国 际 电 信 联 盟

CCITT X.800

国际电报电话咨询委员会

数据通信网：开放系统互连（OSI）；安全、结构和应用

CCITT 应用的开放系统互连（OSI）安全体系结构

X.800 建议书

1991 年，日内瓦

前言

CCITT（国际电报电话咨询委员会）是国际电信联盟（ITU）的一个永久性机构。CCITT 负责研究技术、运营和资费等问题，并发布有关这些问题的建议书，以期实现全球范围的电信标准化。

CCITT 全体会议每四年召开一次，确定研究主题，并批准各研究组编写的建议书。在全体会议期间，CCITT 各成员按照 CCITT 第 2 号决议确定的程序批准建议书（1988 年，墨尔本）。

X.800 建议书由第 7 研究组编写，按照第 2 号决议的程序，于 1991 年 3 月 22 日通过。

CCITT 注

本建议书为简要而使用的“主管部门”一词，既指电信主管部门，又指经认可的运营机构。

X.800 建议书

CCITT 应用的开放系统互连（OSI）安全体系结构 [1)]

0 引言

X.200 建议书描述了开放系统互连（OSI）参考模型。它建立了一个框架，用于协调提出有关系统互连的、现有的和未来的建议。

OSI 的目标是允许异类的计算机系统实现互连，从而实现应用进程之间的有用通信。在不同时期，必须建立安全控制机制，以便保护应用进程之间的信息交换。通过此类控制，应使不当获取或修改数据的成本大于这么做可能获得的价值，或者应使获取数据所消耗的时间大得都使数据失去了价值。

本建议书定义了安全相关的体系结构一般要素，这些要素可适当地用在开放系统之间的通信需要得到保护的情况中。它在参考模型框架内建立了指南和约束条件，以改善现有的建议书或者在 OSI 范畴内提出新的建议书，从而确保安全通信，并提供与 OSI 一致的安全保护方法。

安全背景将有助于理解本建议书。对不是非常了解安全问题的读者，建议先阅读附件 A。

本建议书扩展了参考模型（X.200 建议书），以涵盖方方面面的安全问题，它们都是通信协议的一般性体系结构要素，但在参考模型中未对之做论述。

1 应用范畴

本建议书：

a) 对安全服务和相关机制进行一般性描述，这可通过参考模型来提供；以及

b) 定义在参考模型中的位置，在这些位置上提供服务和机制。

本建议书扩展了 X.200 建议书的应用领域，以涵盖开放系统之间的安全通信。

已为参考模型的所有层定义了基本的安全服务和机制及其适当的定位。此外，定义了安全服务和机制相对参考模型的体系结构关系。在端系统、装置和组织中可能需要额外的安全措施。这些措施适用于各种各样的应用情景。额外的安全措施所需的安全服务定义超出了本建议书的范围。

---

1) X.800 建议书和 ISO 7498-2（信息处理系统 — 开放系统互连 — 基本参考模型 — 第 2 部分：安全体系结构）在技术上是一致的。

OSI 安全功能只涉及通信路径中存在的显著问题，以保证端系统之间实现安全的信息传输。OSI 安全不涉及端系统、装置和组织所需的安全措施，除非它们对 OSI 中可见之安全服务的选择和定位有影响。后面这些安全问题可被标准化，但不在 OSI 建议书的范围内。

