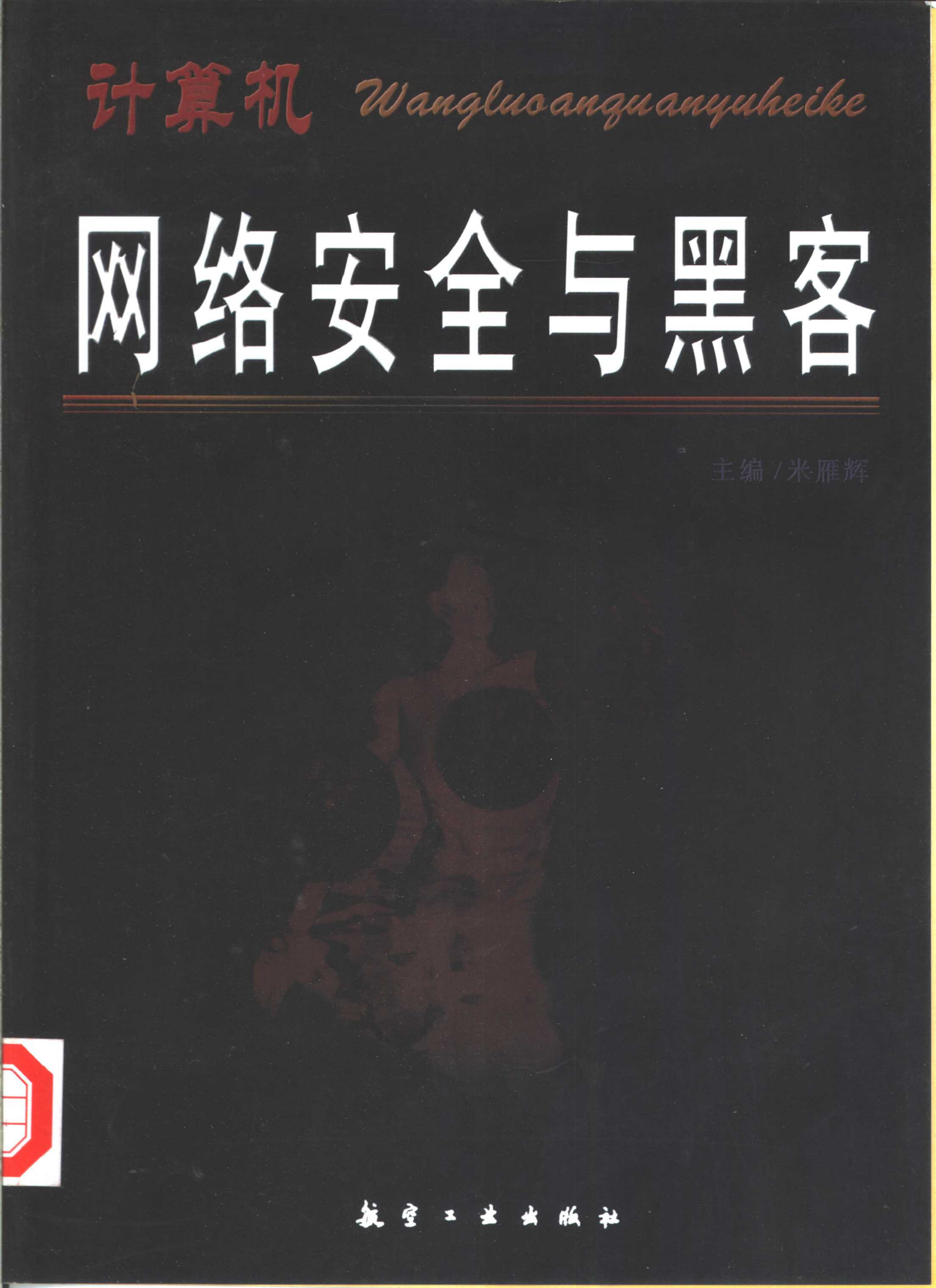
计算机 Wangluoanquanyuheike

# 网络安全与黑客

主编/米雁辉



航空工业出版社

# 网络安全与黑客

主 编　米雁辉

航空工业出版社

## 内 容 提 要

本书共分为 7 章。第 1 章介绍了黑客与网络安全的基础知识。第 2 章以具体的实例介绍了黑客攻击别人计算机的手法。第 3 章详细介绍了防火墙的基本概念以及如何选择和组建防火墙来保护用户的计算机系统。第 4 章讲解了如何利用 Windows NT 和 UNIX 操作系统来配置各项网络安全设置，以防黑客的攻击。第 5 章通过大量的实例阐述如何维护数据库系统的安全。第 6 章详细讲解了各种网络协议安全以及计算机的加密技术。第 7 章介绍了如何使用各种网络安全工具，并辅以大量的使用实例加以说明。

