语中的信息泛指音讯、消息。但不同学科关于信息定义的表述是不同的。曾有人统计，信息的定义在我国报刊上竟有 30 多种不同的说法。

对于"安全"也没有统一的定义，根据《汉语大词典》中的解释，"安全"一是指"平安，无危险"；二是指"保护，保全"，因此其基本含义可以解释为：客观上不存在威胁，主观上不存在恐惧。

"信息安全"同样也没有公认、统一的定义。国际、国内对信息安全的论述，大致可以

分成两大类：一类是指具体的信息技术系统的安全；另一类是指某一特定信息体系（如一个国家的银行信息系统、军事指挥系统等）的安全。但有人认为这两种定义均失之于过窄，而应把信息安全定义为："一个国家的社会信息化状态不受外来的威胁与侵害；一个国家的信息技术体系不受外来的威胁与侵害"。原因是：信息安全，首先是一个国家宏观的社会信息化状态是否处于自主控制之下，是否稳定的问题，其次才是信息技术安全问题。

### 1.1.1 信息安全的特征

信息入侵者不管怀有什么阴谋诡计，采用什么手段，他们都要通过攻击信息的下列四个安全特征来达到目的。所谓"信息安全"，在技术上的含义就是保证在客观上杜绝对信息"四性"的安全威胁，使得信息的主人在主观上对其信息的本源性放心。信息安全的四个基本特征是：

- 完整性（integrity）

完整性即信息在存储或传输过程中保持不被修改、不被破坏和不丢失的特性。信息的完整性是信息安全的基本要求。破坏信息的完整性是影响信息安全的常用手段。目前对于动态传输的信息，许多协议确保信息完整性的方法大多是收错重传、丢弃后续包。但黑客的攻击可以改变信息包内部的内容。

- 可用性（availability）

可用性是指信息可被合法用户访问并按要求的特性使用，即当需要时能否存取所需信息。例如在网络环境下破坏网络和有关系统的正常运行就属于对可用性的攻击。

- 保密性（confidentiality）

保密性是指信息不泄漏给非授权的个人和实体，或供其利用的特性。

- 可控性（controllability）

可控性是指对信息的传播及内容具有控制能力。任何信息都要在一定传输范围内可控，如密码的托管政策。托管政策即将加密算法（或后门）交由第三方或第四方管理，在使用时要严格按有关管理规定执行。

### 1.1.2 信息安全的意义

安全，是人类有序存在的前提条件，它构成了国家存在的最重要的理由。对安全的追求，在任何国家、任何时候都享有最优先的地位。

信息，是人类社会宝贵的智力资源，也是国家的关键战略资源。善于开发利用这种资源，就能有效地促进经济和社会的发展。特别是在新技术革命正在世界范围内广泛兴起的今天，大力发展利用信息资源，发展信息事业，对于繁荣一国经济（知识经济）、促进社会安定和发展、提高国家在国际社会中的地位等都具有十分重要的意义。

在国家和国防都依重信息体系的当代，必须保证信息安全。信息安全事关政权的巩固、国防的强大，直接关系到国家安全。当今世上，什么都可以"全球一体化"（例如"全球科技一体化"、"全球商业一体化"乃至"全球经济一体化"等），但就是信息安全不可以全球一体化，国家和国防的信息安全更不可能全球一体化——国家、国防信息的命根就在于安全。