本建议书增加了 X.200 建议书中定义的概念和原则；不对之进行修改。本建议书不是一个实施规范，也不作为用于评价一个实际实施方案是否符合要求的基础。

2 参考文献

X.200 建议书 — CCITT 应用的开放系统互连参考模型。

ISO 7498 — 信息处理系统 — 开放系统互连 — 基本参考模型（1984 年）。

ISO 7498-4 — 信息处理系统 — 开放系统互连 — 基本参考模型 — 第 4 部分：管理框架（1989 年）。

ISO 7498/AD1 — 信息处理系统 — 开放系统互连 — 基本参考模型 — 附录 1：无连接模式传输（1987 年）。

ISO 8648 — 信息处理系统 — 开放系统互连 — 网络层的内部组织（1988 年）。

3 定义和缩写

3.1 本建议书建立在 X.200 建议书所提出的概念基础上，使用了当中定义的以下术语：

a) （N)－连接；

b) （N)－数据传输；

c) （N)－实体；

d) （N)－设施；

e) （N)－层；

f) 开放系统；

g) 对等实体；

h) （N)－协议；

j) （N)－协议数据单元；

k) （N)－中继；

l) 路由；

m) 排队；

n) （N)－服务；

p) （N)－服务数据单元；

q) （N)－用户数据；

r) 子网

s) OSI 资源；以及

t) 传输句法。

3.2 本建议书使用以下术语，它们分别来自不同的建议书/国际标准：

无连接传输模式（ISO 7498/AD1）

端系统（X.200/ISO 7498 建议书）

中继与路由功能（ISO 8648）

管理信息库（MIB）（ISO 7498-4）

此外，还使用了以下缩略语：

OSI：开放系统互连；

SDU：服务数据单元；

SMIB：安全管理信息库；以及

MIB：管理信息库。

3.3 本建议书使用了以下定义：

3.3.1 **access control 访问控制**

防止未授权使用资源，包括防止以未授权方式使用资源。

3.3.2 **access control list 访问控制表**

实体列表，连同其访问权限，被授权可访问某资源。

3.3.3 **accountability 责任性**

实体的一种属性，用于确保实体的行动可被唯一地追溯至该实体。

3.3.4 **active threat 主动威胁**

故意地、未经授权地更改系统状态的威胁。

注 — 安全相关的主动威胁的例子可以是：修改消息、消息重播、插入虚假消息、冒充某授权实体以及拒绝服务等。

3.3.5 **audit 审计**

参见“安全审计”。

3.3.6 **audit trail 审计跟踪**

参见“安全审计跟踪”。

3.3.7 **authentication 身份验证**

参见“数据来源身份验证”和“对等实体身份验证”。

注 — 在本建议书中，术语“身份验证”在使用时与数据完整性无关，当论及数据完整性时，使用术语“数据完整性”。

3.3.8 **authentication information 身份验证信息**

用于建立所声称实体有效性的信息。

3.3.9 **authentication exchange 身份验证交换**

利用信息交换手段用于确保实体身份的一种机制。

3.3.10 **authorization 授权**

授予权限，包括授予基于访问权限进行访问的权限。

3.3.11 **availability 可用性**

已授权实体一旦需要就可访问和使用的特性。

3.3.12 **capability 性能**

一个标记，作为某资源的一个标识符，用于表明有此标记则有权访问该资源。

3.3.13 **channel 信道**

信息传输路径。

3.3.14 **ciphertext 密文**

通过使用密码而生成的数据。结果数据的语义内容是不可用的。

注 — 密文本身是可加密的，这样将生成超级加密的输出结果。

3.3.15 **cleartext 明文**

可理解的数据，其语义内容是可用的。

3.3.16 **confidentiality 保密性**

使信息不泄漏给未授权的个人、实体或过程或者不使信息为其利用的特性。

3.3.17 **credentials 凭证**

传输用于建立某实体宣称之身份的数据。

3.3.18 **cryptanalysis 密码分析**

对密码系统与/或其输入和输出进行分析，以便获得机密的变量与/或敏感的数据，包括明文。

3.3.19 **cryptographic checkvalue 密码校验值**

通过对数据单元执行密码转换（参见“密码学”）而得到的信息。

注 — 校验值的推导可能需要执行一个或多个步骤，是有关密钥和数据单元的数学函数的结果。它通常用于检查数据单元的完整性。

3.3.20 **cryptography 密码学**

由原理、手段和方法等组成的学科，用于数据转换，以便隐藏其信息内容，防止其被不可察觉的修改与/或防止其被未经授权的使用。

注 — 密码学确定用于加密和解密的方法。对加密原理、手段或方法的攻击称为密码分析。

3.3.21 **data integrity 数据完整性**

数据未被以未授权方式修改或破坏的特性。

3.3.22 **data origin authentication 数据来源身份验证**

确认收到的数据来源就是所声称的数据来源。

3.3.23 **decipherment 解密**

对应可逆加密的逆转。

3.3.24 **decryption 解密**

参见“解密”。

3.3.25 **denial of service 拒绝服务**

阻止对资源的授权访问或者延误时敏操作。

3.3.26 **digital signature 数字签名**

数据追加到数据单元或者对数据单元进行加密转换（参见“密码学 cryptography”），使数据单元的接收者能够证明数据的来源和数据单元的完整性，并防止伪造，如被接收者伪造。

