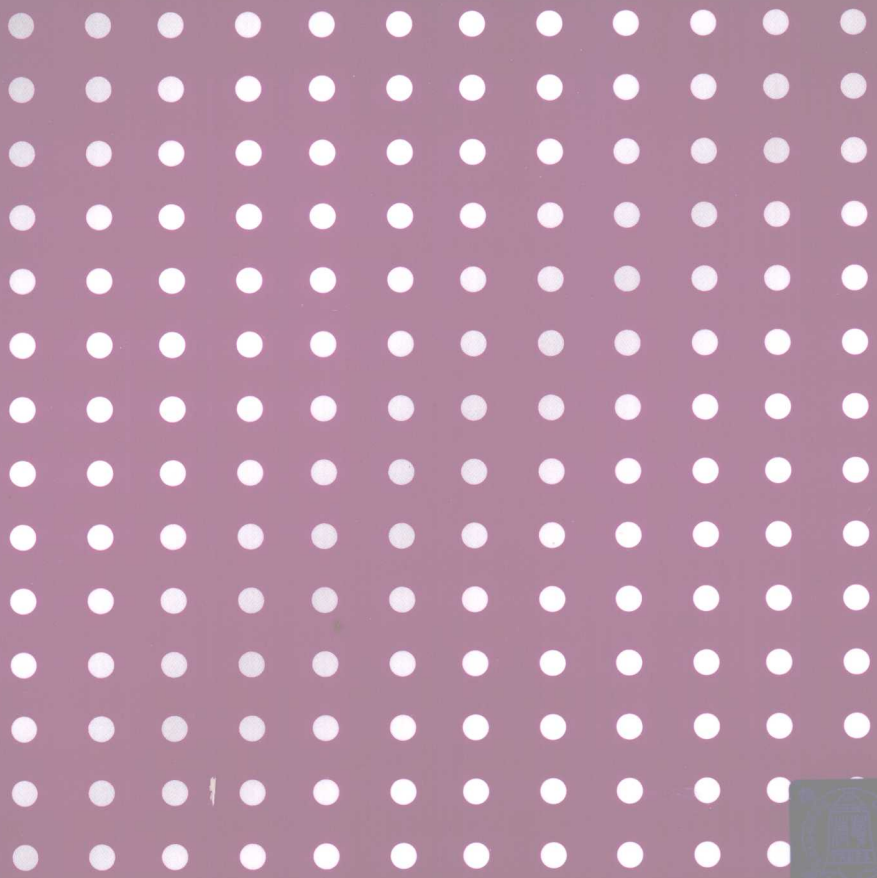
高等院校信息技术规划教材

信息系统攻防技术

程煜 余燕雄 编著



清华大学出版社

高等院校信息技术规划教材

信息系统攻防技术

程煜 余燕雄 编著

清华大学出版社
北京

内 容 简 介

本书全面介绍信息系统各种攻防手段的基本原理和应用技术，对信息安全的相关概念与技术进行了深入探讨，详尽地分析了信息系统的各种攻击技术和相应防御措施。对于具体攻击技术，本书首先剖析原理，讲述流程，然后结合案例，强调实际应用中所需的信息安全知识，同时给出了相应的用户对策。

本书叙述简洁，结构清晰，理论体系较完整，可作为信息安全专业的“信息安全导论”课程和计算机、电子信息、通信工程等专业的“信息安全”课程的教材。同时，全书结合实例，讲解透彻，通俗易懂，也可供工程技术人员作为参考用书。

图书在版编目（CIP）数据

信息系统攻防技术/程煜，余燕雄编著. —北京：清华大学出版社，2009.9
（高等院校信息技术规划教材）
ISBN 978-7-302-20018-5

Ⅰ. 信… Ⅱ. ①程… ②余… Ⅲ. 信息系统－安全技术－高等学校－教材
Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2009)第 063667 号

责任编辑：袁勤勇　顾　冰
责任校对：时翠兰
责任印制：孟凡玉

出版发行：清华大学出版社　　地　　址：北京清华大学学研大厦 A 座
http://www.tup.com.cn　　邮　　编：100084
社　　总　　机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京嘉实印刷有限公司
经　　销：全国新华书店
开　　本：185×260　　印　　张：14　　字　　数：326 千字
版　　次：2009 年 9 月第 1 版　　印　　次：2009 年 9 月第 1 次印刷
印　　数：1～3000
定　　价：19.50 元

