实战网络安全

银石动力　编著

北京邮电大学出版社

·北京·

内 容 简 介

本书阐述了网络所涉及的安全问题，还通过实例、实训来增强读者的理解及动手能力。主要内容包括网络安全基础知识、物理与环境安全、操作系统安全、网络通信安全、Web 安全、数据安全、病毒及其预防、黑客攻击与防范、防火墙技术及有关网络安全的法律法规。

本书不仅适合应用型大学本科学生使用，同时也适合于对网络安全感兴趣的读者。

图书在版编目（CIP）数据

实战网络安全/银石动力编著.—北京：北京邮电大学出版社，2004

ISBN 7-5635-0853-8

Ⅰ.实… Ⅱ.银… 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 110421 号

书　　名： 实战网络安全

编　　著： 银石动力

责任编辑： 郭 弢　张学静

出 版 者： 北京邮电大学出版社（北京市海淀区西土城路 10 号）邮编：100876

发行部电话：（010）62282185　62283578（传真）

电子信箱： publish@bupt.edu.cn

经　　销： 各地新华书店

印　　刷： 北京通州皇家印刷厂

开　　本： 787 mm×1 092 mm　1/16

印　　张： 22.5

字　　数： 606 千字

印　　数： 1—3 000 册

版　　次： 2005 年 1 月第 1 版　2005 年 1 月第 1 次印刷

ISBN 7-5635-0853-8/TP・142　　定价：32.00 元

前　言

伴随着网络信息化建设的不断深入，网络安全问题已经越来越成为人们关注的焦点。建好了内外互联的网络，建好了繁杂的应用系统，安全问题就成为用户关注的头等大事。九一一事件是现实世界中的恐怖袭击事件。如果有一天，全世界的.com、.net等网站被袭击瘫痪，这将是网络世界中的九一一事件再版。然而，这样的事件不是不可能的。

在网络给人们带来便利生活的同时，也让人饱受安全问题的困扰：黑客的入侵使商业机密被竞争对手窃取，病毒的破坏使多年积累的宝贵数据毁于一旦，等等。据报道，自从互联网问世以来，已经遭到约63000种病毒的袭击，经济损失高达650亿美元，如何强化网络安全意识、提高网络安全技能已经成为刻不容缓的问题。

随着网络技术应用的日益广泛，对网络安全专业人才的需求也与日俱增，广大网络工程和管理人员以及个人网络用户也希望能找到一本迅速提高自己网络安全技能方面的书籍，本书正是应广大读者这一需求而创作的。书中全面介绍了网络安全的常见问题，针对各种问题均给出了详细的解决方法和防范措施，使读者遇到网络安全问题的时候不再感到手足无措。

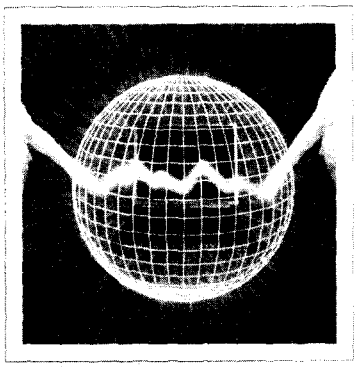
本书共分11章，从几个不同角度介绍了网络安全问题。第一部分（第一章）介绍了网络安全基础，讲述了网络安全的基本概念、安全体系结构等知识，第二部分（第二章至第五章）介绍了病毒和入侵及其防范措施等相关内容。其中，第二章介绍了目前比较流行的一些木马和病毒，第三章和第四章介绍了“黑客”入侵常用的方式，第五章介绍了注册表在网络安全方面的应用。第三部分（第六章至第十一章）介绍了防火墙的相关内容。其中，第六章介绍了网络安全的策略，第七章至第十章详细介绍了堡垒主机、数据包过滤和代理服务等防火墙相关知识，第十一章介绍了防火墙构筑的实例。

本书的适用范围较广，无论是个人用户还是局域网的安全防护在本书中均有介绍。本书和配套光盘是大中小型网络工程师的必备参考用书，可作为网络日常安全维护的指导用书，也可以作为各类网络培训机构和大中专院校相关课程的教材和参考用书。

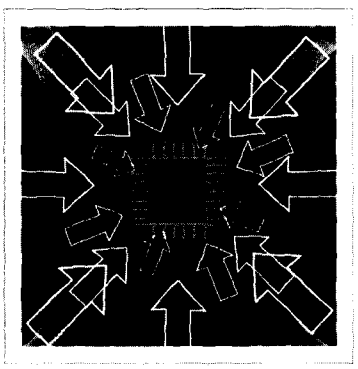
由于网络技术发展迅速，知识结构比较庞大，相关内容较多，疏漏之处在所难免，希望广大读者不吝指正。