3.3.27 **encipherment 加密**

对数据进行加密转换（参见“密码学”），以生成密文。

注 — 加密可能是不可逆转的，在这种情况下，相应的解密过程不能切实执行。

3.3.28 **encryption 加密**

参见“加密”。

3.3.29 **end-to-end encipherment 端对端加密**

在源端系统内或在源端系统上对数据进行加密，对应地，仅在目的端系统内或在目的端系统上进行解密。（另可参见“逐个链路加密”。）

3.3.30 **identity-based security policy 基于身份的安全策略**

基于用户、一组用户或代表用户访问资源/对象之实体身份的安全策略，

3.3.31 **integrity 完整性**

参见“数据完整性”。

3.3.32 **key 密钥**

控制加密与解密操作的符号序列。

3.3.33 **key management 密钥管理**

依据安全策略生成、存储、分发、删除、存档和应用密钥。

3.3.34 **link-by-link encipherment 逐个链路加密**

对通信系统的各个链路单独进行加密。（另可参见“端到端加密”。）

注 — 逐个链路加密意味着在中继实体中，数据将以明文形式出现。

3.3.35 **manipulation detection 操作检测**

一种用于检测某数据单元是否已被修改（无论是意外的还是故意的）的机制。

3.3.36 **masquerade 冒充**

某实体假装是另一个不同的实体。

3.3.37 **notarization 公证**

由可信的第三方注册数据，使得之后保证数据特性确信成为可能，如内容、来源、时间和交付等。

3.3.38 **passive threat 被动威胁**

未经许可而透露信息的威胁，它不改变系统的状态。

3.3.39 **password 口令**

机密的验证信息，一般由一串字符组成。

3.3.40 **peer-entity authentication 对等实体身份验证**

确认关联中的对等实体就是所声称的实体。

3.3.41 **physical security 物理安全**

为资源提供物理保护以免遭蓄意和意外威胁的措施。

3.3.42 **policy 策略**

参见“安全策略”。

3.3.43 **privacy 隐私**

每个人都享有的、控制或影响与其相关的什么信息可被收集和存储以及这些信息可被什么人或对什么人泄露的权利。

注 — 由于该术语涉及个人权利，因此它无法很精确，除了出于安全性方面的需要，应避免使用之。

3.3.44 **repudiation 否认**

涉及通信的实体之一否认曾参与全部或部分通信。

3.3.45 **routing control 路由控制**

在处理路由过程中使用规则，以便选择或避开特定的网络、链路或中继。

3.3.46 **rule-based security policy 基于规则的安全策略**

基于全局规则、针对所有用户的一种安全策略。这些规则通常依赖于对所访问资源敏感性与用户、一组用户或代表用户之实体拥有相应属性情况的比较。

3.3.47 **security audit 安全审计**

对系统记录和活动所做的一种独立审核和检查，以便测试系统控制的恰当性，确保符合既定策略和操作程序的要求，检测违反安全行为，并就控制、策略和程序提出修改建议。

3.3.48 **security audit trail 安全审计跟踪**

收集的和可能用于推动安全审计的数据。

3.3.49 **security label 安全标签**

绑定于某资源（可以是一个数据单元）的标记，用于命名或指定该资源的安全属性。

注 — 标记与/或绑定可以是显性的或隐性的。

3.3.50 **security policy 安全策略**

用于提供安全服务的准则集（参见基于身份的和基于规则的安全策略）。

注 — 一套完整的安全策略必定将解决很多 OSI 范畴之外的问题。

3.3.51 **security service 安全服务**

由通信开放系统某一层提供的一种服务，用于保证系统或数据传输可获得足够的安全。

3.3.52 **selective field protection 选择性字段保护**

保护待传输消息中的特定字段。

3.3.53 **sensitivity 敏感性**

资源的一种特性，指的是它的价值或重要性，可包括它的脆弱性。

3.3.54 **signature 签名**

参见“数字签名”。

3.3.55 **threat 威胁**

对安全的某种潜在冲突。

3.3.56 **traffic analysis 流量分析**

通过对流量流的观测来推断信息（存在、不存在、数量、方向和频率）。

3.3.57 **traffic flow confidentiality 流量流机密性**

保密服务，以防流量分析。

3.3.58 **traffic padding 流量填充**

生成虚假的通信实例、虚假的数据单元与/或数据单元内虚假的数据。

3.3.59 **trusted functionality 可信的功能**

依据某些准则认为是正确的功能，如依据安全策略建立的准则。

4 记号

本建议书中所用的层记号等同于 X.200 建议书中定义的层记号。

除非另有定义，否则术语“服务”指的是安全性方面的服务。

5 安全服务和机制的一般性描述

5.1 概述

本节对包括在 OSI 安全体系结构和机制中以实施相应服务的安全服务做一论述。下面描述的安全服务是基本的安全服务。在实践中，它们将在适当的层中、以适当的组合方式被调用，通常不含非 OSI 服务和机制，以满足安全策略与/或用户要求。特定的安全机制可用来实现基本安全服务的组合。在系统实际的实现过程中，可为直接调用而对基本的安全服务进行特殊的组合。

5.2 安全服务

以下被认为是安全服务，可在 OSI 参考模型框架内有选择地来提供这些服务。身份验证服务要求身份验证信息与本地存储的信息和传输的数据（公证）进行比较，以便实现身份验证。

5.2.1 身份验证

这些服务为通信对等实体身份验证和数据来源身份验证而提供，如下所述。

5.2.1.1 对等实体身份验证

该服务，当由(N)－层来提供时，将确认(N+1)-实体，其对等实体为声称的(N+1)-实体。

提供该服务是为了在建立连接时或者在数据传输时，确认一个或多个连接于一个或多个其它实体之实体的身份。该服务提供了使用信心，确保实体不会试图冒充或未经授权重播之前的连接。带或不带活性检测的单向和相互对等实体身份验证方案都是可能的，都可提供不同程度的保护。

5.2.1.2 数据来源身份验证

该服务，当由(N)－层来提供时，将确认(N+1)-实体，其数据来源为声称的、对等(N+1)-实体。

数据来源身份验证服务用于确认数据单元的来源。该服务不提供针对复制或修改数据单位的保护。

5.2.2 访问控制

该服务用于防止经由 OSI 未经授权地使用资源。这些可能是经由 OSI 协议访问的 OSI 或非 OSI 资源。这种保护服务可用于各种各样类型的资源访问（例如，使用通信资源；阅、写或删某种信息资源；处理资源）或者访问所有资源。

对访问的控制将依据各种各样的安全策略（参见第 6.2.1.1 节）。

5.2.3 数据机密性

提供该服务，旨在保护数据免受未经授权的透露，如下所述。

5.2.3.1 连接机密性

提供该服务，旨在保护(N)－连接上所有(N)－用户－数据的机密性。

注 — 取决于使用和层，它可能不适合于保护所有数据，例如，加急数据或连接请求中的数据。

5.2.3.2 无连接机密性

提供该服务，旨在保护单个无连接(N)－SDU 中所有(N)－用户－数据的机密性。

5.2.3.3 选择性字段机密性

提供该服务，旨在保护(N)－连接上或单个无连接(N)－SDU 中(N)－用户－数据内选定字段的机密性。

5.2.3.4 流量流机密性

提供该服务，旨在保护可能源自流量流观测结果的信息。

5.2.4 数据完整性

该服务用于对抗主动攻击，可能采取如下所述形式中的一种。

注 — 对一个连接而言，在连接开始之时使用对等实体身份验证服务以及在整个连接过程中使用数据完整性服务，可共同为该连接上传输的所有数据单元的来源、这些数据单位的完整性提供确认服务，并可额外地为数据单位复制提供检测服务，例如，通过使用序列号。