## 1.2 信息安全的基本内容

信息安全不能独立于信息系统，其基本内容包括实体安全、运行安全、信息资产安全和人员安全等几个部分。

### 1.2.1 实体安全

实体安全就是保护计算机设备、设施（含网络）以及其他媒体免遭地震、水灾、火灾、有害气体和其他环境事故破坏的措施和过程。它包括三个方面：

**环境安全**：指对计算机信息系统所在环境的安全保护；

**设备安全**：指对计算机信息系统设备的安全保护，如设备的防盗和防毁，防止电磁信息泄漏，防止线路截获，抗电磁干扰以及电源保护等；

**媒体安全**：指对媒体的安全保管，目的是保护存储在媒体上的信息。其安全功能可归纳为两个方面：一是媒体的防盗；二是媒体的防毁，如防霉和防砸等。

### 1.2.2 运行安全

运行安全是信息安全的重要环节，是为保障系统功能的安全实现，提供一套安全措施（如风险分析，审计跟踪，备份与恢复，应急等）来保护信息处理过程的安全。

**风险分析**：指对计算机信息系统进行人工或自动的风险分析。它首先是对系统进行静态的分析（尤指系统设计前和系统运行前的风险分析），旨在发现系统的潜在安全隐患；其次是对系统进行动态的分析，即在系统运行过程中测试、跟踪并记录其活动，旨在发现系统运行期的安全漏洞；最后是系统运行后的分析，并提供相应的系统脆弱性分析报告。

**审计跟踪**：指对计算机信息系统进行人工或自动的审计跟踪、保存审计记录和维护详尽的审计日志。其安全功能可归纳为三个方面：记录和跟踪各种系统状态的变化，如提供对系统故意入侵行为的记录和对系统安全功能违反的记录；实现对各种安全事故的定位，如监控和捕捉各种安全事件；保存、维护和管理审计日志。

**备份与恢复**：指对系统设备和系统数据的备份与恢复，对系统数据的备份和恢复可以使用多种介质（如磁介质、纸介质、光碟、缩微载体等）。其安全功能可归纳为三个方面：提供场点内高速度、大容量自动的数据存储，备份和恢复；提供场点外的数据存储，备份和恢复，如通过专用安全记录存储设施对系统内的主要数据进行备份；提供对系统设备的备份。

**应急**：指在紧急事件或安全事故发生时，保障计算机信息系统继续运行或紧急恢复。其安全功能可归纳为三个方面：紧急事件或安全事故发生时的影响分析；应急计划的概要设计或详细制订；应急计划的测试与完善。

### 1.2.3 信息资产安全

信息资产包括文件、数据等，其安全是防止信息资产被故意的或偶然的非授权泄露、更改、破坏或使信息被非法的系统辨识，控制，即确保信息的完整性、保密性，可用性和可控性。信息资产安全包括七个方面：

**操作系统安全**：指对计算机信息系统的硬件和软件资源的有效控制，能够为所管理的资

源提供相应的安全保护。它们或是以底层操作系统所提供的安全机制为基础构造安全模块，或者完全取代底层操作系统，目的是为建立安全信息系统提供一个可信的安全平台。

**数据库安全**：指对数据库系统所管理的数据和资源提供安全保护。它一般采用多种安全机制与操作系统相结合，实现数据库的安全保护。一种选择是安全数据库系统，即从系统设计、实现、使用和管理等各个阶段都遵循一套完整的系统安全策略的安全数据库系统。二是以现有数据库系统所提供的功能为基础构造安全模块，旨在增强现有数据库系统的安全性。

**网络安全**：指提供访问网络资源或使用网络服务的安全保护。网络安全管理是为网络的使用提供安全管理，如帮助协调网络的使用，预防安全事故的发生；跟踪并记录网络的使用，监测系统状态的变化；实现对各种网络安全事故的定位，探测网络安全事件发生的确切位置；提供某种程度的对紧急事件或安全事故的故障排除能力.

**病毒防护**：指提供对计算机病毒的防护。病毒防护包括单机系统的防护和网络系统的防护。单机系统的防护侧重于防护本地计算机资源，而网络系统的防护侧重于防护网络系统资源。计算机病毒防护产品是通过建立系统保护机制预防、检测和消除病毒。

**访问控制**：指保证系统的外部用户或内部用户对系统资源的访问以及对敏感信息的访问方式符合组织安全策略。主要包括：出入控制和存取控制。出入控制主要是阻止非授权用户进入机构或组织。一般是以电子技术、生物技术或者电子技术与生物技术结合阻止非授权用户进入。存取控制指主体访问客体时的存取控制，如通过对授权用户存取系统敏感信息时进行安全性检查，以实现对授权用户的存取权限的控制。

