计算机网络

安全技术研究

◎吴朔媚　宋建卫　著

NORTHEAST NORMAL UNIVERSITY PRESS
WWW.NENUP.COM
东北师范大学出版社

计算机网络安全技术研究

◎吴朔媚 宋建卫 著

NORTHEAST NORMAL UNIVERSITY PRESS
WWW.NENUP.COM
东北师范大学出版社

图书在版编目(CIP)数据

计算机网络安全技术研究 / 吴朔媚，宋建卫著 . —长春：东北师范大学出版社，2016.8
ISBN 978-7-5681-2220-7

Ⅰ. ①计… Ⅱ. ①吴… ②宋…Ⅲ. ①计算机网络—安全技术—研究 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字 (2016) 第 208701 号

□责任编辑：于天娇　□封面设计：优盛文化
□责任校对：何　云　□责任印制：张允豪

东北师范大学出版社出版发行
长春市净月经济开发区金宝街 118 号（邮政编码：130117）
销售热线：0431-84568089
网址：http://www.nenup.com
电子函件：sdcbs@mail.jl.cn
三河市佳星印装有限公司印装
2017 年 3 月第 1 版　2017 年 3 月第 1 次印刷
幅画尺寸：185mm×260mm　印张：10.75　字数：220 千

定价：45.00 元

前　言

信息时代的今天，电子邮件、网络银行、网络图书、网络社区等网络服务业得到了突飞猛进的发展，成为了各行各业经营和发展的重要工具，从某种意义上来讲，其对网络应用的好坏直接关系到自身的发展和经济效益的获得，基于此，就计算机网络技术的相关问题进行深入的分析和研究就显得尤为重要和必要了。

而就当前我国所处的宏观经济环境、政治环境和网络环境来看，由于种种主客观因素，使得计算机网络安全问题逐渐凸显，一旦网络系统受到安全的威胁，必将会给使用者带来不同程度的经济损失和名誉损失。《计算机网络安全技术研究》主要研究了网络安全基础、网络安全与病毒防范、部署安全防火墙系统三大部分的内容，其中理论知识通俗易懂，以“必须、够用”为原则，强调实用性和适用性；实训和习题部分以“科学、合理”为原则，强调代表性和有效性，同时本书涉及到的技术都有对应的产品做有效的支持，经市场调研，确实能够帮助阅读者更好的理解和掌握计算机网络安全相关的知识和技能，相信本书能够为知识需求者的学习、工作和生活有所裨益。

目 录

第1章 计算机网络安全概述 …… 1

1.1 计算机网络安全的含义 …… 1
1.2 影响计算机网络安全的因素 …… 2
1.3 计算机网络安全体系结构 …… 4
1.4 计算机网络安全设计 …… 4
1.5 计算机网络安全的评价标准 …… 6
1.6 计算机网络安全的研究意义 …… 8

第2章 数据加密与身份鉴别 …… 9

2.1 数据加密技术 …… 9
2.2 身份鉴别技术 …… 22

第3章 黑客攻击与防范 …… 23

3.1 黑客概述 …… 23
3.2 黑客攻击的步骤与防范 …… 23

3.3 端口扫描与安全防范 …… 28
3.4 拒绝服务攻击与防范 …… 30
3.5 缓冲区溢出 …… 33
3.6 特洛伊木马 …… 34

第4章 网络操作系统的安全 …… 37

4.1 Windows XP 操作系统的安全 …… 37
4.2 Windows 2003 操作系统的安全 …… 45
4.3 UNIX 操作系统的安全 …… 52
4.4 Linux 操作系统的安全 …… 54

第5章 计算机病毒及其防范 …… 61

5.1 计算机病毒概述 …… 61
5.2 计算机病毒的分类 …… 62
5.3 计算机病毒的工作原理 …… 63
5.4 常见计算机病毒介绍 …… 64
5.5 计算机病毒的防范 …… 67
第6章 防火墙技术介绍 …… 70
6.1 网络安全概述 …… 70
6.2 网络安全关注的范围 …… 71
6.3 防火墙的必备技术 …… 71