本书既可作为计算机初学者的入门教材，也可作为计算机网络专业人员的参考书。

**图书在版编目（CIP）数据**

网络安全与黑客 / 米雁辉主编.
—北京：航空工业出版社，2001.1
ISBN 7-80134-794-3

Ⅰ.网… Ⅱ.米… Ⅲ.计算机网络-安全技术-基本知识
Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字（2000）第 78057 号

航空工业出版社出版发行
(北京市安定门外小关东里 14 号 100029)
北京云浩印刷厂印刷　　全国各地新华书店经售
2001 年 2 月第 1 版　　2001 年 2 月第 1 次印刷
开本：787×1092　1/16　　印张：14.5　　字数：298 千字
印数：1-8000　　定价：21.00 元

本社图书如有缺页、倒页、脱页、残页等情况，请与本社发行部联系调换。联系电话：010-65934239 或 64941995

# 前　言

自从 1981 年 IBM 型计算机诞生之后，计算机在功能不断增加的前提下，体积、耗能、成本大大降低，从而进入了社会的各个领域。在我国，计算机的发展速度也相当快，目前计算机的拥有量呈直线上升之势。计算机的发展无疑将给我们带来现代化的社会、科学化的管理和高效率的工作和生活，促使我们进入一个新时代——信息时代。

但是，由于越来越多的涉及国家军政、经济、工商情报以及一些私人数据等敏感信息都是通过计算机来进行处理，因此，一旦计算机运行失灵或泄漏了所存储的信息，轻则延误工作，重则使国家安全及人民生命财产安全遭受不可估量的损失。尤其是随着计算机网络的发展，使得计算机黑客更加容易通过非法手段攻击别的计算机，从而达到他们的非法目的。

本书正是围绕着计算机网络安全这个中心主题，从描述计算机网络系统所面临的安全问题入手，讨论如何建立一个安全的计算机网络系统来避免遭受计算机黑客的攻击，同时还通过各种实例说明了黑客常用的攻击手段和方法。全书包括七部分内容：

- 计算机网络安全概述
- 黑客技术介绍
- 防火墙技术及虚拟专用网
- 计算机操作系统安全访问和控制
- 数据库系统安全
- 网络协议安全及加密技术
- 网络安全工具

各个部分的内容都通过非常丰富及栩栩如生的实例来进行讲解，让读者能够即学即用，因此本书非常适合初、中级计算机爱好者使用，同时也可作为网络专业人员的参考书目。

本书由阿勇工作室编写，米雁辉主编。由于编者水平有限，本书疏漏与错误之处在所难免，敬请读者批评指正。

编　者

2000 年 11 月

# 目 录



此为试读，需要完整PDF请访问：www.ertongbook.com

# 第 1 章　计算机网络安全概述

在现代社会中，大量的数据信息被收集和存储在大型的计算机数据库中，并在与综合通信网相连的计算机以及终端设备之间相互传送。如果计算机用户没有适当的安全措施，这些信息在传输过程中就易被截收，或在存储时被取出和复制，造成信息的泄露，产生保密隐患。并且，信息在存储和传输期间还会受到非法删除、更改或增添，从而导致对计算机资源及计算机服务的非法干预与使用。

与此同时计算机本身固有的脆弱性也在不断地被利用，如计算机硬件设备易受自然灾害与人为灾害的破坏。如果计算机硬件受到外界电磁场的干扰，也很容易破坏系统的正常运行，导致大量信息出错或者丢失。

计算机网络系统软件也易受到各种各样的攻击，如有的软件可以很容易被非法复制。国家的金融、商业、科研及军政等诸多部门中已使用了大量的计算机网络系统。对于计算机网络系统中的机密信息、个人数据以及工商业机密情报等必须采取很有效的安全防范措施，否则这些信息一旦被窃取或删改，对计算机用户将引发难以估量的损失。