高等院校信息技术规划教材

系 列 书 目

书　名	书　号	作　者
数字电路逻辑设计	978-7-302-12235-7	朱正伟　等
计算机网络基础	978-7-302-12236-4	符彦惟　等
微机接口与应用	978-7-302-12234-0	王正洪　等
XML 应用教程(第 2 版)	978-7-302-14886-9	吴　洁
算法与数据结构	978-7-302-11865-7	宁正元　等
算法与数据结构习题精解和实验指导	978-7-302-14803-6	宁正元　等
工业组态软件实用技术	978-7-302-11500-7	龚运新　等
MATLAB 语言及其在电子信息工程中的应用	978-7-302-10347-9	王洪元
微型计算机组装与系统维护	978-7-302-09826-3	厉荣卫　等
嵌入式系统设计原理及应用	978-7-302-09638-2	符意德
C++ 语言程序设计	978-7-302-09636-8	袁启昌　等
计算机信息技术教程	978-7-302-09961-1	唐　全　等
计算机信息技术实验教程	978-7-302-12416-0	唐　全　等
Visual Basic 程序设计	978-7-302-13602-6	白康生　等
单片机 C 语言开发技术	978-7-302-13508-1	龚运新
ATMEL 新型 AT89S52 系列单片机及其应用	978-7-302-09460-8	孙育才
计算机信息技术基础	978-7-302-10761-3	沈孟涛
计算机信息技术基础实验	978-7-302-13889-1	沈孟涛　著
C 语言程序设计	978-7-302-11103-0	徐连信
C 语言程序设计习题解答与实验指导	978-7-302-11102-3	徐连信　等
计算机组成原理实用教程	978-7-302-13509-8	王万生
微机原理与汇编语言实用教程	978-7-302-13417-6	方立友
微机组装与维护用教程	978-7-302-13550-0	徐世宏
计算机网络技术及应用	978-7-302-14612-4	沈鑫剡　等
微型计算机原理与接口技术	978-7-302-14195-2	孙力娟　等
基于 MATLAB 的计算机图形与动画技术	978-7-302-14954-5	于万波
基于 MATLAB 的信号与系统实验指导	978-7-302-15251-4	甘俊英　等
信号与系统学习指导和习题解析	978-7-302-15191-3	甘俊英　等
计算机与网络安全实用技术	978-7-302-15174-6	杨云江　等
Visual Basic 程序设计学习和实验指导	978-7-302-15948-3	白康生　等
Photoshop 图像处理实用教程	978-7-302-15762-5	袁启昌　等
数据库与 SQL Server 2005 教程	978-7-302-15841-7	钱雪忠　著

计算机网络实用教程	978-7-302-16212-4	陈　康　等
多媒体技术与应用教程	978-7-302-17956-6	雷运发　等
数据结构	978-7-302-16849-2	闫玉宝　等著
信息系统分析与设计	978-7-302-16901-7	杜娟、赵春艳、白宏伟等　著
微机接口技术实用教程	978-7-302-16905-5	任向民　著
基于 Matlab 的图像处理	978-7-302-16906-2	于万波　著
C 语言程序设计	978-7-302-16938-3	马秀丽　等
SAS 数据挖掘与分析	978-7-302-16920-8	阮桂海　等
C 语言程序设计	978-7-302-17781-4	向　艳　等
工程背景下的单片机原理及系统设计	978-7-302-16990-1	刘焕成　著
多媒体技术实用教程	978-7-302-17069-3	吴　青　著
Web 应用开发技术	978-7-302-17671-8	高　屹　等
C 语言程序设计	978-7-302-17781-4	向　艳　等
ASP. NET 实用教程	978-7-302-16338-1	康春颖、张　伟、王磊等　著
Visual FoxPro 9.0 程序设计	978-7-302-17858-3	张翼英　等
Visual Basic 在自动控制中的编程技术	978-7-302-17941-2	龚运新　等
计算机网络安全实用技术	978-7-302-17966-5	符彦惟　等
Visual FoxPro 程序设计基础教程	978-7-302-18201-6	薛　磊　等
数据结构与算法	978-7-302-18384-6	赵玉兰　等
信息系统攻防技术	978-7-302-20018-5	程　煜　等