5.2.4.1 带恢复功能的连接完整性

提供该服务，旨在保护(N)－连接上所有(N)－用户－数据的完整性，并检测对整个 SDU 序列内任何数据（尝试恢复）所做的任何修改、插入、删除或重播。

5.2.4.2 不带恢复功能的连接完整性

同第 5.2.4.1 节，但不做任何恢复尝试。

5.2.4.3 选择性字段连接完整性

提供该服务，旨在保护经由某个连接传输的(N)－SDU 之(N)－用户－数据内选定字段的完整性，确定所选数据是否有过修改、插入、删除或重播。

5.2.4.4 无连接完整性

该服务，当由(N)－层来提供时，将确保请求(N+1)－ 实体的完整性。

提供该服务，旨在保护单个无连接 SDU 的完整性，确定收到的 SDU 是否有过修改。此外，可对重播做有限检测。

5.2.4.5 选择性字段无连接完整性

提供该服务，旨在保护单个无连接 SDU 内选定字段的完整性，确定所选字段是否有过修改。

5.2.5 不可否认

该服务可能采取两种形式中的一种或两种。

5.2.5.1 带来源证明功能的不可否认

为数据的接收方提供该服务，旨在证明数据的来源。这将防止发送方虚假否认其曾发送过数据或其内容的任何企图。

5.2.5.2 带交付证明功能的不可否认

为数据的发送方提供该服务，旨在证明数据的交付。这将防止接收方之后虚假否认其曾接收过数据或其内容的任何企图。

5.3 特定的安全机制

下面的机制可被纳入适当的(N)－层中，以便提供第 5.2 节中所述的某些服务。

5.3.1 加密

5.3.1.1 加密可以提供数据或流量流信息的机密性，并可作为以下各节中所述之诸多其它安全机制的一部分或作为其补充。

5.3.1.2 加密算法可能是可逆的或不可逆的。可逆加密算法一般有两种分类：

a) 对称的（即秘密密钥）加密，当中，知晓加密密钥即意味着知晓解密密钥，反之亦然；以及

b) 不对称的（如公共密钥）加密，当中，知晓加密密钥并不意味着知晓解密密钥，反之亦然。此类系统的两个密钥有时被称为“公钥”与“私钥”。

不可逆加密算法可能会或可能不会使用密钥。当它们使用密钥时，该密钥可以是公钥或私钥。

5.3.1.3 加密机制的存在意味着除了一些不可逆加密算法的情况外，可使用密钥管理机制。在第 8.4 节中给出了有关密钥管理方法的一些指导方针。

5.3.2 数字签名机制

这些机制定义了两个程序：

a) 对一个数据单元进行签名；以及

b) 对一个经签名的数据单元进行验证。

第一个过程使用的信息是签名者私有的（即唯一的和机密的）。第二个过程使用的程序和信息是公开的，但从中不能推导出签名者的私密信息。

5.3.2.1 签名过程涉及数据单元的加密或数据单元加密校验值的产生，使用签名者的私密信息作为私钥。

5.3.2.2 验证过程涉及使用公用程序和信息来确定签名是否利用签名者的私密信息产生。

5.3.2.3 签名机制的本质特征是签名只能使用签名者的私密信息产生。因此，当对签名进行验证时，它随后可随时证明给第三方看（如裁判或仲裁者），只有私密信息的唯一持有者才可产生签名。

5.3.3 访问控制机制

5.3.3.1 这些机制可以使用实体经验证的身份或实体的信息（如在一组已知实体中的会员资格）或实体的能力，以确定和执行实体的访问权限。如果实体试图使用某个未经授权的资源，或者对授权资源进行不恰当的访问，那么访问控制功能将拒绝此类尝试，并可能报告事件，以便发出警报与/或记录为安全审计跟踪的一部分。向发送方通告任何有关拒绝访问无连接数据传输情况，都只能源自对数据来源的访问控制。

5.3.3.2 例如，访问控制机制可以基于使用以下一项或多项信息：

a) 访问控制信息库，在当中维护对等实体的访问权限。该信息可由授权中心或由被访问实体来维护，并可采取访问控制列表或层次矩阵或分布式结构的形式。这预先假定对等实体身份验证已得到保证。

b) 身份验证信息，如口令、拥有和随后展示拥有访问实体之权限的证据；

c) 能力、拥有和随后展示拥有访问能力定义的实体或资源之权限的证据。

注 — 一种无法实施并应以某种可信方式传达的能力。

d) 安全标签，当与实体关联时，可用于允许或拒绝访问，通常根据某个安全策略。

e) 尝试访问的时间；

f) 尝试访问的路由；以及

g) 访问的持续时间。

5.3.3.3 访问控制机制可用于通信关联的任何一端与/或任何的中间点。

涉及来源或任何中间点的访问控制用于确定发送方是否已获授权可与接收方进行通信与/或使用所需的通信资源。

在无连接数据传输目标端的对等级别访问控制机制要求，在来源端必须是预先已知的，并必须记录在安全管理信息库中（参见第 6.2 节和第 8.1 节）。

5.3.4 数据完整性机制

5.3.4.1 有关数据完整性的两个问题是：单个数据单元或字段的完整；以及数据单位或字段流的完整性。一般来说，使用不同的机制来提供这两种类型的完整性服务，虽然若没有提供第一种服务而提供第二种服务是不现实的。

5.3.4.2 确定单个数据单元的完整性涉及两个过程：一个在发送实体，一个在接收实体。发送实体添加一定的数据量给数据单元，该数据量是数据本身的一个函数。该数据量可以是补充信息，如块校验码或加密校验值，其本身可以是加密的。接收实体相应地生成一定的数据量，并与收到的数据量进行比较，以确定数据在传输过程中是否被修改了。该机制单独并不能防止重播单个数据单元。在体系结构的适当层中，检测操作可能在该层或更高层上产生恢复行动（例如，通过重新传输或纠错）。

5.3.4.3　对连接模式的数据传输，为保护数据单元序列的完整性（即防止错序、丢失、重播和插入或修改数据），需要另外一些形式的明确排序，如顺序编号、时间戳或加密链。

5.3.4.4　对无连接模式的传输数据，时间戳可用来提供有限形式的保护，以防止重播单个数据单元。

5.3.5　身份验证交换机制

5.3.5.1　以下是一些可用于身份验证交换的技术：

a)　使用身份验证信息，如由发送实体提供并由接收实体校验的口令；

b)　加密技术；以及

c)　使用实体的特性与/或财产。

5.3.5.2　可将机制纳入(N)－层，以便提供对等实体身份验证。如果机制未能成功对实体进行身份验证，那么这将导致拒绝或终止连接，也可能成为安全审计跟踪的一个条目与/或安全管理中心的一份报告。

5.3.5.3　当使用加密技术时，可将之与“握手”协议结合起来，以防止重播（即确保活跃度）。

5.3.5.4　身份验证交换技术的选择将取决于在何种情况下需要用到这些技术：

a)　时间戳与同步时钟；

b)　双边和三边握手（分别针对单方面和相互身份认证）；以及

c)　由数字签名与/或公证机制实现的不可否认服务。

5.3.6　流量填充机制

流量填充机制可用来提供各种各种级别的保护，以防止流量分析。只有当流量填充受到机密性服务保护时，该机制才有效。

5.3.7　路由控制机制

5.3.7.1　路由可动态地或预先约定地进行选择，以便只使用物理上安全的子网、中继或链路。

5.3.7.2　在检测持续进行的攻击时，端系统希望责成网络服务提供商通过不同的路由来建立连接。

5.3.7.3　可以通过安全策略来禁止携带某些安全标签的数据通过某些子网、中继或链路。连接的发起方（或无连接数据单元的发送方）也可以指定路由警告，要求避开特定的子网、链路或中继。

5.3.8　公证机制

5.3.8.1　在两个或多个实体间进行传输的数据，其属性，如完整性、来源、时间和目的地，可以通过提供公证机制来保证。通过第三方公证来提供保证，参与通信的各实体信任之，其中包含必要的信息，可以以一种可验证的方式来提供所需的保证。各个通信实例视情可对公证方提供的服务使用数字签名、加密和完整性机制。在调用这种公证机制时，通过受保护的通信实例和公证，在参与通信的各实体之间传输数据。