**加密**：即提供数据加密和密钥管理。对数据的加密包括三个方面：对文字的加密；对语音的加密；对图像、图形的加密。密钥管理包括：密钥分发或注入；密钥更新；密钥回收；密钥归档；密钥恢复；密钥审计。

**鉴别**：即提供身份鉴别和信息鉴别。身份鉴别是提供对信息收发方（包括用户，设备和进程）真实身份的鉴别，主要用于阻止非授权用户对系统资源的访问。信息鉴别是提供对信息的正确性，完整性和不可否认性的鉴别。信息完整性鉴别目的在于证实信息内容未被非法修改或遗漏；不可否认鉴别，使得信息发送者不可否认对信息的发送和信息接收者不可否认对信息的接收。

### 1.2.4 人员安全

人员安全主要是指信息系统使用人员的安全意识、法律意识、安全技能等。人员的安全意识与其接受的安全技能培训和教育的关系如图 1.1 所示。

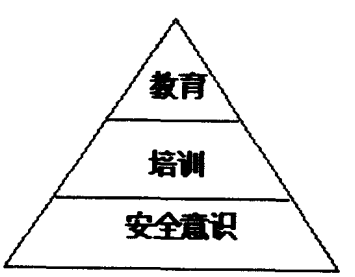


图 1.1 安全意识与教育培训的关系

## 1.3 网络安全体系框架

安全体系框架的形成主要是根据确定它所要保护的资源，对资源攻击者的假设及其攻击的目的、技术手段以及造成的后果来分析信息系统所受到的已知的、确定的和该系统有关的威胁并且考虑到构成系统各部件的缺陷、错误共同造成的风险，然后建立起系统的安全目标。一个恰当的安全目标应该把注意力集中到系统最高权力机关认为必须注意的那些方面，以最大限度体现系统资源拥有者或管理者的安全管理意志。概括地说，安全目标的实质是：当系统在进行一般操作时，在安全范围内什么是允许的，什么是不允许的。

### 1.3.1 安全体系框架的内容

网络安全体系框架包括服务原语、安全机制、安全服务和应用业务，四者的关系如图1.2所示：

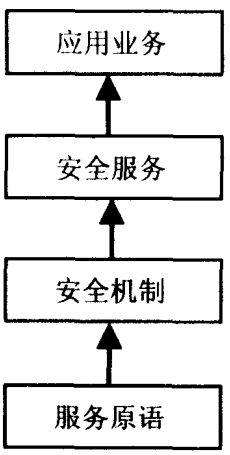


图1.2 网络安全体系框架

### 1.3.2 服务原语

服务原语是整个网络安全体系框架的基础，指的是信息安全所涉及到的一些基本技术，如网络技术、密码技术等。

### 1.3.3 安全机制

安全机制是实现安全服务的技术措施，某一安全机制可以服务于多种安全服务。参照ISO7498-2的特定安全机制和选用安全机制，结合近年来安全技术的发展，在图1.3中列出了常见的13项安全机制，其中与安全服务有关的安全机制有八个，与管理有关的安全机制有五个。