第7章 SecPath 防火墙体系结构 …… 79

7.1 SecPath 防火墙家族成员 …… 79
7.2 SecPath 防火墙业务特性 …… 85
7.3 SecPath 系列防火墙的典型应用 …… 90

第8章 安全区域 …… 93

8.1 安全区域介绍 …… 93

8.2 安全区域的基本配置 …… 96

第9章 访问控制列表 ACL …… 98

9.1 ACL 原理 …… 98

9.2 ACL 种类 …… 101

第10章 包过滤技术 …… 106

10.1 包过滤技术介绍 …… 106

10.2 包过滤防火墙基本配置 …… 107

10.3 ASPF 原理介绍 …… 109

10.4 ASPF 基本配置 …… 113

10.5 黑名单原理 …… 115

10.6 黑名单基本配置 …… 116

第11章 地址转换（NAT） …… 118

11.1 NAT 提出背景 …… 118

11.2 NAT 基本原理 …… 119

11.3 NAT 基本配置 …… 122

第12章 报文统计与攻击防范 …… 125

12.1 报文统计基本概念 …… 125

12.2 报文统计基本配置 …… 126

12.3 攻击防范 …… 130

12.4 攻击防范基本配置 …… 137

第13章 运行模式 …… 145

13.1 工作模式 …… 145

13.2 透明模式基本配置 …… 151

第 14 章　防火墙典型组网及常见故障诊断 …… 157

14.1　防火墙常见组网 …… 157

14.2　防火墙常见故障诊断 …… 159

参考文献 …… 162

第1章
计算机网络安全概述

1.1　计算机网络安全的含义

计算机网络安全不仅包括组网的硬件、管理控制网络的软件，也包括共享的资源，快捷的网络服务，所以定义网络安全应考虑涵盖计算机网络所涉及的全部内容。参照 ISO 给出的计算机安全定义，认为计算机网络安全是指："保护计算机网络系统中的硬件、软件和数据资源，不因偶然或恶意的原因遭到破坏、更改、泄露，使网络系统连续可靠性地正常运行，网络服务正常有序。"

网络安全的基本要求：

1. 机密性（Confidentiality）：它是指网络中的数据、程序等信息不会泄露给非授权的用户或实体。即信息只能够被授权的用户所使用，它是保护网络系统安全的重要手段。

2. 完整性（Integrity）：它是指网络中的数据、程序等信息未经授权保持不变的特性。即当网络中的数据、程序等信息在传输过程不会被篡改、删除、伪造、重放等破坏。

3. 可用性（Availability）：它是指当网络中的信息可以被授权用户或实体访问，并且可以根据需要使用的特性。即网络信息服务在需要时，准许授权用户或实体使用，或者当网络部分受到破坏需要降级使用时，仍可以为授权用户或实体提供有效的服务。

4. 可靠性（Reliablity）：它是指网络系统能够在特定的时间和特定的条件下完成特定功能的特性。可靠性是网络系统安全最基本的要求。

5. 可控性（Controllablity）：它是指对网络信息的传播和内容具有控制能力的特性。

它可以保证对网络信息进行安全监控。

6. 不可抵赖性（Non-Repudiation）：它是指在网络系统的信息交互过程中，确认参与者身份的真实性。它可以保证发送方无法对他发送的信息进行否认，并且可以通过数字取证、证据保全，使公证方可以方便地介入，通过法律来管理网络。

1.2 影响计算机网络安全的因素

1.2.1 网络系统自身的脆弱性

脆弱性是指计算机或网络系统在硬件、软件、协议设计和实现、系统采取的安全策略存在的不足和缺陷。脆弱性存在的直接后果就是允许非法或非授权用户获取或提高访问权限，从而给攻击者以可乘之机破坏网络系统。

总的来说，计算机网络系统脆弱性主要是由程序员不安全编程和错误操作造成的，网络协议本身的缺陷以及用户的错误使用和设置所造成的。归纳起来主要有以下几个方面。

1. 设置错误

它主要是指系统管理员或用户的错误设置，这类由于错误设置导致的系统脆弱性很受攻击者喜欢，因此，也是最常见的脆弱性。许多产品制造商在产品推向市场时为用户设置了许多默认参数，这些设置的目的主要是对用户的充分信任，方便新用户的使用，但是这些设置可能会给计算机网络系统带来很大的安全隐患。