前言 foreword

如果说30年前美国小说《P-1的春天》描述的病毒控制计算机酿成灾难的故事叫人难以想象，10年前上映的美国大片《黑客帝国》讲述的科幻故事令人着迷而困惑，那么今天隐藏在网络生活中的计算机病毒和黑客却让人们恐惧和愤恨。

近年来，黑客针对自身防范力量比较弱的中小企业网站实施攻击，造成这些企业和个人损失巨大，一些地方甚至形成了只有交“保护费”才能免遭病毒攻击正常运营的局面。

2003年底到2004年初肆虐网络的“熊猫烧香”木马病毒，在短短的两个月内使上百万个人用户、网吧及企业局域网用户遭受感染和破坏。用户计算机中毒后会出现蓝屏、频繁重启以及系统硬盘中数据文件被破坏等现象，更重要的是它可以盗取网民银行和游戏账号、密码，从而窃取用户的财产或虚拟财产。连续多年被指为年度十大病毒、被反病毒专家称为最危险的后门程序“灰鸽子”于2001年问世，随着“灰鸽子2007”的发布，于2004年3月集中爆发，病毒仅10多天就有500多个变种产生。与“熊猫烧香”的“张扬”不同，“灰鸽子”更像一个隐形的“贼”，潜伏在用户“家”中，监视用户的一举一动，甚至用户与MSN、QQ好友聊天的每一句话都难逃“贼”眼。

过去，病毒的制作者多是为了显示自己超人的技术，而今天病毒的制作者更多是为了牟利。在利益驱使下，病毒制作、销售、传播、盗取信息等已形成了分工明确的黑色产业链条。互联网“地下经济”已经组织化、规模化、公开化，制造木马、传播木马、盗窃账户信息、第三方平台销赃、洗钱，分工明确，形成了一个非常完善的流水线作业的程序，产业链上的每一环都有不同的牟利方式。据不完全统计，“灰鸽子”病毒程序直接售卖价值就达2000万元以上，用于窃取账号等的幕后黑色利益可想而知。

面对黑色病毒产业链，必须站在维护国家安全和促进中国互联网健康快速发展的高度来保障网络安全，建立网络安全国家应急体系，加大对网络安全领域犯罪的打击，完善立法，加快防病毒和网络攻击的技术及工具产品的研发，确保网络安全。

在这场信息安全的战争中，黑客就是敌方。分析研究黑客的攻击方法和攻击模式可以更加了解黑客的思想，从而制定出有效的防范措施。同时，在掌握黑客的攻击方法后，还可以进行渗透测试，检查网络的安全性，实现网络信息的安全。本书强调从进攻的角度研究防御，从实践出发，由实践上升到理论，再用理论指导实践，培养信息安全专业学生的理论功底、实际动手能力，使学生能够运用攻防技术分析和解决实际问题。

全书共分8章，各章主要内容如下。

第1章：绪论。主要介绍了信息安全的基本知识和目前面临的威胁及应对措施，希望通过本章的学习，读者可以对信息安全有一个较为全面的了解。

第2章：系统攻击典型案例。首先介绍了一些网络攻防的基础知识，主要是网络协议和常用网络命令，尤其是常用网络命令，在攻防实践中大量使用，应该重点掌握用法；本章后一部分以典型案例为主线详细描述了系统攻击的一般流程，希望读者能够了解黑客攻击全过程。

第3章：缓冲区溢出攻击与防范。漏洞攻击、认证攻击和木马是黑客最主要的攻击手段，缓冲区溢出漏洞攻击更是最常见的攻击方式。本章结合案例，针对缓冲区溢出的基本原理，系统地分析了利用溢出漏洞的攻击过程，给出了防范缓冲区溢出漏洞攻击的有效措施。需要注意的是，本章使用的案例重在使用户清楚了解利用溢出漏洞的攻击过程，案例本身并不复杂，限于篇幅所限，很多高级技术不能一一列举，有兴趣的读者可以到网上下载“缓冲区溢出教程”详细研究。