作者

目　录



第一章 网络安全基础



本章从网络安全的基础开始，分别介绍网络安全的基本概念、相关知识以及一些网络命令的使用，通过这些内容的学习，读者可以对网络安全有一个基本的认识。

第一节 网络安全的基本概念

1.1.1 什么是网络安全

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不会由于偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可以连续正常地运行，网络服务不会中断。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，凡是涉及到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。

随着计算机技术的飞速发展，信息网络已经成为社会发展的重要推动因素。信息网络涉及到政府、军事、文教等诸多领域，其中存贮、传输和处理的信息有许多是政府重要的宏观调控决策、商业经济信息、银行资金转帐、股票证券、能源资源数据、科研数据等重要信息，有很多是敏感信息，甚至是国家机密。所以难免会吸引来自世界各地的各种人为攻击（例如信息泄漏、信息窃取、数据篡改、数据删添、计算机病毒等）。

所以网络安全是一个关系国家安全的重要问题。其重要性正随着全球信息化的不断加快而越来越受到人们的注意。网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性学科。

网络安全的具体含义会随着使用角度的变化而变化。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其机密性、完整性和真实性均受到保护，避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯自己的利益和隐私。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“后门”、病毒、非法存取、拒绝服务及网络资源非法占用和非法控制等威胁，制止和防范网络黑客的攻击。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，防止机要信息泄露，避免对社会产生危害，给国家造成重大损失。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。

1.1.2 网络安全的种类和特征

1. 网络安全的类型

网络安全由于不同的环境和应用而产生了不同的类型。主要有以下几种：

（1）运行系统安全，即保证信息处理和传输系统的安全。它侧重于保证系统正常运行，避免因为系统的崩溃和损坏而对系统存储、处理和传输的信息造成破坏和损失，避免由于电

磁泄漏，产生信息泄露，干扰他人或受他人干扰。

（2）网络上系统信息的安全。包括用户口令鉴别，用户存取权限控制，数据存取权限、方式控制，安全审计，安全问题跟踪，计算机病毒防治，数据加密等。

（3）网络上信息传播安全，即信息传播后果的安全，包括信息过滤等。它侧重于防止和控制由非法、有害的信息进行传播所产生的后果，避免公用网络上大量自由传输的信息失控 。

（4）网络上信息内容的安全。它侧重于保护信息的保密性、真实性和完整性，避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。其本质是保护用户的利益和隐私。

2. 网络安全的特征

网络安全的特征比较多，概括起来主要有以下四个方面：

（1）保密性：信息不泄漏给非授权用户、实体或过程，或不提供其利用的特性。

（2）完整性：数据未经授权不能进行改变的特性。即信息在存储或传输过程中保持不被修改、不被破坏和丢失的特性。

（3）可用性：可对被授权实体访问并按需求使用的特性。即当需要时能否存取所需的信息。例如网络环境下拒绝服务、破坏网络和有关系统的正常运行等都属于对可用性的攻击 。

（4）可控性：对信息的传播及内容具有控制能力。

1.1.3 TCP/IP 协议的安全问题

1. TCP/IP协议数据流采用明文传输

TCP/IP 协议数据流采用明文传输，用户的帐号、口令等重要信息也无一例外。攻击者可以截取含有帐号、口令的数据包进行攻击。所以这种信息传播方式无法保障信息的保密性和完整性。

2. 源地址欺骗（Source address spoofing）或 IP 欺骗（IP spoofing）

IP 协议依据 IP 头中的目的地址项来发送 IP 数据包。如果目的地址是本地网络内的地址，该 IP 包就被直接发送到目的地。如果目的地址不在本地网络内，该 IP 包就会被发送到网关，再由网关决定将其发送何处。这是 IP 路由 IP 包的方法。我们发现 IP 路由 IP 包时对 IP 头中提供的源地址不做任何检查，并且认为 IP 头中的源地址即为发送该包的机器的 IP 地址。当接收到该包的目的主机要与源主机进行通信时，它以接收到的 IP 包的 IP 头中源地址作为其发送的 IP 包的目的地址，来与源主机进行数据通信。IP 的这种数据通信方式虽然非常简单和高效，但它同时也是 IP 的一个安全隐患，很多网络安全事故都是因为 IP 的这个缺点引发的。