2. 设计错误

它是指设计实现时，因为程序员由于自己的疏忽和为了自己方便而设计了一些后门，这类脆弱性很难发现，而且一旦发现也很难修补，它对网络系统的安全威胁非常大，这类脆弱性只有通过重新设计和实现。

3. 网络协议自身的缺陷

它是指网络协议自身的缺陷和不足所造成的安全隐患。网络协议是指计算机之间为了互联而共同遵守的规则，目前计算机网络大都采用 TCP/IP 协议，TCP/IP 协议在设计之初力求开放性和运行效率，缺乏对安全性的总体构想和设计，所以存在许多脆弱性，从而留下很多安全隐患。

4. 输入验证错误

它是指对用户输入数据的合法性进行验证，导致攻击者非法进入系统。大多数缓冲区溢出脆弱性 CGI 类脆弱性都是由这种原因引起的。RedHat6.2 的 dump 命令都存在这种脆弱性。

5. 访问验证错误

它是指程序的访问验证部分存在可以被利用的逻辑错误，从而有可能使非法攻击者跳过访问控制进入系统。早期 AIX 的 rlogin 就存在这种脆弱性。

6. 意外情况处理错误

它是指程序在实现逻辑中没有考虑到一些应该考虑的意外情况，从而造成运行错误。这种错误很常见，例如，没有检查文件是否存在就直接打开设备文件从而导致拒绝服务。

7. 竞争条件

它是指程序在处理实体时，时序和同步方面存在问题，在处理过程中可能提供一个机会窗口给非法攻击者以可乘之机。早期的 Solaris 系统的 ps 命令就存在这种类型的脆弱性。

8. 环境错误

它是指一些环境变量的错误设置所形成的脆弱性。

1.2.2　计算机网络面临的安全威胁

计算机网络面临的安全威胁大体可分为两种：一是对网络本身的威胁，二是对网络中信息的威胁。对网络本身的威胁包括对网络设备和网络软件系统平台的威胁；对网络中信息的威胁除了包括对网络中数据的威胁外，还包括对处理这些数据的信息系统应用软件的威胁。

影响计算机网络安全的因素很多，对网络安全的威胁主要来自人为的无意失误、人为的恶意攻击和网络软件系统的漏洞和“后门”三个方面的因素。

1. 人为的无意失误是造成网络不安全的重要原因。

网络管理员在这方面不但肩负重任，还面临越来越大的压力。稍有考虑不周，安全配置不当，就会造成安全漏洞。另外，用户安全意识不强，不按照安全规定操作，如口令选择不慎，将自己的账户随意转借他人或与别人共享，都会对网络安全带来威胁。

2. 人为的恶意攻击是目前计算机网络所面临的最大威胁。

人为攻击又可以分为两类：一类是主动攻击，它以各种方式有选择地破坏系统和数据的有效性和完整性；另一类是被动攻击，它是在不影响网络和应用系统正常运行的情况下，进行截获、窃取、破译以获得重要机密信息。这两种攻击均可对计算机网络造成极大的危害，导致网络瘫痪或机密泄漏。

3. 软件的漏洞和“后门”。

软件不可能没有安全漏洞和设计缺陷，这些漏洞和缺陷最易受到黑客的利用。另

外，许多软件都存在设计编程人员为了方便而设置的“后门”。这些漏洞和“后门”恰恰是黑客进行攻击的首选目标。

安全威胁这种对安全的潜在侵害在网络系统中主要表现在以下几个方面：

1. 非授权访问。指对网络设备及信息资源进行非正常使用或越权使用等。如操作员安全配置不当造成的安全漏洞，用户安全意识不强，用户口令选择不慎，用户将自己的账号随意转借他人或与别人共享。

2. 冒充合法用户。主要指利用各种假冒或欺骗的手段非法获得合法用户的使用权限，以达到占用合法用户资源的目的。

3. 破坏数据的完整性。指使用非法手段，删除、修改、重发某些重要信息，以干扰用户的正常使用。

4. 干扰系统正常运行，破坏网络系统的可用性。指改变系统的正常运行方法，减慢系统的响应时间等手段。这会使合法用户不能正常访问网络资源，使有严格响应时间要求的服务不能及时得到响应。