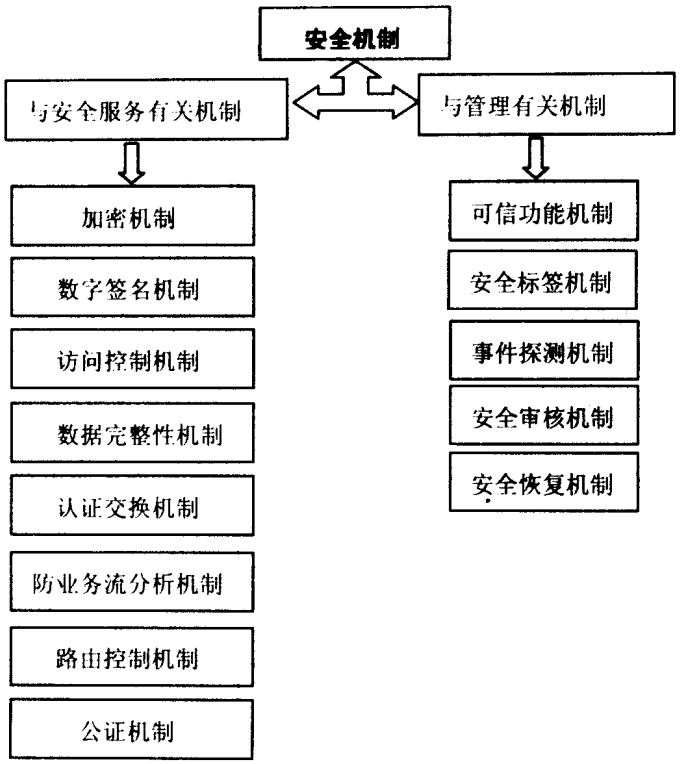


图 1.3 安全机制

**加密机制**：用来加密数据或通信中的信息。它既可以单独使用，也可以同其他机制结合使用。加密算法一般分为：对称密钥系统和公开密钥系统。

**数字签名机制**：由两个过程组成，对信息进行签名的过程和对已签名的信息进行证实的过程。前者要使用签字者的私有信息（如私有密钥）；后者使用公开的信息（如公开密钥）和过程，以鉴定签名是否由签字者的私有信息所产生。数字签名机制必须保证签名只能由签字者的私有信息产生。

**访问控制机制**：根据实体的身份及安全策略来决定该实体的访问权。分自主访问控制和强制访问控制。它的实现常基于以下某一或某几个措施：服务控制信息库、认证信息（如口令）、安全标签等。

**数据完整性机制**：在通讯中，发送方根据要发送的数据产生额外的信息（如校验码），加密后随数据一同发出；收方接到数据后，产生相应的额外信息，并与接收到的额外信息进行比较，以判断在通讯过程中数据是否被篡改过。

**认证交换机制**：根据认证信息、加密技术和实体所具有的特性来实现。

**防业务流分析机制**：通过填充冗余的业务流来防止攻击者进行流量分析，填充的信息要加密保护才能实现。

**路由控制机制**：为了使用安全的子网、中继站和链路，既可预先安排网络中的路由，也可动态地进行选择。安全策略可以禁止带有某些安全标签的信息通过某些子网、中继站和链路。连接的发起者也可规定一些路由要求，如要避开某些网络成分。

**公证机制**：由第三方（公证方）参与的数字签名机制。它是基于通信双方对第三方的绝

对信任让公证方备有适用的数字签名、加密或完整性机制等。当实体间互相通信时，就由公证方利用其所提供上述机制进行公证。有的公证机制可以在实体连接期间进行实时证实，有的则在连接结束后进行非实时证实。公证机制既可以防止收方伪造签字，或否认收到过发给它的信息；又可戳穿发方对所签发的信息的抵赖。

**可信功能机制**：扩充其他安全机制的应用范围，或增加其他安全机制的效用。

**安全标签机制**：安全性的细化，标明安全对象的敏感程度或保护级。

**事件探测机制**：探测与安全性有关的事件，既要探测安全破坏事件，也探测正常事件。

**安全审核机制**：独立地对安全系统的记录和活动进行检查，测试系统控制信息是否正常，确保安全政策的正常实施。

**安全恢复机制**：从安全破坏状态恢复到安全状态，分为：立即、临时和长期。

### 1.3.4 安全服务

安全服务是指网络为其应用提供的某些功能或辅助业务。安全机制是安全服务的基础，只有有了安全的安全机制，才可能有可靠的安全服务，因此，安全机制是信息系统获得安全的基础。常见的安全服务有对象认证安全服务、访问控制安全服务、数据保密性安全服务、数据完整性安全服务和抗抵赖安全服务等。