5.4 普遍的安全机制

本节描述若干不特定于任何特定服务的机制。因此，在第 7 节中，它们没有明确被描述为处于某特定层中。这些普遍存在的安全机制中的一些机制，可被视为安全管理方面的问题（参见第 8 节）。一般来说，这些机制的重要性直接关系到所需的安全级别。

5.4.1 可信的功能

5.4.1.1 可信的功能可用于扩展范围，或者促成其它安全机制的有效性。直接提供安全机制或者提供对安全机制访问的任何功能，都应是值得信赖的。

5.4.1.2 用于确保信任的程序可以放置在本建议书讨论范围之外的硬件和软件中，并且在任何情况下，可随感知到的威胁等级和受保护信息的价值不同而不同。

5.4.1.3 一般来说，这些程序昂贵而难以实施。可以通过选择一个体系结构来尽可能减少问题，所选的体系结构应允许在各模块中实施安全功能，各模块可分开制作并可由非安全相关功能来提供。

5.4.1.4 对受保护层之上关联的保护必须通过其它手段来提供，如通过适当的可信功能。

5.4.2 安全标签

5.4.2.1 包括数据项的资源，可能拥有与之相关的安全标签，例如，用于指明灵敏度级别。在传输过程中，为与数据一起传输适当的安全标签，它常常是必要的。一个安全标签可以是与所传输数据相关的额外数据，或者可以是隐含的，例如，通过使用特定的密钥加密数据来隐含，或者通过上下文数据来隐含，如来源或路由。显性的安全标签必须明确标识，以便可对之进行适当校验。此外，它们必须安全地绑定至与其相关的数据上。

5.4.3 事件检测

5.4.3.1 安全相关事件检测包括明显违反安全事件的检测，还可能包括检测“正常的”事件，如成功访问（或登录）。可通过 OSI 中的实体来检测安全相关事件，包括安全机制。通过事件处置管理部门来维护有关事件构成的规范（参见第 8.3.1 节）。例如，检测各种各种与安全相关的事件可能带来一个或多个以下行动：

a) 本地报告事件；

b) 远程报告事件；

c) 记录事件（参见第 5.4.3 节）；以及

d) 恢复行动（参见第 5.4.4 节）。

以下为此类安全相关事件的例子：

a) 特定的安全冲突；

b) 特定的选定事件；以及

c) 事件计数器溢出。

5.4.3.2 该领域的标准化将考虑有关事件报告和事件记录的相关信息传输问题，以及用于事件报告和事件记录传输的语法和语义定义问题。

5.4.4 安全审计跟踪

5.4.4.1 由于其允许通过后续的安全审计，潜在地允许检测和调查违反安全情况，因此安全审计跟踪提供了一种宝贵的安全机制。安全审计独立地对系统记录和行为进行审核和检查，以便测试系统控制是否恰当，从而确保符合既定策略和操作程序的要求，为损坏评估提供帮助，并提出有关改变控制、策略和程序的建议。安全审计需要在安全审计跟踪中记录与安全相关的信息，并分析和报告来自安全审计跟踪的信息。日志或记录被认为是一种安全机制，在本节中进行描述。分析并生成报告被认为是一种安全管理功能（参见第 8.3.2 节）。

5.4.4.2 通过规定待记录之安全相关事件的种类（如明显地违反安全或成功完成操作），可以根据各种各样的要求，收集安全审计跟踪信息。

已知存在的安全审计跟踪，可作为一种威慑，吓阻某些潜在的安全攻击源。

5.4.4.3 OSI 安全审计跟踪将考虑应选择记录哪些信息、在什么条件下记录信息，以及用于交换安全审计跟踪信息的语法和语义定义。

5.4.5 安全恢复

5.4.5.1 安全恢复处理来自机制的请求，如事件处置和管理功能，作为应用一系列规则的结果，采取恢复行动。这些恢复行动可能有三种类型：

a) 立即的；

b) 临时的；以及

c) 长期的。

例如：

立即的行动，可立即中止操作，像断开连接。

临时的行动，可造成某实体的临时失效。

长期的行动，可将某实体纳入“黑名单”或改变某密钥。

5.4.5.2 标准化的科目包括针对恢复行动的协议以及针对安全恢复管理的协议（参见第 8.3.3 节）。

5.5 对安全服务与机制关系的说明

表 1/X.800 说明了哪些机制（单独或与其它机制结合），被认为有时适于提供各项服务。本表对这些关系进行了概述，但并不是确定性的描述。本表中所述的服务和机制在第 5.2 节和第 5.3 节中有描述；在第 6 节中有对关系的更全面描述。

表 1/X.800

对安全服务和机制关系的说明

机制 服务	加密	数字签名	访问控制	数据完整性	身份验证交换	流量填充	路由控制	公证
对等实体身份验证	Y	Y	·	·	Y	·	·	·
数据来源身份验证	Y	Y	·	·	·	·	·	·
访问控制服务	·	·	Y	·	·	·	·	·
连接机密性	Y	.	·	·	·	·	Y	·
无连接机密性	Y	·	·	·	·	·	Y	·
选择性字机密性	Y	·	·	·	·	·	·	·
流量流机密性	Y	·	·	·	·	Y	Y	·
带恢复功能的联机完整性	Y	·	·	Y	·	·	·	·
不带恢复功能的联机完整性	Y	·	·	Y	·	·	·	·
选择性字段连接完整性	Y	·	·	Y	·	·	·	·
无连接完整性	Y	Y	·	Y	·	·	·	·
选择性字段无连接完整性	Y	Y	·	Y	·	·	·	·
不可否认来源	·	Y	·	Y	·	·	·	Y
不可否认交付	·	Y	·	Y	·	·	·	Y