5. 病毒与恶意攻击。指通过网络传播病毒或恶意 Java、active X 等，其破坏性非常高，而且用户很难防范。

1.3 计算机网络安全体系结构

安全体系结构是针对网络安全性能提出的，OSI 安全体系结构主要包括三部分内容：安全服务、安全机制和安全管理。

安全服务就是一个系统所提供所有安全功能的总称，从分层协议来分析，底层协议实体为上层协议实体提供安全服务，同时实现对外的安全服务。OSI 安全体系结构中，一共提供了 5 种安全服务：认证服务、保密服务、数据完整性服务、访问控制服务和防抵赖服务。

安全机制是促进安全服务实现的机制，包括加密机制、访问控制机制和完整性机制等。同一种安全服务可以用多项安全机制来实现，一种安全机制也能为多种安全服务提供基础。

OSI 安全管理主要有两方面的内容，首先是安全管理，即网络和系统中各种安全服务和安全机制的管理，如认证或加密服务的激活、密钥等参数的分配、更新等；其次是管理的安全，是指各种活动的安全管理，例如，系统本身的安全管理。

1.4 计算机网络安全设计

整体的网络安全主要表现在以下几个方面：网络的物理安全、网络拓扑结构安全、

网络系统安全、应用系统安全和网络管理的安全等。

1. 网络的物理安全

网络的物理安全是整个网络系统安全的前提。在网络工程的设计和施工中，优先考虑保护人和网络设备不受电、火灾和雷击的侵害；考虑布线系统与照明电线、动力电线、通信线路、暖气管道及冷热空气管道之间的距离；考虑布线系统和绝缘线、裸体线以及接地与焊接的安全；必须建设防雷系统，防雷系统不仅考虑建筑物防雷，还必须考虑计算机及其他弱电耐压设备的防雷。总体来说，物理安全的风险主要有，地震、水灾、火灾等环境事故；电源故障；人为操作失误或错误；设备被盗、被毁；电磁干扰；线路截获；高可用性的硬件；双机多冗余的设计；机房环境及报警系统、安全意识等，因此，要尽量避免网络的物理安全风险。

2. 网络拓扑结构安全

网络拓扑结构设计也直接影响到网络系统的安全性。假如在外部和内部网络进行通信时，内部网络的机器安全就会受到威胁，同时也影响在同一网络上的许多其他系统。透过网络传播，还会影响到连上 internet/intranet 的其他的网络；影响所及，还可能涉及法律、金融等安全敏感领域。因此，我们在设计时有必要将公开服务器（Web、DNS、Email 等）和外网及内部其他业务网络进行必要的隔离，避免网络结构信息外泄；同时，还要对外网的服务请求加以过滤，只允许正常通信的数据包到达相应主机，其他的请求服务在到达主机之前就应该遭到拒绝。

3. 网络系统的安全

所谓系统的安全是指整个网络操作系统和网络硬件平台是否可靠且值得信任。目前，恐怕没有绝对安全的操作系统可以选择，无论是 Microsoft 的 Windows 2000 或者其他任何商用 Linux 操作系统，其开发厂商必然有其“后门”（back door）。因此，我们可以得出如下结论：没有完全安全的操作系统。不同的用户应从不同的方面对其网络作详尽的分析，选择安全性尽可能高的操作系统。因此，不但要选用尽可能可靠的操作系统和硬件平台，并对操作系统进行安全配置。而且，必须加强登录过程的认证（特别是在到达服务器主机之前的认证），确保用户的合法性；其次应该严格限制登录者的操作权限，将其完成的操作限制在最小的范围内。

4. 应用系统的安全

应用系统的安全跟具体的应用有关，它涉及面广。应用系统的安全是动态的、不断变化的。应用的安全性也涉及信息的安全性，它包括很多方面。

5. 网络管理的安全

网络管理的安全措施主要有：物理措施、访问控制、数据加密、防止计算机网络

病毒、安装网络防病毒系统和其他措施。

1.5 计算机网络安全的评价标准

1.5.1 国际标准

根据美国国防部开发的计算机安全标准——可信任计算机标准评价准则（Trusted Computer Standards Evaluation Criteria，TCSEC），即网络安全橙皮书，一些计算机安全级别被用来评价一个计算机系统的安全性。