**对象认证安全服务**是辨明使用对象身份合法性的过程。它是针对主动攻击的主要防护措施，它的主要功能是识别和鉴别。其中识别是辨明一个对象的身份；鉴别是证明该对象的身份就是其声明的身份。

**访问控制安全服务**就是防止越权使用信息。它是针对越权使用资源和非法访问的防御措施。可分为自主访问控制和强制访问控制。

**数据保密性安全服务**是针对信息泄漏、窃听等被动威胁的防范措施。这组安全服务又细分为：信息保密、选择段保密和业务流保密。

**数据完整性安全服务**即防止非法篡改信息、文件和业务流，即资源的可获得性。

**抗抵赖安全服务**是针对对方进行抵赖的防范措施，可用来证实已发生过的操作。这组安全服务又分为：

- 防发送方抵赖，即防止信息发送者否认发送过信息；
- 防递交方抵赖，即防止信息接收者否认接收过信息；
- 公证，即通信双方互不信任，但对第三方绝对信任，于是依靠第三方证实已发生过的操作。

### 1.3.5 应用业务

网络所涉及的应用业务比较多，常见的有信息发布与信息浏览、电子邮件、电子商务、电子政务、视频点播等。网络的应用业务靠系统所提供的安全服务来保障其安全性。在考虑网络所面临的安全威胁时，除威胁方以外，另一个方面就是网络的应用业务。

## 1.4 网络安全模型

下面将讨论在互联网（Internet）[1] 上一种常见的网络安全模型，见图 1.4。通信双方通过互联网传输消息。要实现信息交换，通信双方必须相互配合，即通信双方通过共同定义一个从源到目的的路由和使用相同的协议（如 TCP/IP 协议）建立一个逻辑信道。

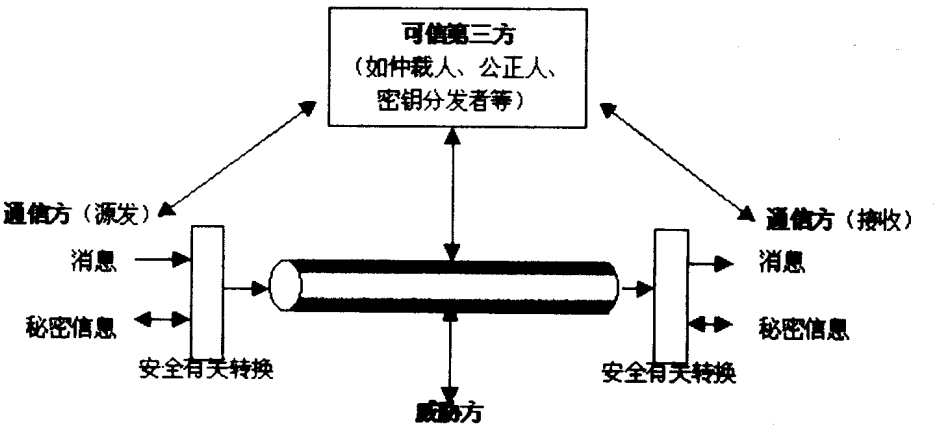


图 1.4 网络安全模型

由于在传输信息时存在威胁方影响信息的保密性、完整性、可用性等特性的可能性，因此必须考虑使用一些技术来保护信息免遭窃取、篡改和破坏。所有提供安全服务的技术由两个部分组成：

- 对所传送信息的安全有关转换。如消息的加密处理，即扰乱消息使得威胁方不能读取；或利用一个基于消息内容的额外代码来验证发送者的身份。
- 通信双方所共同拥有的一些秘密信息，但希望威胁方无法知晓。如对称密码体制所使用的加密密钥，在传输消息前用于扰乱消息，在接收端用于解除扰乱[2]。

[1] **说明**：此处的互联网指网际互联。Intranet 就是互联网的一个例子。

[2] **说明**：在公钥密码体制中，只需要其中一方拥有秘密信息。

为实现安全通信，一般需要可信第三方参与。例如为保障电子商务中交易的安全性和可靠性就需要颁发数字证书的证书认证（CA）中心，或在公正安全机制中需要可信第三方来实现公正。