第4章：身份认证攻击与防范。本章系统、充分地介绍了针对身份认证的各种攻击形式，给出了在系统开发和应用阶段进行有效合理屏蔽的思路和方法。这一章的重点是SQL注入攻击，这部分的案例使用到了大量的SQL语句，而且都做了充分的说明。如果读者要掌握更多的数据库相关知识，可以参看《数据库系统概念》。

第5章：木马攻击与防范。详细介绍了木马的工作原理、攻击实例、“免杀”技术和防御措施，并给出了一个木马的部分源代码，供学习使用。

第6章：隐藏与清理。介绍了信息系统攻击中隐藏攻击者信息和痕迹的手段，同时也提供了发现隐藏的攻击者的方法。

第7章：防火墙的使用与攻击。详细说明了防火墙在信息安全体系中的作用和使用方法（包括具体的配置命令），针对面向防火墙的攻击给出了具体的防御措施。

第8章：现代密码学攻击与防范。介绍了当前信息安全技术发展最前沿的科技成果和相关应用。随着科学研究的不断进步，所有的信息安全攻防都会建立在现代密码学的应用基础上。

本书由余燕雄和程煜设计编写，在编写过程中得到了马进先生的大力支持，在此表示由衷的感谢。由于时间仓促和水平有限，而且信息攻防技术一日千里，书中难免有错漏之处，敬请各位读者谅解并提出宝贵意见。您的意见和建议请发到编者电子邮箱：chengyu@whut.edu.cn，在此不尽感激。

编　者

2009年春于武汉

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602　　计算机与信息分社营销室 收

邮编：100084　　电子邮件：jsjjc@tup.tsinghua.edu.cn

电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：信息系统攻防技术

ISBN：978-7-302-20018-5

个人资料：

姓名：_____ 年龄：_____ 所在院校/专业：_____

文化程度：_____ 通信地址：_____

联系电话：_____ 电子信箱：_____

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书的总体满意度：

从语言质量角度看 □很满意 □满意 □一般 □不满意

从科技含量角度看 □很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？（可附页）

_____

_____

您希望本书在哪些方面进行改进？（可附页）

_____

_____

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页（http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn）上查询。

目录 contents

第1章 chapter 1

绪　论

1.1 信息安全概述

1.1.1 什么是信息安全

“安全”的基本含义为“远离危险的状态或特性”或“主观上不存在威胁，主观上不存在恐惧”。安全问题是普遍存在的，在各个领域都存在着安全问题。伴随着计算机网络的飞速发展，人们对信息的存储、处理和传递过程中涉及的安全问题越来越关注，信息领域的安全问题变得非常突出。

信息安全是一个广泛而又抽象的概念，不同领域不同方面对其概念的阐述都会有所不同。建立在网络基础之上的现代信息系统的安全定义是保护信息系统的硬件、软件及相关数据，使之不因为偶然或者恶意侵犯而遭受破坏、更改及泄露，保证信息系统能够连续、可靠、正常地运行。

信息安全是是一门交叉学科。广义上，信息安全涉及多方面的理论和应用知识，除了数学、通信、计算机等自然科学外，还涉及法律、心理学等社会科学。狭义上，也就是通常说的信息安全，只是从自然科学的角度介绍信息安全的研究内容。信息安全各部分研究内容及相互关系如图 1-1 所示。