IP的这一安全隐患常常会使TCP/IP网络遭受两类攻击。最常见的一类是DoS（Denial-of-Service）攻击，即拒绝服务攻击。基本上这种攻击原理相当简单，就是针对某个网站或服务器的某个端口（如：80）进行大量数据包攻击，造成该网站或服务器无法提供相关的网络存取服务（如：浏览网页），如此便达到瘫痪该网站或服务器的运作，造成相关的商业或其他方面损失的目的。例如：2000年美国Yahoo网站被攻击至瘫痪而无法运作就是一个典型的例子。以TCP-SYN Flooding攻击为例，攻击者向被攻击主机发送许多TCP-SYN包。这些TCP-SYN包的源地址并不是攻击者所在主机的IP地址，而是攻击者自己填入的IP地址。当被攻击主机接收到攻击者发送来的TCP-SYN包后，会为这个TCP连接分配一定的资源，并且会以接收到的数据包中的源地址（即攻击者自己伪造的IP地址）为目的地址向目的主机发送TCP-（SYN+ACK）应答包。

由于攻击者自己伪造的IP地址一定是精心选择的不存在的地址，所以被攻击主机永远也不可能收到它发送出去的TCP-SYN包的应答包，因而被攻击主机的TCP状态将会处于等待状态。如果被攻击主机的TCP状态有超时控制的话，直到超时，为该连接分配的资源才会被回收。因此如果攻击者向被攻击主机发送足够多的TCP-SYN包，并且足够快，被攻击主机的TCP模块肯定会因为无法为新的TCP连接分配到系统资源而处于服务决绝状态。并且即使被攻击主机所在网络的管理员监听到了攻击者的数据包也无法依据IP头的源地址信息判定攻击者是谁。不单是TCP-SYN Flooding攻击者在实施攻击时自己填入伪造的IP源地址，实际上每一个攻击者都会利用IP不检验IP头源地址的特点，自己填入伪造的IP源地址来进行攻击，使自己不被发现。

IP的不进行源地址检查还常常会使TCP/IP网络遭受另一类最常见的攻击，即劫持攻击。

攻击者通过攻击被攻击主机获得某些特权。这种攻击只对基于源地址认证的主机奏效，基于源地址认证是指以IP地址作为安全权限分配的依据。以防火墙为例，一些网络的防火墙只允许本网络信任的网络的IP数据包通过。但是由于IP不检测IP数据包中的IP源地址是否为发送该包的源主机的真实地址，攻击者仍可以采用IP源地址欺骗的方法来绕过这种防火墙。另外有一些以IP地址作为安全权限分配的依据的网络应用，攻击者很容易使用IP源地址欺骗的方法获得特权，从而给被攻击者造成严重的损失。

解决方法：这一IP本身的缺陷造成的安全隐患目前是无法从根本上消除的，只能采取一些弥补措施来使其造成的危害减少到最小的程度。防御这种攻击的最理想的方法是：每一个连接局域网的网关或路由器在决定是否允许外部的IP数据包进入局域网之前，先对来自外部的IP数据包进行检查。如果该IP包的IP源地址是其要进入的局域网内的IP地址，该IP包就被网关或路由器拒绝，不允许进入该局域网。这种方法虽然能够很好地解决问题，但是考虑到一些以太网卡接收他们自己发出的数据包，并且在实际应用中局域网与局域网之间也常常需要有相互的信任关系以共享资源，这种方案不具备太高的实际价值。另外一种较为理想的防御方法是当IP数据包发出局域网时检验其IP源地址，即每一个连接局域网的网关或路由器在决定是否允许本局域网内部的IP数据包发出局域网之前，先对来自该IP数据包的IP源地址进行检验。如果该IP包的IP源地址不是其所在局域网内部的IP地址，该IP包就被网关或路由

器拒绝，不允许该包离开局域网。这样一来，攻击者至少需要使用其所在局域网内的IP地址才能通过连接该局域网的网关或路由器。如果攻击者要进行攻击，根据其发出的IP数据包的IP源地址就会很容易发现谁实施了攻击。因此建议每一个ISP或局域网的网关或路由器都对出去的IP数据包进行IP源地址的检验和过滤。如果每一个网关或路由器都做到了这一点，IP源地址欺骗将基本上无法奏效。在当前并不是每一个网关或路由器都能做到这一点的情况下，网络管理员只能将自己管理的网络置于尽可能严密的监视之下，以防备可能到来的攻击。