自从1985年橙皮书成为美国国防部的标准以来，就一直没有改变过，多年以来一直是评估多用户主机和小型操作系统的主要方法。其他子系统（如数据库和网络）也一直用橙皮书来解释评估。橙皮书把安全的级别从低到高分成4个类别：D类、C类、B类和A类，每类又分几个级别，如表1-1所示。

表1-1 安全级别

类 别	级 别	名 称	主要特征
D	D	低级保护	没有安全保护
C	C1	自主安全保护	自主存储控制
	C2	受控存储控制	单独的可查性，安全标识
B	B1	标识的安全保护	强制存取控制，安全标识
	B2	结构化保护	面向安全的体系结构，较好的抗渗透能力
	B3	安全区域	存取监控、高抗渗透能力
A	A	验证设计	形式化的最高级描述和验证

D级是最低的安全级别，拥有这个级别的操作系统就像一个门户大开的房子，任何人都可以自由进出，是完全不可信任的。对于硬件来说，没有任何保护措施，操作系统容易受到损害，没有系统访问限制和数据访问限制，任何人不需任何账户都可以进入系统，不受任何限制可以访问他人的数据文件。属于这个级别的操作系统有DOS和Windows 98等。

C1级是C类的一个安全子级。C1级的系统又称为选择性安全保护（Discretionary Security Protection）系统，它描述了一个典型的用在UNIX系统上安全级别。这种级别的系统对硬件拥有某种程度的保护，如用户拥有注册账号和口令，系统通过账号和口令来识别用户是否合法，并决定用户对程序和信息拥有什么样的访问权，但硬件受到损害的可能性仍然存在。

用户拥有的访问权是指对文件和目标的访问权。文件的拥有者和超级用户可以改

变文件的访问属性，从而对不同的用户授予不同的访问权限。

C2 级除了包含 C1 级的特征外，应该还具有访问控制环境（Controlled Access Environment）权力。该环境具有进一步限制用户执行某些命令或者访问某些文件的权限，而且还加入了身份认证等级。另外，系统对发生的事情加以审计，并写入日志中，如什么时候开机，哪个用户在什么时候从什么地方登录，等等，这样通过查看日志，就可以发现入侵的痕迹，如多次登录失败，也可以大致推测出可能有人想入侵系统。审计除了可以记录下系统管理员执行的活动以外，还加入了身份认证级别，这样就可以知道谁在执行这些命令。审计的缺点在于它需要额外的处理时间和磁盘空间。

使用附加身份验证就可以让一个 C2 级系统用户在不是超级用户的情况下有权执行系统管理任务。授权分级使系统管理员能够给用户分组，授予他们访问某些程序的权限或访问特定的目录。能够达到 C2 级别的常见操作系统有如下几种：

（1）UNIX 系统；

（2）Novell 3. X 或者更高版本；

（3）Windows NT，Windows 2000 和 Windows 2003。

B 级中有三个级别，B1 级即标志安全保护（Labeled Security Protection），是支持多级安全（例如，秘密和绝密）的第一个级别，这个级别说明处于强制性访问控制之下的对象，系统不允许文件的拥有者改变其许可权限。

安全级别存在秘密和绝密级别，这种安全级别的计算机系统一般在政府机构中，比如国防部和国家安全局的计算机系统。

B2 级，又叫结构保护（Structured Protection）级别，它要求计算机系统中所有的对象都要加上标签，而且给设备（磁盘、磁带和终端）分配单个或者多个安全级别。

B3 级，又叫做安全域（Security Domain）级别，使用安装硬件的方式来加强域的安全，例如，内存管理硬件用于保护安全域免遭无授权访问或更改其他安全域的对象。该级别也要求用户通过一条可信任途径连接到系统上。

A 级，又称验证设计（Verified Design）级别，是当前橙皮书的最高级别，它包含了一个严格的设计、控制和验证过程。该级别包含较低级别的所有的安全特性。

安全级别设计必须从数学角度上进行验证，而且必须进行秘密通道和可信任分布分析。可信任分布（Trusted Distribution）的含义是：硬件和软件在物理传输过程中已经受到保护，以防止破坏安全系统。橙皮书也存在不足，TCSEC 是针对孤立计算机系统，特别是小型机和主机系统。假设有一定的物理保障，该标准适合政府和军队，不适合企业，这个模型是静态的。