· 认为机制是不恰当的。

Y 是。认为机制是恰当的，从自身角度而言或者结合其它机制角度而言。

注 — 在某些情况下，该机制提供了超过需要的相关服务，但仍可以使用。

6 服务、机制与层的关系

6.1 *安全分层原理*

6.1.1 使用以下原则来确定安全服务在各层中的分配情况以及随后安全机制在各层中的安置情况：

a) 实现服务的可选方法数量应尽可能少；

b) 通过在多层上提供安全服务来构建安全系统是可以接受的；

c) 安全所需的额外功能不应不必要地复制现有的 OSI 功能；

d) 应避免违反层的独立性；

e) 可信功能的数量应尽可能少；

f) 只要实体依赖于由较低层上的某实体提供的安全机制，则任何中间层都应以以下方式来构建，即不得违反安全规定；

g) 只要可能，某层的额外安全功能都应以以下方式来定义，即不排除实施方案作为一个独立模块；以及

h) 假定本建议书适用于由端系统构成的开放系统（端系统包含所有七个层）和中继系统。

6.1.2 对各层上的服务定义可能需要进行修改，以便提供安全服务请求，不论所请求的服务是在该层上提供还是在较低层上提供。

6.2 调用、管理和使用受保护的(N)－服务模型

应结合第 8 节中包含的、有关安全管理问题的一般性论述，来阅读本节。其目的是指明安全服务和机制可通过管理接口与/或服务调用，由管理实体来激活。

6.2.1 确定通信实例的保护特性

6.2.1.1 概述

本节描述为面向连接的和无连接的通信实例调用保护服务。在面向连接的通信情况下，通常在建立连接时请求/提供保护服务。在无连接服务调用情况下，为无连接服务请求的各个实例请求/提供保护服务。

为了简化下面的描述，术语“服务请求”用于表示建立连接或请求无连接服务。为选定数据调用保护服务可以通过请求选择性字段保护来实现。例如，这可以通过建立若干连接来实现，各个连接拥有不同的保护类型或等级。

本安全体系结构包含众多安全策略，包括基于规则的策略、基于身份的策略以及二者的混合。安全体系结构还包含管理部门提供的保护服务、动态选择的保护服务以及二者的混合。

6.2.1.2 服务请求

对每个(N)－服务请求，（N+1)－实体都可请求所需的目标安全保护。(N)－服务请求将指定安全服务以及参数和任何额外的相关信息（如灵敏度信息与/或安全标签），以实现目标安全保护。

在每个通信实例之前，(N)－层需访问安全管理信息库（SMIB）（参见第 8.1 节）。SMIB 将包含（N+1）－实体相关的、管理部门提出的保护要求方面的信息。需要可信的功能来执行这些管理部门提出的安全要求。

在某个面向连接的通信实例期间提供安全特性可要求商定所需的安全服务。商定机制和参数所需的程序可作为一个单独的程序，或者作为正常连接建立程序的一个有机组成部分。

当商定机制和参数作为一个单独的程序时，商定结果（即安全机制的类型以及提供此类安全服务所需的安全参数）将输入安全管理信息库（参见第 8.1 节）。

当商定机制和参数作为正常连接建立程序的一个有机组成部分时，(N)－实体之间的商定结果将暂存于 SMIB 中。在谈判之前，每个(N)－实体都将会访问 SMIB，以获取谈判所需的信息。

(N)－层将拒绝服务要求，如果它违反管理部门提出的要求，这些要求登记在有关（N+1)－实体的 SMIB 中。

(N)－层也将添加至请求的保护服务中，它们将在 SMIB 中进行定义，强制用于获得目标安全防护。

如果（N+1)－实体没有指定目标安全保护，那么(N)－层将依据 SMIB 遵循某安全策略。利用默认安全保护，在 SMIB 为（N+1)－实体定义的范围内，这可实施通信。

6.2.2 提供保护服务

确定管理部门提出的安全要求和动态选择的安全要求组合后，如第 6.2.1 节所述，作为最低目标，(N)－层将尝试实现对目标的保护。这将通过以下方法中的一种或者两种来实现：

a) 直接在(N)－层内调用安全机制；与/或

b) 向（N-1)－层请求保护服务。在这种情况下，必须通过组合(N)－层中的可信功能与/或特定的安全机制，将保护范围扩展至(N)－服务。

注 — 这并不表示(N)－层中的所有功能都是可信的。

因此，(N)－层确定它是否能够实现对所请求目标的保护。如果它不能够做到这一点，那么不会出现任何通信实例。

6.2.2.1 建立一个受保护的(N)－连接

下面的讨论旨在解决(N)－层内的服务提供问题，（相对于（N-1）－服务）。

在某些协议中，为实现满意的目标保护，操作顺序至关重要。

a) 对外的访问控制

(N)－层可提供对外的访问控制，即它可在本地确定（从 SMIB 处）是否可以尝试或禁止建立受保护的(N)-连接。

b) 对等实体身份验证

如果目标保护包括对等实体身份验证，或者如果已知（从 SMIB 处）目的地(N)－实体将要求进行对等实体身份验证，那么必须进行身份验证交换。根据需要，这可以采用两次或三次握手的方式来提供单方面的或相互的身份验证。

有时，身份验证交换可被纳入通常的(N)－连接建立过程中。在其它情况下，身份验证交换可独立于(N)－连接建立来完成。

c) 访问控制服务

目的地(N)－实体或中间实体可提出访问控制限制条件。如果远程访问控制机制需要特定的信息，那么发起(N)－实体在(N)－层协议内或经由管理信道来提供该信息。

d) 机密性

如果已选定总的或选择性的机密性服务，那么受保护的(N)－连接必须建立。这必须包括建立适当的工作密钥和商定连接的加密参数。这可通过在身份验证交换中做出预先安排或者通过一个单独的协议来实现。

e) 数据完整性

如果所有(N)－用户－数据的完整性，带恢复功能或不带恢复功能，或者选择性字段的完整性已被选中，那么必须建立受保护(N)－连接。这可以是等同于为提供机密性服务而建的连接，并可提供身份验证服务。同样的考虑适用于针对受保护(N)－连接的机密性服务。

f) 不可否认服务

如果已选定带来源证明功能的不可否认服务，那么必须确立适当的加密参数，或者必须建立一个与公证实体的受保护连接。

如果已选定带交付证明功能的不可否认服务，那么必须确立适当的参数（不同于那些带来源证明功能的不可否认服务所要求的参数），或者必须建立一个与公证实体的受保护连接。

注 — 建立受保护(N)－连接可能会因缺少关于加密参数的协议而失败（可能包括未拥有适当的密钥），或者通过访问控制机制来拒绝。

6.2.3 执行一个受保护的(N)－连接

6.2.3.1 在受保护(N)－连接的数据转换阶段，必须提供商定的保护服务。

在(N)－服务边界将可见到以下服务：

a) 对等实体身份验证（间隔地）；

b) 选择性字段保护；以及

c) 主动攻击报告（例如，在进行数据处理时，正在提供的服务为“不带恢复功能的连接完整性”－参见第 5.2.4.2 节）。

此外，也可能需要以下服务：

a) 安全审计跟踪记录；以及

b) 事件检测与处置。

6.2.3.2 符合选择性应用要求的服务:

a) 机密性；

b) 数据完整性（可能带身份验证服务）；以及

c) 不可否认（由接收方或发送方）。

注 1 — 对选定用于某服务的数据项，提出了两种标记技术。第一种涉及强类型的使用，预计表示层将认可某些类型，这些类型要求应用某些保护服务；第二种涉及某种形式的单个数据项标记，对之应采用规定的保护服务。