3. 路由选择欺骗（Source Routing spoofing）

与路由器源路由攻击方法一样，在TCP/IP协议中，为测试目的，IP数据包设置了一个选择：IP Source Routing，该选项可以直接指明到达节点的路由。攻击者就利用这个选项进行欺骗，进行非法连接。攻击者冒充某个可信节点的IP地址，构成一个通往某个服务器的直接路径和返回路径，利用可信用户作为通往服务器的路由中的最后一站，就可向服务器发送请求，对其进行攻击。在TCP/IP协议的两个传输层协议TCP和UDP中，由于UDP是面向非连接的，因而没有初始化的连接建立过程，所以UDP更容易被欺骗。

4. 路由选择信息协议攻击（RIP Attacks）

RIP协议用来在局域网中发布动态路由信息。它是为了在局域网中的节点提供一致路由选择和可达性信息而设计的。但是各节点对收到的信息并不检查其真实性（TCP/IP协议没有提供这个功能），因此攻击者可以在网上发布假的路由信息，利用ICMP的重定向信息欺骗路由器或主机，将正常的路由器定义为失效路由器，从而达到非法存取的目的。

5. 鉴别攻击（Authentication Attacks）

利用TCP/IP协议只能识别IP地址的缺陷，攻击者通过窃取口令从该节点上非法登录服务器。

6. TCP序列号欺骗（TCP Sequence number spoofing）

由于TCP序列号可以预测，因此攻击者可以构造一个TCP包序列号，对网络中的某个可信节点进行攻击。

7. TCP序列号轰炸攻击（TCP SYN Flooding Attack），简称SYN攻击

TCP是一个面向连接、可靠的传输层协议。黑客可以不断向服务器发送连接请求，而又不返回应答包，使得服务器总处于等待状态，而无法释放资源。

第二节 OSI安全体系结构

国际标准化组织（ISO）已经提出一个建议性标准（DIS7498-2，OIS参考模型第二部分：安全性体系结构）、ISO把它作为开放系统互联（OIS）标准的一部分。在安全性方面，它可以提供重要的指导作用。DIS7498-2包括以下内容：

（1）重要安全性要点清单

（2）为组织提供安全性任务而给予的帮助

（3）为实施者和购买者提供的指南

（4）标准化安全性实施的办法

ISO的这一标准的两个根本目的是：

（1）为OSI各层提供安全性要点的功能分配，从而指导基于OSI标准的改进。

（2）提供一个供应商和消费者都可以进行安全性评估的机构框架。

在OSI标准提供的框架中，还定义了安全性服务和安全性机制。为了理解OIS安全性体系结构，我们按照安全性威胁、安全性服务和安全性机制三部分来讨论。

1.2.1 安全性威胁

损害一个机构或个人所拥有信息的安全的行为称做安全性威胁。安全性威胁有两种类型：被动威胁和主动威胁。对这两种威胁的处理方法稍有不同。

1. 被动威胁

通常被动威胁不改变系统中的数据，或者说，被动威胁只是读取系统中的信息，以从中获取利益。由于没有自发信息，被动威胁留下的痕迹很少，或者根本没有留下痕迹，因而很难发现被动威胁。然而，被动威胁通常是可以预防的，而且预防也是对付这种威胁的基本手段。

在一个网络中，被动威胁包括两个方面：侵入者获取系统泄露的消息内容，或者通过读数据包头（通信量分析）以确定信源方和目的的位置和身份。当然，如果一条信息已经存放在主机系统的文件中，那么被动威胁可能导致入侵文件系统来获取已经存储的信息。

对付被动威胁的主要方法是采用加密技术，如果没有解密密钥，所获得的信息是看不懂的。加密是通过使用代码或密码来实现的。代码使用一个预定义的表来替换每条消息或消息的某一部分中的每个词或句子。与之相比，密码使用一个算法将数据信息译成难以破译的密文。密码技术可以容易地实现自动化，因而常常被计算机和网络安全系统所采用。常规的加

密方法将原始数据转换成难懂的密文。要实现这一转换，需要用到一个算法和控制这一算法的密钥。密钥由位串组成。发送者和接收者都要拥有密钥，因而密钥的管理也成为一个问题。算法必须要有足够的复杂度，以排除从密文中破译出信息的可能。