## 1.1　计算机网络系统安全的本质

随着计算机网络在现代社会各个领域的广泛应用，计算机网络的安全问题已显得日益突出。计算机网络的主要作用是各节点间各种软、硬件资源的共享。当资源共享广泛应用于政治、军事、经济以及科技各个领域时，在计算机网络上传输和存储的大量信息都需要保护。

实际上，计算机网络可以看成一个比较复杂的计算机操作系统。因此，许多能够用于计算机操作系统的各种安全控制方法同样也适用于计算机网络。如同在操作系统中那样，一个安全的计算机网络必须满足保密性和完整性的安全要求。但是，由于计算机网络可以看成是许多分离计算机通过通信子网联接起来的一个复杂系统。为了能够达到各种软、硬件资源共享的目的，所以计算机网络的保密性不仅涉及计算机信息存放的保密性，更重要的是要考虑到信息传输的保密性。同样，信息的完整性不仅要考虑信息修改、删除、替换，还要考虑信息的相互插入和它们次序的重新排列。

一个安全的计算机网络不仅要具有很高的保密性和完整性，而且必须考虑通信双方的真实性，这就是说，必须具有某种双方都认可的方式对计算机网络通信双方进行相互确认和鉴别。比如当计算机网络用于各个不同的银行之间进行电子资金转账业务时，账号的确认与鉴别就是十分紧迫重要的问题。

### 1.1.1　网络安全的重要性及安全模型

计算机网络每天都会遇到各种各样的威胁，这些威胁来自各个方面，有各种自然灾害引起的，也有计算机自身的弱点以及各种失误产生的，还有各种设施、设备的失常造成的。这些威胁的一个共同特点是其偶然性。对于这种威胁，一般可以采取一定的预防措施，以

尽量避免这些意外事件的发生或者减少事故发生后的损失。另一类威胁则是来自人为的威胁。人为威胁的目的就是要使对方蒙受损失或使自己获得某种非法利益。

一个计算机网络系统涉及到很多因素，比如人、各种设施与设备、计算机网络系统软件与应用软件、计算机网络系统内存储的数据、各种供给品等。计算机网络系统安全的本质就是要保证各方面因素能够发挥它们的正常作用。它包括以下几方面的内容：

- 要明确计算机网络系统的脆弱性与它的弱点。
- 要估计到对计算机网络系统的各种威胁，以及存在的各种特殊问题。
- 要保护系统内的各种资源不遭到自然与人为的破坏。
- 要开发与实施卓有成效的安全策略，尽可能减小系统所面临的各种风险。
- 要经常检查各种安全管理措施的实施情况与有效性。
- 要准备适当的应急计划，使系统遭到破坏或攻击时能够尽快恢复正常工作。

不同的计算机网络系统有不同的安全要求，这要根据它的作用以及在受到破坏与攻击时所造成的损失来决定，其安全要求并没有一个统一的标准。从理论上讲，一个计算机网络系统越安全越好。但是要根据用户的实际情况采取相应的措施，使系统的性能价格比达到一个合理的水平。

网络安全技术是一门新型学科，许多方面还不是很成熟。为了适应计算机网络技术的发展，国际标准化组织（ISO）的计算机专业委员会（ISO / IEC JTC1/SC21）根据开放系统互连参考模型（OSI / RM）制定了一个网络安全体系结构（ISO 7498-2N），该模型主要解决对网络系统中的传输信息进行保密的问题。

为了实现 OSI 环境下的信息安全，ISO 的计算机专业委员会从开放系统互连的体系结构入手，在 OSI / RM 模型中增设了对安全机制、安全服务和安全管理的描述。

### 1. OSI 安全体系结构要求的安全服务

OSI 安全体系结构包括不同的安全服务。这些服务可能包含在体系结构中，也可能包含在体系结构的服务和协议的实现中。针对计算机网络系统受到的威胁，OSI 安全体系结构提出了六类安全服务。

（1）对等实体鉴别服务

这种服务是在两个计算机网络开放系统同等层中的计算机实体建立连接和数据传送期间，为提供对连接计算机实体身份的鉴别而规定的一种服务。这种服务防止假冒计算机实体或重放以前的连接，也即防止伪造连接初始化这种类型的黑客攻击。这种鉴别服务可以是双向的，也可以是单向的。