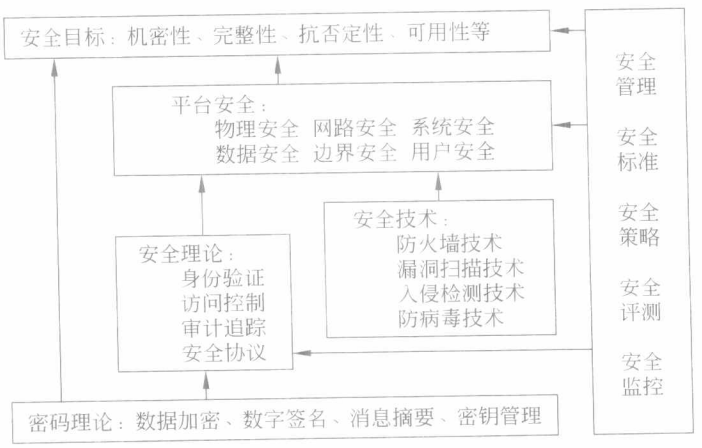


图 1-1　信息安全的研究内容及相互关系

1.1.2 信息安全体系

随着信息系统的广泛建立和各种网络的相互联通，也随着安全对抗技术的不断发展，人们开始发现，信息安全是一个系统工程。单纯地从安全功能及技术组合的层次上孤立地、个别地解决系统的安全问题，常常会事倍功半，顾此失彼。处理系统性的问题，必须从系统的层面上解决，必须从体系结构的层面上全面地考虑问题。于是，人们提出了安全管理问题，对安全的要求不应当是绝对的，而应当是有效的，有效性的评估依据是标准。信息系统安全体系和安全评估标准成为了信息系统安全管理的核心和最基本的内容。

信息系统的安全体系结构研究站在系统全局的角度，将普遍性安全体系原理与信息系统自身的实际相结合，形成满足信息系统安全需求的安全体系结构。它涉及系统的安全需求、安全策略、安全服务、安全机制和安全模型等多个方面。信息安全体系就是为了从管理、技术上保证安全策略得以完整、准确地实现，包括技术体系、组织体系和管理体系。OSI 信息安全体系框架如图 1-2 所示。

图 1-2 OSI 信息安全体系框架

技术体系：全面提供信息系统安全保护的技术保障系统。OSI 安全体系通过技术管理将技术机制提供的安全服务，分别或同时应用在 OSI 协议层的一层或多层上，为数据、信息内容、通信连接提供机密性、完整性和可用性保护，为通信实体、通信连接、通信进程提供身份鉴别、访问控制、审计和抗抵赖保护，这些安全服务分别作用在通信平台、网络平台和应用平台上。保障和运行的安全体系是与 OSI 安全体系不同的技术保障体系，包括物理安全技术和系统安全技术。

组织结构体系：信息系统安全的组织保障系统，由机构、岗位和人事三个模块构成一个体系。机构的设置分为三个层次：决策层、管理层和执行层。

管理体系：由法律管理、制度管理和培训管理三部分组成，是信息系统安全的灵魂。

1.1.3 信息安全服务与机制

安全服务是由参与通信的开放系统的某一层提供的服务，它确保该系统数据传输具有足够的安全性。ISO7498-2 标准是目前国际上普遍遵循的计算机信息系统互连标准，

首次确定了开放系统互连(OSI)参考模型的信息安全体系结构,保证开放系统进程之间远距离安全的交换信息。ISO7498-2 确定了五大类安全服务和八大安全机制,图 1-3 标识的是 OSI 体系服务与机制三维图。