从网络安全的角度看，有两种基本的加密方法：链路加密和端到端加密。链路加密指数据的加密独立于通信链路。这种链路对于简单的网络来说，可能是端到端的连线。链路加密的优点是整个分组（包括分组头信息）都被加密，因而传输的是密文。其缺点是中间节点的数据是明文，由此产生了节点安全性问题，因此用户很难或者根本无法控制其安全性。端到端的加密发生在数据分组的源地址和目的地址处。这种加密方法照顾了中间节点的数据安全，但数据分组是未经加密的明文。使用这两种加密方法的混合系统是最安全的，数据分组头只在端点和中间节点是明文，而数据信息永远不会是明文。对端到端的加密方法稍做变化，即在一个加密的文件中永久存放数据，这种系统可用于替代或补充以上两种加密方法。

密钥管理的任务是在一个密码系统中控制密钥的选择和分配。密钥是一段数字信息，它与加密算法相互作用，以控制信息的加密，因此密钥必须妥善保护以防泄漏。在常规的加密系统中通信链路的两端都有一份密钥的拷贝，因此有损害安全性的可能。通过经常更换密钥，可以把这种损害降低到一定限度内。公开密钥密码系统可以替代常规的加密方法，这种加密方法要用到两个密钥：一个公用密钥用于加密过程，任何一个想加密信息的人都可以使用密钥；另一个私用密钥用于解密过程，该密钥只被它的所有者所知晓。

加密/解密的传统方法是使用一个对称算法，在这个算法中加密信息的发送者和接收者要求拥有相同的密钥。对称算法的缺点在于算法和密钥必须保密。此外，密钥必须从一个人传送到另一个人，因而产生了安全性威胁。然而，该算法的主要优点是可以建立某种鉴定系统，以减少由于伪造信息所带来的问题。替代上述算法的一种新方法——非对称加密系统，最早出现在1976年，公开密钥算法就是这一方法的派生物。非对称系统的优点是，第二个密钥，即解密密钥，只被接收者知晓，并且接收者需要进行解密计算。在这样的系统中，加密/解密算法以及加密密钥可以是公开的。解密密钥与加密密钥是有关系的，但它们实际上是一个巨大的密钥空间中的一个随机样本，以现在的科技水平无法通过一个密钥算出另一个密钥。

使用最广泛的算法是数据加密标准（DES），DES是一种算法，它在电子硬件设备上实现，用来为数学的，二进制编码的信息做加密。需要注意的是，加密往往是发生在OSI模型中的物理层，而解密可以用于任何一层或者所有层上。

被动威胁的第二种形式与信息量分析安全性有关。如果一个入侵者可以阅读数据包头，那么他就可以得知数据的源地址和目的地址，即使消息是加密的。使用链路加密，可以降低或消除这种可能性。加密只可能限制阅读头信息和消息，有些重要的信息可以从通信量分析中得到。例如，可以得到进入或离开某个中间节点的通信总量，加密不能解决这个问题。一个可能的对策是，通过生成持续的随机数流或密文流来填充通信链路，使侵入者很难区分有用的数据与无用的噪声，从而使计算实际的通信总量十分困难，或根本不可能。

2. 主动威胁

我们可以预感到，主动威胁通常要比被动威胁更加严重，因为主动威胁并不是简单的读取数据信号的内容，它常常有意的改动数据控制信号，或者有意的生成伪造的数据。不过主动威胁是否一定要比被动威胁更加严重，还要看这种威胁所造成的损害程度，举个例子来说，贸易机密或国防机密的失窃，即便没有任何改动，也会造成巨大的损失，这种被动威胁要比许多主动威胁严重得多。对于主动威胁，我们所关心的问题是：消息服务的破坏、假冒和消息流的修改。

主动侵入可能发生在通信路线上的几乎任何地方，电缆、微波链路、卫星通道、路由节点、主机或客户计算机系统都可能成为主动侵入的对象。除非像在军事建设中那样在安全性方面投入大量的资金，否则对整个线路设置广泛的物理防范设施是不可能的。事实上，即使在军事机构中，百分之百的保护也是不可能的。然而，无论用何种方法，主动威胁只有在实现物理访问时才能进行。在这种情况下，我们对“物理”的理解应该广泛一些，因为这种物理访问可能是在几百英里之外的一个目标通过拨号访问终端进行的，或者某个远程目标通过无线电信道进行的，而线路刺探（一种未经授权就与通信线路进行连接并对数据进行非法访问的行为）甚至并不需要由一台设备和电缆进行物理的连接。因此我们可以想象，阻止主动侵入是非常困难的，所以挫败主动侵入的安全性目标只能是，迅速检测和恢复由于这种侵入而造成的信息延误和系统瓦解。