（2）数据源鉴别

这是计算机网络传输协议中第 N 层向第 N＋1 层提供的服务。主要用来确保数据是由合法的计算机实体发出的，它为第 N＋1 层提供对数据源的对等实体进行鉴别。

（3）禁止否认

这种服务用来防止发送方在发送数据后又否认自己曾经发送过数据，或接收方在收到数据后否认自己曾经收到过数据。该服务由以下两种服务组成：

- 不得否认发送。这种服务向数据接收者提供数据源的证据，从而可防止发送者否认发送过数据。
- 不得否认接收。这种服务向数据发送者提供数据已交付给接收者的证据，因而接

收者事后不能否认曾收到数据。

实际上，上面这两种服务是一种数字签名服务。

（4）访问控制

计算机网络访问控制服务可以防止没有被授权的用户非法使用计算机系统资源。这种服务不仅对单个用户使用，也可以对一个封闭的用户组中所有的用户使用。

（5）数据完整性

这种服务用来防止非法计算机实体的主动攻击，如对正在交换的数据进行修改、插入，使数据延时以及丢失数据等，从而能够保证接收方收到的信息与发送方发送的信息完全一致。具体提供的数据完整性服务有以下几种：

- 可恢复的数据连接完整性。该服务对一个连接上所有用户数据的完整性提供保障，而且对任何服务数据单元的修改、插入、删除或重放都能够使之复原。
- 数据无连接完整性。该服务提供单个无连接数据单元的完整性，能确定收到的数据单元是否已被修改。
- 选择字段数据无连接完整性。该服务提供单个无连接数据单元中各个选择字段的完整性，能确定选择字段是否被修改。
- 选择字段的数据连接完整性。该服务提供在连接上传送的选择字段的完整性，并能确定所选字段是否已被修改、插入、删除或重放。
- 无恢复的数据连接完整性。该服务除了不具备恢复功能外，其余的功能与前面的几个服务相同。

（6）数据保密

数据保密服务的目的是保护网络中各系统之间交换的数据，防止因数据被截获而造成的泄密。这种服务包括以下内容：

- 选择字段保密。即对一个协议数据单元中的用户数据的一些经选择的字段提供保密。
- 连接保密。即对某个连接上所有的用户数据提供保密。
- 信息流安全。即对有可能从观察信息流就能推导出的信息提供保密。
- 无连接保密。即对一个无连接的数据包的所有用户数据提供保密。

### 2. OSI 安全体系结构要求的安全机制

为了实现上述各种服务，安全体系结构建议采用以下六种安全机制。

（1）交换鉴别机制

交换鉴别是以交换信息的方式来确认实体身份的机制。用于交换鉴别的技术有：

- 口令。由发方计算机提供，收方计算机检测验证。
- 密码技术。将需要交换的数据加密，只有被授权的合法计算机用户才能解密数据，从而得出有意义的明文。

在许多情况下，这种技术与下列技术一起使用：时间标记和同步时钟；双方或三方“握手”；数字签名和公证机构。利用计算机实体的特征或所有权，常采用的技术是指纹识别和身份验证卡等。

（2）访问控制机制

访问控制机制是按事先确定的规则决定计算机主体对计算机客体的访问是否是被授权合法的。比如，当一个计算机主体试图非法使用一个未经授权使用的计算机客体时，该机

此为试读，需要完整PDF请访问：www.ertongbook.com

制将拒绝这一非法行为，并附带向计算机的审计跟踪系统报告。同时计算机的审计跟踪系统将产生报警信号或形成部分追踪审计信息。计算机网络上的访问控制机制与单个计算机网络系统上访问控制机制相类似。

（3）数字签名机制

数字签名机制是解决计算机网络通信中安全问题的一种很有效方法。当计算机通信双方发生下列情况时，就会产生以下的安全问题：

- 否认。发送者事后不承认自己发送过某份文件。
- 篡改。接收者对收到的信息进行部分篡改。
- 冒充。网上的某个用户冒充另一个用户接收或发送信息。
- 伪造。接收者伪造一份文件，声称它发自发送者。

通俗地说，在网络中采用数字签名机制解决通信中的安全问题，就如同日常生活中用手写签名的办法一样。

（4）加密机制

加密机制是提供数据保护的最常用的方法。按密钥类型分，加密算法可分为：对称密钥加密算法和非对称密钥加密算法（或者叫做公共密钥）两种；按密码体制分，又可分为：序列密码和分组密码两种。用加密的方法与其他技术相结合，可以提供数据的保密性和完整性。除了在传输协议对话层的计算机网络系统不提供加密保护外，加密机制可在传输协议的其他各层上进行。