通过如上模型可知每一个安全服务需要完成以下四个基本的任务：

（1）设计一个算法来完成安全相关转换，并且算法应当足够强，以抵抗威胁方的攻击；

（2）为算法产生秘密信息（即密钥）；

（3）为分配和共享秘密信息而开发一些方式或方法；

（4）为通信双方能有效使用安全算法和秘密信息而规范一个通信协议。

本书所关注的安全机制和服务基本上都符合图 1.4 所示的模型，除此以外还有其他安全

模型，例如下面的图1.5所示的网络访问安全模型。在此网络访问安全模型中，主要是防止对信息系统的未授权访问。

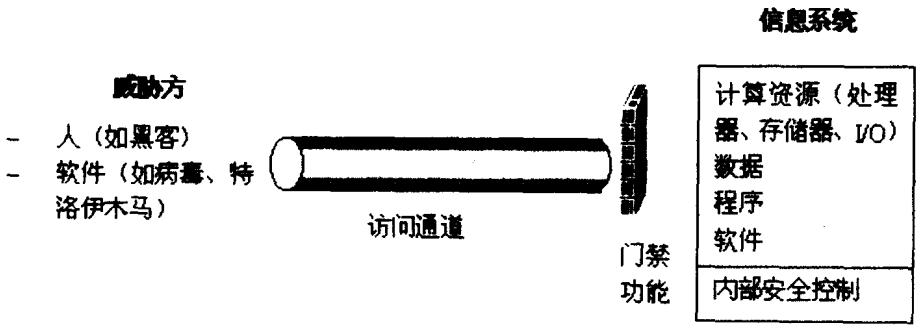


图1.5 网络访问安全模型

对网络实施威胁的人员主要有内部人员、黑客、网络罪犯、间谍等，这些人员都可能对系统弱点进行利用。其中内部人员可能有意或无意泄露系统内部信息资产；黑客是出于个人爱好或追求刺激，其目的是挑战网络的安全防范技术；网络罪犯指出于经济或政治目的，侵入系统窃取信息或实施破坏；间谍包括工业间谍或情报人员，这些人员都是有组织的有目的的侵入系统窃取信息或实施破坏，其力度明显比一般的黑客和网络罪犯都大。

对信息系统（即网络）的未授权访问，一般需要对系统弱点进一步开发利用，其结果是影响应用业务。常见的威胁有以下几种：

- **缺陷或漏洞**：指信息系统中各组成部分和整个网络在设计时，由于考虑不周全或者是设计者本身的技术能力限制，在设计、开发、制造和施工时无意识留下的可供攻击者开发利用的一些特性。
- **后门**：指在各种软硬件中含有的特殊代码，一般是开发者有意或无意留下的，本身没有危害，但可以通过这些代码获得软硬件设备的标识信息或进入操作系统特权控制的信息。
- **错误和冗余**：在信息的生命期（即处理、传输、存储、维护等过程）中，由于人为或系统原因造成的错误以及功能外冗余，影响信息的完整性，有时也会影响信息的机密性和可用性，并且在信息整个生命期的各个环节都可能存在。在一些情况下，错误是一种威胁（如操作员数据输入或存取错误将导致信息的泄露、篡改和丢失）；而在一些情况下，错误可能带来新的脆弱性（如错误地将信息存取权提供给未授权者）。
- **欺骗和窃密**：信息系统作为自动和智能化的系统，如果缺乏相应的安全措施，依靠高技术的手段和方法，是可以欺骗并窃取相关信息的。除通过通信信道的脆弱性进行的威胁外，也包括通过物理方式和逻辑方式直接进行的窃密。欺骗和窃密主要是危及信息的机密性和可用性。
- **蓄意破坏**：是指内部和外部人员有意通过物理手段对信息系统组件、结构和信息进行更改、移动和销毁等，直接危及信息的机密性、完整性、可用性和可控性，严重时会引起整个系统瘫痪和不可恢复。由于进行蓄意破坏的人员特别是内部人员可能熟悉整个系统的情况并拥有某些操作权限和信任关系，因此这种风险带来的破坏一般而言都是巨大的。
- **物理和环境的支持能力下降或丧失**：包括电力供应不足或中断、电压波动，如形成