注 *2* — 假定选择性应用不可否认服务的一个原因可能源自以下情景：在两个(N)－实体同意相互接受某个数据项的最终版本之前，通过关联进行了某种形式的谈判。此时，预期的接收方可请求发送方对最终商定的数据项版本应用不可否认服务（关于来源的和关于交付的）。发送方请求并获得这些服务，传输数据项，随后接收通知，告知接收方已收到和确认数据项。不可否认服务向数据项的发起方和接收方保证：数据项已成功予以传输。

注 *3* — 两种不可否认服务（即有关来源的和有关交付的）通过发起方来调用。

6.2.4 提供受保护的无连接数据传输

在面向连接的协议中的安全服务并非都可用于无连接协议。特别地，防止删除、插入和重播攻击的服务，如果需要的话，必须在面向连接的较高层上进行提供。防止重播攻击的有限保护可以通过时间戳机制来提供。此外，还有许多其它安全服务是无法提供相同等级的安全的，它们可以通过面向连接的协议来实现。

以下是适于无连接数据传输的保护服务：

a) 对等实体身份验证（参见第 5.2.1.1 节）；

b) 数据来源身份验证（参见第 5.2.1.1 节）；

c) 访问控制服务（参见第 5.2.2 节）；

d) 无连接机密性（参见第 5.2.3.2 节）；

e) 选择性字段机密性（参见第 5.2.3.3 节）；

f) 无连接完整性（参见第 5.2.4.4 节）；

g) 选择性字段无连接完整性（参见第 5.2.4.5 节）；以及

h) 不可否认，来源（参见第 5.2.5.1 节）。

服务通过加密、签名机制、访问控制机制、路由机制、数据完整性机制与/或公证机制来提供（参见第 5.3 节）。

无连接数据传输的发起方，将需确保其单个 SDU 包含所需的所有信息，以使之在目的地是可接受的。

7 布局安全服务与机制

本节定义了在 OSI 基本参考模型框架内提供的安全服务，并概述了其实现方式。任何安全服务的提供都是可选的，取决于需求。

在本节中确定特定的安全服务后，由某特定层可选地提供，然后通过运行于该层内的安全机制来提供安全服务，除非另有规定。如第 6 节中所述，许多层将提供特定的安全服务。这些层可能不总是从自身内部来提供安全服务，但可利用在较低层内提供的适当的安全服务。即使在某层内不提供任何安全服务，该层的服务定义也可能需要修改，以便允许安全服务请求传递到某较低层。

注 1 — 普遍的安全机制（参见第 5.4 节）未在本节中进行讨论。

注 2 — 应用加密机制位置的选择在附件 C 中进行讨论。

7.1 物理层

7.1.1 服务

只能在物理层上提供的安全服务，无论是单独提供还是组合提供，如下所示：

a) 连接机密性；以及

b) 流量流机密性。

流量流机密性服务采取两种形式：

1) 完全的流量流机密性服务，只能在某些情况下提供，如双向、同时、同步、点对点传输；以及

2) 有限的流量流机密性服务，可为其它类型的传输提供，如异步传输。

这些安全服务限制于应对被动威胁，并可用于点对点或多对等主体通信。

7.1.2 机制

数据流的总的加密是物理层上的主要安全机制。

适用于物理层的一种具体的加密形式，只能是传输安全性（即扩频安全）。

通过一个透明运行的加密装置，来为物理层提供保护。物理层保护的目标是为整个物理服务数据流提供保护，并提供流量流机密性服务。

7.2 数据链路层

7.2.1 服务

只能在数据链路层提供的安全服务如下所示：

a) 连接机密性；以及

b) 无连接机密性。

7.2.2 机制

加密机制用于在数据链路层上提供安全服务（参见附件 C）。

链路层额外的安全保护功能在针对传送的、常规的层功能之前以及针对接收的、常规的层功能之后执行，即安全机制建立在所有常规的层功能基础之上，并使用所有常规的层功能。

数据链路层上的加密机制对链路层协议是敏感的。

7.3 网络层

在内部对网络层进行组织，以提供协议来执行以下操作：

a) 子网访问；

b) 依赖于子网的聚合；

c) 独立于子网的聚合。

d) 中继和选路

7.3.1 服务

安全服务可以通过协议来提供，协议执行与 OSI 网络服务提供有关的子网访问功能，如下所示：

a) 对等实体身份验证；

b) 数据来源身份验证；

c) 访问控制服务；

d) 连接机密性；

e) 无连接机密性；

f) 流量流机密性；

g) 不带恢复功能的连接完整性；以及

h) 无连接完整性。

这些安全服务可单独提供或组合提供。可通过以下协议来提供的安全服务，即协议执行与从端系统到端系统提供 OSI 网络服务有关的中继和路由操作，等同于那些可通过以下协议来提供的安全服务，即协议执行子网访问操作。