（5）数据完整性机制

数据完整性包括两种形式：第一种是数据单元的完整性；第二种是数据单元序列的完整性。

数据单元的完整性包括两个过程：首先是发生在发送计算机实体，然后是发生在接收计算机实体。保证数据单元完整性的一般方法是：发送计算机实体在数据单元上加一个标记，这个标记可以是数据本身的函数，如一个分组校验（类似于 CRC 校验），或密码校验函数，同时它本身是经过加密的。接收计算机实体同时也产生一个对应的标记，并且将所产生的标记与接收的标记相比较，用来确定在传输过程中计算机信息数据是否被修改过。

数据单元序列的完整性是要求数据单元的编号具有连续性和时间标记的正确性（传送的数据单元不会是过时的），用来防止假冒、丢失、重发、插入或修改过数据单元列。

（6）公证机制

在一个大型的计算机网络中，有许多节点或端节点。所以在使用这个网络时，并不是所有的用户都是诚实的、可信的，同时也可能由于计算机系统故障等原因使信息丢失、迟到等，这很可能会引起各种责任问题。为了解决这个问题，就需要有一个各方都信任的实体——公证机构，如同一个国家设立的公证机构一样，提供公证服务，对出现的问题进行公正的仲裁。

一旦引入公证机制，通信双方在进行数据通信时必须经过这个机构来交换，以确保公证机构能得到必要的信息，供以后仲裁用。

### 3. OSI 安全服务和 OSI 安全机制在网络中的位置

安全服务和安全机制不是一一对应的。有的服务需要由多种机制提供，而有的机制可用于多种服务。还必须指出，安全服务是由相应层的相应安全机制提供的，一种安全服务

不是在所有各层中都能实现。

如果把安全机制按上段中的顺序编号如下：①数据加密；②数字签名；③访问控制；④数据完整性；⑤交换鉴别；⑥公证机制。那么，安全服务机制在网络七层中的位置可以归纳如表 1-1 所示。

表 1-1　安全服务和安全机制在网络七层中的位置

| | 物理层 | 链路层 | 网络层 | 传送层 | 对话层 | 表示层 | 应用层 |
|---|---|---|---|---|---|---|---|
| 对等实体鉴别 | | | ①②⑤ | ①②⑤ | | ①②⑤⑥ | ①②⑤⑥ |
| 访问控制 | | | ③ | ③ | | ③ | ③ |
| 连接的保密性 | ① | ① | ① | ① | | ① | ① |
| 连接字段的保密性 | | ① | ① | ① | | ① | ① |
| 报文流的完整性 | ① | | ① | | | | ① |
| 数据的完整性 | | | ①②④ | ①②④ | | ①②④ | ①②④ |
| 数据源鉴别 | | | ①②④ | ①②④ | | ①②④ | ①②④ |
| 禁止否认服务 | | | | | | ①②④⑥ | ①②④⑥ |
| 安全机制统计结果 | ①⑥ | ① | ① | ①~⑤ | | ①<br>⑥ | ①<br>⑥ |

从表中可以看出，在网络层，除了不提供禁止否认服务外，可提供所有其他的安全服务，除了不利用公证机制之外，采用了所有其他的安全机制。在表示层，除了不提供报文流安全服务外，可提供所有其他的服务。在应用层，有些应用实体是系统提供给所有用户使用的；有些应用实体是用户自己开发、供特定用户专用的，因此，这一层的安全服务一般都是专用的，因人因事而异，而采用的安全机制也相应不同。不过，应用层在原则上可以提供所有的安全服务。

## 1.1.2　计算机网络数据的保密性

从表 1-1.中可以看出，除了对话层外，在网络的其余六层几乎都可以采用加密机制为网络提供安全服务。如同在操作系统和数据库那样，加密是提供网络的保密性、完整性和真实性，并对数据访问进行控制的强有力手段。由于计算机网络本身分散的特点，在计算机网络中采用加密机制对传送的数据信息进行保护尤为重要。

本小节首先着重分析在表示层和应用层中实现的端到端加密方式与可在传输协议中的物理层和链路层中实现的链路加密方式。然后，简单介绍传送层中采用的一种端到端加密方式，并说明这种端到端加密方式与表示层和应用层中的端到端加密方式的区别。接着，较为详细地介绍网络中保障通信真实性的一种方法——数字签名。