第一种侵入方式是破坏或者延误大部分甚至全部信息，这是一个通信体系所面临的最明显的主动威胁。在现代信息社会里，发生这样的事件很容易导致大量资金的损失，甚至更为严重 。

另一种更加巧妙的主动威胁方式是假冒。假冒是一种通过假装成授权的客户或主机来获得系统访问权的侵入方式。在这种情况下，侵入者假装成一个真正的主机、开关、路由器或类似设备，旷日持久的等待与对等用户进行通信以获得数据或服务。努力的假装成一个真正的用户是一种老式的、没有道德的行为，其目的是使目标系统真正相信正与它进行通信的确实是它所希望的主机或客户。假冒作为一种技术，既可以用于被动目的，也可以用于主动目的。之所以把它说成是“主动威胁”是因为它常常具有干扰和破坏性质。

主动威胁的第三种方法是修改消息流。在这种情况下，入侵者可能对消息进行有选择的修改、删除、延误、重排序，以及复制真正的消息或插入虚假的消息。如果阻碍了数据分组中CRC差错校验码的传输，即使是加密的消息也可能受到破坏。用于传输的数据包是由协议软件形成的，它需要有一个或多个循环冗余校验和，该校验和要经过发送方的计算和接收方的再计算，如果发送方和接收方的校验和不同，通常需要重传该数据包。用于此类的方法是，可以在加密以前对消息内容的明文生成一个操作检验码（MDC），这样即使数据包被改动，也可以通过差错纠正测试。但是，被加密的明文也可能被修改以形成一个不同的校验和。MDC只是检测消息流修改的一种方式，同样存在几种其他的校验方式，这种方法被统称为MAA（信息鉴别算法）。

1.2.2 安全性服务

安全性服务用于增强一个系统或组织的信息传输的安全性。在OIS模型中，定义了5组服务：机密性、鉴别、完整性、无拒绝和访问控制。在一个分层通信体系结构（如OSI模型）中，安全性服务几乎可以建立在任何地方。OSI安全性体系机构更加明确，它规定了每一层要提供的特定服务。安全性服务与OSI各层之间的关系可参见表1-2-1。

表1-2-1　安全性服务与OSI各层之间的关系

OSI各层	机密性	通信流量的机密性	鉴别	完整性	无拒绝	访问控制
应用层	Y	Y	Y	Y	Y	Y
表示层	Y	Y	Y	–	Y	Y
会话层	–	–	–	–	–	–
传输层	Y	–	Y	Y	–	–
网络层	Y	Y	Y	Y	–	Y
数据链路层	Y	–	–	–	–	–
物理层	Y	Y	–	–	–	–

机密性保证数据不能被未经授权的个人、实体或进程所访问。一般来说，这种服务可以提供一种保护数据传输不受被动侵入的机制。机密性的概念可以应用于整个消息或者消息内的字段，在后一种情况中经常采用选择字段机密性这一术语。通信协议所使用的服务类型对数据机密性会产生不同的影响。面向连接的服务建立一个虚拟连接，对用户来说好像有一条实际的端到端的电路，这种服务有时成为虚拟电路或虚拟连接。与面向连接的服务相对的是无连接服务，无连接的服务是一个服务类，它并不建立一条虚拟的或逻辑的连接，也不保证数据单元一定以特定的顺序进行传输，无连接的服务是灵活的、健壮的，并提供无连接的应用支持。无连接的应用需要路径服务，但不需要面向连接的服务。

鉴别可以保证接收到的数据是正确的、一致的。鉴别还包括对诸如远程终端上的人员身份的核实。数据源鉴别要确认所收到的数据的源方是否是所要求的。对等实体鉴别确认所关联的对等实体是否是所要求的。OIS更加清楚的强调了鉴别的概念，OIS中的鉴别特指证实接收的数据就来自所要求的源方。数据源鉴别连同无连接的服务一起操作，而对等实体鉴别通常与面向连接的服务一起操作。在其他的模型中，鉴别的概念可能和数据完整性混为一谈，但是在OSI中，这两者是有明显区别的。

数据完整性可以保证数据没有以未经授权的方式被改动或者破坏。数据完整性和鉴别这两个概念结合得非常紧密，即便在OSI中也是如此。这种结合还延伸到支持服务的机制中。从表1-2-1中可以看到，数据完整性服务和鉴别服务的机制是相同的，它们都很强的依赖于把加