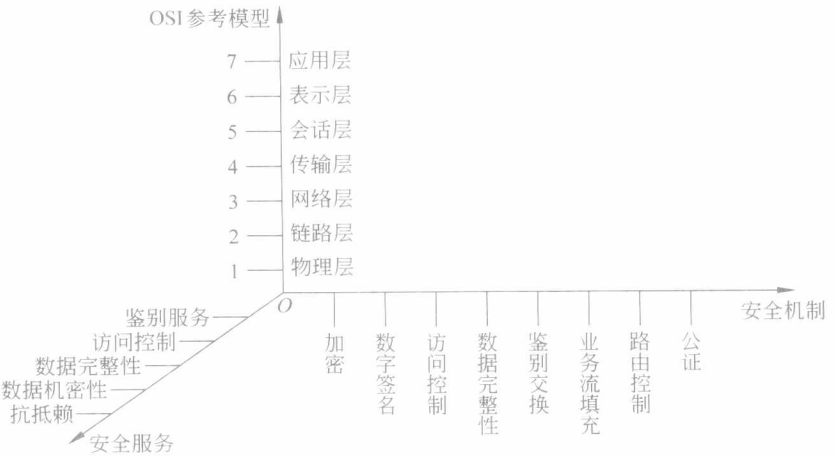


图 1-3 OSI 体系服务与机制三维图

1. OSI 安全体系的安全服务

1) 鉴别服务

鉴别服务提供对通信中的对等实体和数据来源的鉴别,包括对等实体鉴别和数据原发鉴别。对等实体鉴别用于确认有关的对等实体是所需的实体。当这种服务由 N 层提供时,将使 $N+1$ 层实体确信交互的对等实体正是它所需要的 $N+1$ 层实体。对等实体鉴别在连接建立或在数据传送阶段的某些时刻提供使用,用以证实一个或多个连接实体的身份。使用这种服务可以(仅仅在使用时间内)确信:一个实体此时没有试图冒充(一个实体伪装为另一个不同的实体)别的实体,或没有试图将先前的连接作非授权地重放(出于非法的目的而重新发送截获的合法通信数据项的拷贝)。实施单向或双向对等实体鉴别也是可能的,可以带有效期检验,也可以不带,这种服务能够提供各种不同程度的鉴别保护。

数据原发鉴别用于确认接收到的数据的来源是所要求的。这种服务由 N 层提供时,将使 $N+1$ 层实体确信数据来源正是所要求的对等 $N+1$ 层实体。数据原发鉴别服务对数据单元的来源提供确认,这种服务对数据单元的重放或篡改不提供鉴别保护。

2) 访问控制

访问控制防止对资源的未授权使用,包括防止以未授权方式使用某一资源。这种服务提供保护以对付开放系统互连可访问资源的非授权使用,这些资源可以是经开放系统互连协议访问到的 OSI 资源或非 OSI 资源。这种保护服务可应用于对资源的各种不同类型的访问(如使用通信资源、读写或删除信息资源、处理资源的操作),或应用于对某种资源的所有访问。

3）数据机密性

数据机密性服务对数据提供保护，使之不被泄露，包括下面4种服务。

（1）连接机密性：这种服务为一次 N 层连接上的全部 N 层用户数据保证机密性。但是，对于某些使用中的数据，或在某些层次上将所有数据（例如加速数据或连接请求中的数据）都保护起来反而是不适宜的。

（2）无连接机密性：这种服务为单个无连接的 N-SDU（N 层服务数据单元）中的全部 N 层用户数据提供机密性保护。

（3）选择字段机密性：这种服务为那些被选择的字段保证机密性，这些字段或处于 N 层连接的 N 层用户数据中，或为单个无连接的 N-SDU 中的字段。

（4）通信业务流机密性：通过这种服务提供的保护，使他人无法通过观察通信业务流推断出其中的机密信息。

4）数据完整性

数据完整性服务用于应付主动威胁。在一次连接中，连接开始时使用对某实体的鉴别服务，并在连接的存活期使用数据完整性服务就能为在此连接上传送的所有数据单元的来源提供确证，为这些数据单元的完整性提供确证。例如使用顺序号可为数据单元的重放提供检测。数据完整性按照完整程度分成下面5种：

（1）带恢复的连接完整性：这种服务为 N 层连接上的所有 N 层用户数据保证其完整性，并检测整个 SDU 序列中的数据遭到的任何篡改、插入、删除，还可能同时进行补救或恢复。

（2）无恢复的连接完整性：与上款的服务相同，只是不做补救或恢复。

（3）选择字段的连接完整性：这种服务为在一次连接上传送的 N 层用户数据中的选择字段保证其完整性，所取形式是确定这些被选字段是否遭到了篡改、插入、删除或不可用。

（4）无连接完整性：这种服务当由 N 层提供时，对发出请求的那个 $N+1$ 实体提供了完整保护。这种服务为单个的无连接的 SDU 保证其完整性，所取形式可以是一个接收到的 SDU 是否遭到了篡改。此外，在一定程度上也能提供对连接重放的检测。

（5）选择字段无连接完整性：这种服务为单个连接上的 SDU 中的被选字段保证其完整性，所取形式为被选字段是否遭到了篡改。

5）抗抵赖（否认）

抗抵赖服务可取如下两种形式或两者之一：

（1）有数据原发证明的抗抵赖：为数据的接收者提供数据的原发证据。这将使发送者不承认未发送过这些数据或否认其内容的企图不能得逞。

（2）有交付证明的抗抵赖：为数据的发送者提供数据交付证据。这将使接收者事后不承认收到过这些数据或否认其内容的企图不能得逞。

2. OSI 安全体系的安全机制

1）加密

如图1-4所示，加密是把可理解的明文消息通过密码算法变换成不可理解的密文的