### 1. 端到端加密方式

端到端加密是在网络表示层或应用层上进行的加密。表示层的主要任务是对不同系统采用的数据表示形式进行转换，使异种数据表示形式转换成本系统可识别的数据表示形式

（例如，EBCDIC 码与 ASCII 码之间的转换）。数据加密本身也是一种对数据的变换，把它放在表示层中很容易实现。如图 1-1 所示。

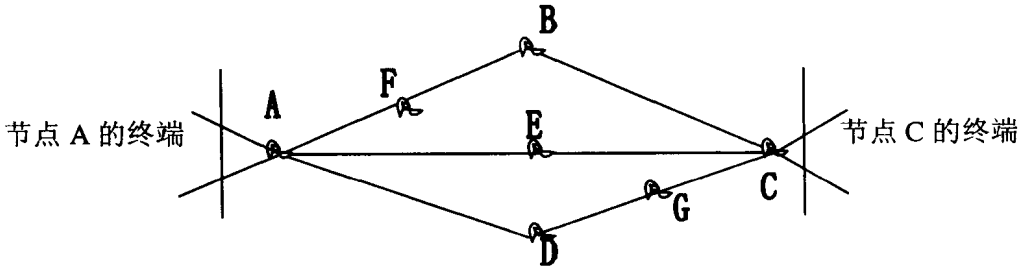



图 1-1 网络拓扑结构实例

当节点 A 的终端要与节点 C 的终端进行计算机数据通信时，首先将要发送的计算机数据加密发往节点 A，节点 A 根据网络的信息流量和最短路径决定路由器把收到的数据原封不动地转发给下一个节点，比如说是 E，然后节点 E 把它再原封不动地转发给节点 C。节点 C 收到这个加密数据后，再把它原封不动地转发给终端上，被加密的数据才能解密，还原成明文。

由于被传输的信息在应用层或表示层就被加密。因此信息在进入通信子网之前就已加密，在网络中传输时，不论是在物理线路上还是在中间节点主机上，信息本身都始终处于加密状态。而到达目的节点之后，信息也没有被立即解密，同时也不必对中间节点及中间节点上的操作人员提出特别要求。但是这种加密方式中的缺点是同时供网络确定报文目的地的编址信息和一些必要的网络控制信息，例如，路由信息、信息帧的格式等是以明文方式出现在通信线路上，从而不能避免入侵者对网络信息流的分析和篡改报文路由之类的主动攻击。

### 2. 链路加密方式

链路加密方式是一种把数据置于物理通信链路之前对数据进行加密的方式。因此，它既可以应用在网络的物理层，也可以应用在数据链路层。

随着信息技术的发展，网络黑客可以轻易地从有线和无线通信的信道中窃得有用的信息。因此，采取链路加密措施是十分必要的。要想防止入侵者对网络进行业务流分析，以及要想对网络口令、控制信息进行保护，只有进行链路加密才能达到目的。因为这些信息属于网络第 1 层和第 2 层中特有的信息，在其他层次加密不能对它们起到保护作用。

链路加密是对网络相邻节点之间（包括端节点与相邻节点之间）在通信线路上传输的数据进行保护。加密/解密发生在两个网络节点间（或端节点与相邻节点之间）通信线路上的两个保密设备之中，这两个保密设备置于相邻节点的通信线路的两端，位于各自节点及相应的调制解调器上。在这种加密方式中，两个相邻节点的保密设备使用的密钥是相同的。

在链路加密方式中，报文在第 2 到第 7 层之间都是以明文的形式出现，只是在链路层的结束、物理层的开始之间，报文得到加密，然后以密文的形式在物理线路上传输。当报文传到通信路径的某个中间节点时，报文在中间节点上被相应保密设备解密，以明文形式出现，随后再被加密，发送给下一个节点。

链路加密不仅加密了正文，而且加密了所有各层的控制信息。因此，接收节点必须对

收到的密文解密，否则无法对报文在网络中的传送加以控制，无法决定报文传送的路由。由此可见，链路加密只对线路上的通信予以保护，而对主机（包括端节点和中间节点）上的报文不予保护。在各节点上的报文以明文形式出现，极易受到攻击，这种加密方式要求中间节点是可信的。不过，这种加密方式可以有效地防止对网络业务流进行分析，并对网络口令和在链路层中产生的控制信息进行了有效保护。