1.5.2 国内标准

我国根据自己的国情也都制定了相关的标准，1999 年 10 月经国家质量技术监督局批准发布的《计算机信息系统安全保护等级划分准则》将计算机安全保护划分为以下 5 个级别：

- 第 1 级为用户自主保护级（GB1 安全级）：它的安全保护机制使用户具备自主安全保护的能力，保护用户的信息免受非法的读写破坏。
- 第 2 级为系统审计保护级（GB2 安全级）：除具备第一级所有的安全保护功能外，要求创建和维护访问的审计跟踪记录，使所有的用户对自己的行为的合法性负责。
- 第 3 级为安全标记保护级（GB3 安全级）：除继承前一个级别的安全功能外，还要求以访问对象标记的安全级别限制访问者的访问权限，实现对访问对象的强制保护。
- 第 4 级为结构化保护级（GB4 安全级）：在继承前面安全级别安全功能的基础上，将安全保护机制划分为关键部分和非关键部分，对关键部分直接控制访问者对访问对象的存取，从而加强系统的抗渗透能力。
- 第 5 级为访问验证保护级（GB5 安全级）：这一个级别特别增设了访问验证功能，负责仲裁访问者对访问对象的所有访问活动。

1.6 计算机网络安全的研究意义

网络安全是一个关系国家安全和主权、社会的稳定、民族文化的继承和发扬的重要问题。其重要性，正随着全球信息化步伐的加快而变得越来越重要。“家门就是国门”，安全问题刻不容缓。

网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

网络安全的具体含义会随着“角度”的变化而变化。比如，从用户（个人、企业等）的角度来说，他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私，访问和破坏。从网络运行和管理者角度说，他们希望对本地网络信息的访问、读写等操作受到保护和控制，避免出现“陷门”、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁，制止和防御网络黑客的攻击。对安全保密部门来说，他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵，避免机要信息泄露，避免对社会产生危害，对国家造成巨大损失。从社会教育和意识形态角度来讲，网络上不健康的内容，会对社会的稳定和人类的发展造成阻碍，必须对其进行控制。

第2章
数据加密与身份鉴别

2.1　数据加密技术

2.1.1　数据加密的概念

加密是保证网络资源安全的一种方式，而数据加密（Encryption）是指将明文信息（Plaintext）采取数学方法进行函数转换成密文（Ciphertext），只有特定接受方才能将其解密（Decryption）还原成明文的过程。其中，明文（Plaintext）是加密前的原始信息，密文（Ciphertext）是明文被加密后的信息。发送方用加密密钥，通过加密算法或设备，将信息加密后发送出去。接受方在收到密文后，用解密密钥将密文解密，恢复为明文。如果传输中有人窃取，他只能得到无法理解的密文，从而对信息起到保密作用。其数据加密模型如图 2-1 所示。

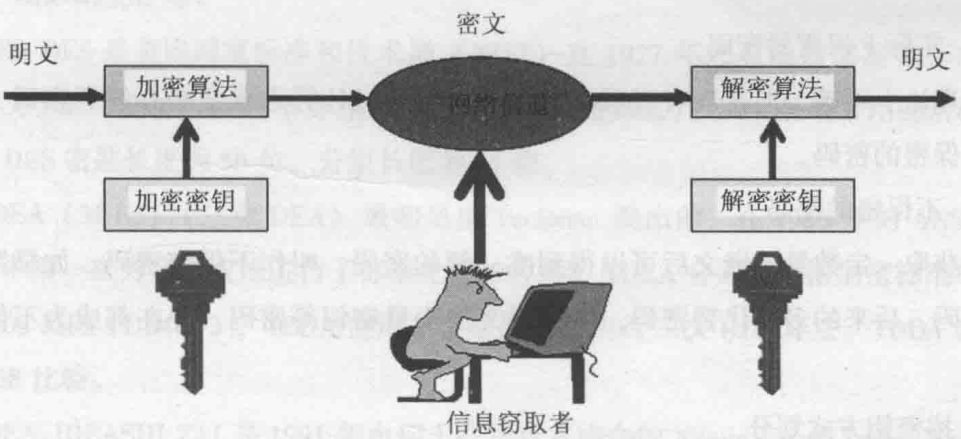

图 2-1　数据加密模型