### 3. 传送层加密方式

传送层加密是在网络七层模型的中间对数据进行加密。这种加密对用户是透明的，由系统自动实现。以这种方式加密，每个节点要有与其他节点通信所需的密钥。在这一层次加密时，它不仅把正文数据予以加密，还把传送层及其以上各层的控制信息也都予以加密。

仍以图 1-1 为例。假定节点 A 的终端要与节点 C 的终端进行通信。首先把数据发送到节点 A。请注意，终端到节点 A 之间的通信以明文方式进行。在节点 A 对数据加密后，根据所选的路由把数据发往下一个节点，比如 E。节点 E 收到数据后原封不动地转发给节点 C。节点 C 收到数据后，将其解密，得到明文，然后把明文发送给终端。在这整个过程中，从节点 A 的终端到节点 C，以及从节点 C 到它的终端的通信都是以明文方式进行。对数据的加密和解密分别在节点 A 和 C 上进行。这就是传送层加密方式与应用层或表示层的端到端加密的主要区别。这种加密方式不能保障从用户终端到终端所属节点之间通信的安全性。

### 4. 数字签名

计算机网络中对网络安全的一个特殊要求是通信的真实性。这就要求通信双方能互相证实，以防第三者假冒通信的一方，窃取信息。在网络中实现通信真实性的方法是数字签名。数字签名能解决以下问题：

- 接收者能够核实发送者对报文的签名。
- 接收者不能伪造对报文的签名。
- 发送者事后不能抵赖对报文的签名。

实现数字签名的方法很多，这里介绍一种简单的用公开密钥算法实现的签名方法。

假设 M 和 N 进行通信。M 为发送者，N 为接收者。M 生成了一个自己的秘密密钥 SKM，并向所有可与他通信的用户发布了一个公开密钥 PKM。N 也生成了一个自己的秘密密钥 SKN，并公开了自己的公开密钥 PKN。在这个公开密钥系统中，加密算法为 E，解密算法为 D。

当 M 要想给 N 发送一条报文 X 时，他先用自己的秘密密钥 SKM 对报文 X 签名：

Y=Dskm(X)

然后把 Y 传送给 N。N 可以用 M 的公开密钥对 Y 进行加密运算，就可从 Y 中恢复出 X，即

X=Epkm(Y)

=Epkm(Dskm(X))

因为只有 M 才拥有秘密密钥 SKM，所以除 M 之外无法产生密文，这说明以这种方式就可使 M 对报文 X 进行“签名”。M 对这种签名是无法抵赖的。如果 M 事后抵赖，任何第三者都能用 M 的公开密钥 PKM 对已签名的报文 Dskm(X)进行解密恢复 X，从而可证

明 N 所收到的报文 Dskm(X)确实来自 M。

反之，N 也不能对收到的报文进行伪造。如果 N 把 X 伪造成 X'，则 N 无法在公证人面前出示 Dskm(X)，因为秘密密钥 SKM 仅为 M 所知。这样，M 用自己的秘密密钥对报文 X 签名后，他事后不能抵赖自己发送过这条报文，接收者也无法伪造 M 发送过的报文。

经 M 签名的报文，若不进行加密，则任何人都可以利用 M 的公开密钥 PKM 把明文 X 析出，为此，当 M 向 N 发送这条已签名的报文时，必须用接收者 N 的公开密钥 PKN 对它加密，也就是

Epkm(Y)=Epkn(Dskm(X))

N 在收到 Epkm(Y)后，先用自己的秘密密钥 SKN 对之解密，得到一个经 M 签名的报文 Dskm(X)，再用 M 的公开密钥 PKM 对之加密，以求出真正的明文 X。这种具有保密性的数字签名过程，如图 1-2 所示。

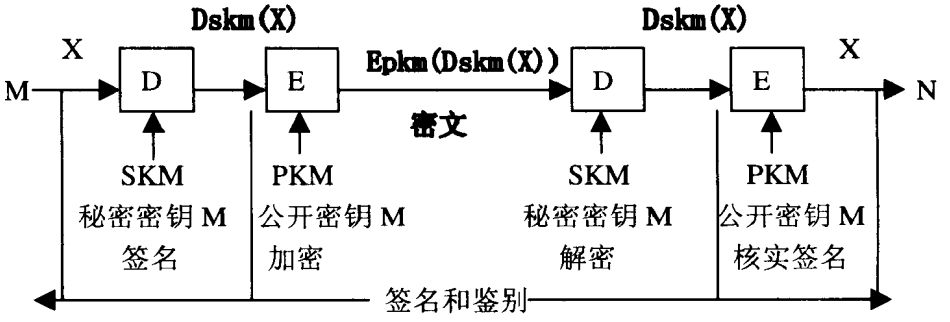



图 1-2 具有保密性的签名

## 1.1.3 计算机网络数据的完整性控制机制

网络上数据的完整性依赖于数据的正确产生、正确存储和正确传送。在计算机网络中，通常用校验和、协议、公证和数字签名的方法来解决数据完整性问题。

（1）校验和

在网络中，为了增强信息完整性的保障程度，还采用一种密码校验和的校验方式。密码校验和是一般检错码，只是它的计算规则不公开，并且不容易从已知校验例子中推导出来。密码校验和是使用一个复杂的函数来计算校验和。较典型的一种密码校验和是以密文反馈分组链路加密模式中使用的 DES 算法，直到最后一块也被加密后，把它当作校验和使用。

为了避免这种方法不能识别报文分组的缺点，可以对每块报文分组赋以一个块号。密码校验和不仅可用 DES 产生，也可用 RSA 算法产生，其防止报文分组的方法也是一样的。

（2）协议

通信协议必须可靠，必须能检测信息的复制（重放）、删除、修改和次序重排。

（3）公证

在网络中设置一个权威的公证中心，通信双方经过公证中心进行通信。用户与公证中心的通信可以用密码校验和、数字签名的技术来防伪存真。

（4）数字签名

如前所述，还可以用数字签名的方法来保证数据的真实性，从而维护数据的完整性。

## 1.2　计算机网络系统安全的维护

计算机网络安全的主要目的是保护存储在系统中的数据信息，这些信息有三个特性。

（1）可用性。无论何时，只要需要，数据信息必须是可用的。

（2）完整性。完整性是指数据信息必须按它的原型保存，不能被非法修改。完整性是对信息的精确性与可靠性的度量。

（3）保密性。数据信息必须按拥有者的要求保持一定的秘密性。只有得到拥有者的许可，其他人才能够获得该信息，必须防止非授权泄露信息。

正是信息的这些特性构成了计算机网络系统安全策略的基础。计算机对电子信息提供的保护，至少应与其他方法对非电子信息提供的保护达到一样的程度，然而，由于电子信息比其他形式的信息面临着更大的威胁，所以计算机安全更严格。无论对电子信息采取什么样的安全措施，都必须考虑到计算机网络系统的脆弱性与计算机网络系统面临的各种威胁。

### 1.2.1　计算机网络系统的易受攻击性

计算机本身存在着一些固有的弱点与脆弱性，使非授权用户利用这些弱点可以对计算机系统进行非法访问，这种非法访问会使系统内存储信息的完整性受到威胁，也可能使信息遭到破坏而不能继续使用，更为严重的是可以窃取有价值的信息而不留任何痕迹。另外，计算机系统还易受各种自然灾害以及各种误操作的破坏。计算机网络系统的脆弱性主要表现在以下几方面。

（1）存储数据的密度极高

在一块磁盘或一卷磁带中，可以存储大量数据信息，而一块磁盘很容易放在口袋中带出办公室，这些存储介质也很容易受到意外损坏。不管哪种情况，都会造成大量信息的丢失。

（2）数据泄露

计算机网络系统工作时能够辐射出电磁波，任何人都可以借助并不复杂的设备在一定的范围内收到它，从而造成信息泄露。这种电磁辐射在任何电子设备中都是存在的。

（3）数据的可访问性

电子信息可以很容易被拷贝下来而不留任何痕迹，一台远程终端上的用户可以通过计算机网络连接到计算中心的系统上，在一定条件下，他可以访问到系统中的所有数据，并可以按他的需要将其拷贝、删改或破坏。

（4）磁性介质的剩磁效应

保存在磁性存储介质中的数据可能会将存储介质永久性地磁化，所以存储介质中的信息有时擦除不净或不能完全擦除。当将一块存储过机密信息的磁盘消除其机密信息时，首先要做的就是将其中的数据擦掉。如果这种擦除不彻底的话，其中就会留下可读信息的痕迹。一旦被利用，就会产生泄密。另外，在大多数计算机操作系统中，删除文件仅仅是将该文件的文件名删除，并将相应的存储空间释放，而文件的真正内容还原封不动地保留在存储介质上，利用这一点可以偷取机密信息。

此为试读，需要完整PDF请访问：www.ertongbook.com