7.3.2 机制

7.3.2.1 通过以下协议来使用相同的安全机制，即协议执行与从端系统到端系统提供 OSI 网络服务有关的子网访问、中继和路由操作。在这一层中执行路由操作，因此，路由控制置于这一层中。提供的确定的安全服务如下所示：

a) 对等实体身份验证服务通过适当组合密码衍生的或受保护的身份验证交换、受保护的口令交换和签名机制来提供；

b) 数据来源身份验证服务通过加密或签名机制来提供；

c) 访问控制服务通过适当使用特定的访问控制机制来提供；

d) 连接机密性服务通过加密机制与/或路由控制来提供；

e) 无连接机密性服务通过加密机制与/或路由控制来提供；

f) 流量流机密性服务通过流量填充机制并结合网络层或更低层上的机密性服务与/或路由控制来实现；

g) 不带恢复功能的连接完整性服务通过数据完整性机制有时并结合加密机制来提供；以及

h) 无连接完整性服务通过数据完整性机制有时并结合加密机制来提供。

7.3.2.2 以下协议中的机制，即协议执行与从端系统到端系统提供 OSI 网络服务有关的子网访问操作，经由单个子网提供服务。

对子网管理部门提供的子网保护功能，将按照子网访问协议的要求进行实施，但通常会在针对传送的常规子网功能之前和针对接收的常规子网功能之后来执行。

7.3.2.3 通过以下协议提供的机制，即协议执行与从端系统到端系统提供 OSI 网络服务有关的中继和路由操作，经由一个或多个互连的网络提供服务。

这些机制将在针对传送的中继和路由功能之前和针对接收的中继和路由功能之后进行调用。在路由控制机制的情况下，在将数据以及必要的路由约束条件传送给中继和路由功能之前，从 SMIB 中导出适当的路由约束条件。

7.3.2.4 网络层中的访问控制可以承担许多作用。例如，它允许端系统来控制网络连接的建立以及拒绝不必要的呼叫。它还允许一个或多个子网来控制网络层资源的使用。在某些情况下，后者的目的与网络使用收费有关。

注 — 建立一个网络连接常常会导致子网管理部门收费。可以通过控制访问以及通过选择反向收费或其它网络的具体参数，来尽可能降低成本。

7.3.2.5 可通过某个特定子网的要求将访问控制机制施加于以下协议，即协议执行与从端系统到端系统提供 OSI 网络服务有关的子网访问操作。当访问控制机制通过以下协议来提供时，即协议执行与从端系统到端系统提供 OSI 网络服务有关的中继和路由操作，可以使用它们来控制中继实体对子网的访问以及控制对端系统的访问。显然，访问控制的隔离程度是相当粗糙的，只区分网络层实体。

7.3.2.6 如果流量填充结合网络层中的加密机制（或者来自物理层的机密性服务）来使用，那么可实现一个合理的流量流机密性等级。

7.4 传输层

7.4.1 服务

可以在传输层上提供的安全服务，无论是单独提供还是组合提供，如下所示：

a) 对等实体身份验证；

b) 数据来源身份验证；

c) 访问控制服务；

d) 连接机密性；

e) 无连接机密性；

f) 带恢复功能的连接完整性；

g) 不带恢复功能的连接完整性；以及

h) 无连接完整性。

7.4.2 机制

确定可以提供的安全服务如下所示：

a) 对等实体身份验证服务通过适当组合密码衍生的或受保护的身份验证交换、受保护的口令交换和签名机制来提供；

b) 数据来源身份验证服务通过加密或签名机制来提供；

c) 访问控制服务通过适当使用特定的访问控制机制来提供；

d) 连接机密性服务通过加密机制来提供；

e) 无连接机密性服务通过加密机制来提供；

f) 带恢复功能的连接完整性服务通过数据完整性机制有时并结合加密机制来提供；

g) 不带恢复功能的连接完整性服务通过数据完整性机制有时并结合加密机制来提供；以及

h) 无连接完整性服务通过数据完整性机制有时并结合加密机制来提供。

以以下方式来操作保护机制，即可以为单个传输连接调用安全服务。提供这样的保护机制，可以将单个传输连接与所有其它传输连接隔离开来。

7.5 会话层

7.5.1 服务

在会话层中未提供任何安全服务。

7.6 表示层

7.6.1 服务

设施将由表示层来提供，用于支持应用层向应用过程提供以下安全服务：

a) 连接机密性；

b) 无连接机密性；以及

c) 选择性字段机密性。

表示层中的设施也可支持应用层向应用过程提供以下安全服务：

d) 流量流机密性；

e) 对等实体身份验证；

f) 数据来源身份验证；

g) 带恢复功能的连接完整性；

h) 不带恢复功能的连接完整性；

j) 选择性字段连接机密性；

k) 无连接完整性；

m) 选择性字段无连接完整性；

n) 带来源证明功能的不可否认；以及

p) 带交付证明功能的不可带来。

注 — 由表示层提供的设施指的是那些依赖于机制的设施，它们只能工作于数据的传输语法编码上，例如，并将包括那些基于加密技术的设施。

7.6.2 机制

对以下安全服务，支持机制可置于表示层内，如果是这样的话，那么可以结合应用层安全机制来使用，以提供应用层安全服务：

a) 对等实体身份验证服务可通过语法转换机制（如加密）来支持；

b) 数据来源身份验证服务可通过加密或签名机制来支持；

c) 连接机密性服务可通过加密机制来支持；

d) 无连接机密性服务可通过加密机制来支持；

e) 选择性字段机密性服务可通过加密机制来支持；

f) 流量流机密性服务可通过加密机制来支持；

g) 带恢复功能的连接完整性服务可通过数据完整性机制有时并结合加密机制来支持；

h) 不带恢复功能的连接完整性服务可通过数据完整性机制有时并结合加密机制来支持；

j) 选择性字段连接完整性服务可通过数据完整性机制有时并结合加密机制来支持；

k) 无连接完整性服务可通过数据完整性机制有时并结合加密机制来支持；

m) 选择性字段无连接完整性服务可通过数据完整性机制有时并结合加密机制来支持；

n) 带来源证明功能的不可否认服务可通过适当组合数据完整性、签名和公证机制来支持；以及

p) 带交付证明功能的不可否认服务可通过适当组合数据完整性、签名和公证机制来支持。

用于数据传输的保密机制，当置于上面层中时，将包含在表示层中。

上面列表中的一些安全服务可以另外由完全包含在应用层内的安全机制来提供。

只有机密性安全服务可以完全由包含在表示层内的安全机制来提供。

表示层中的安全机制作为传送转换语法的最后转换阶段以及接收转换过程的初始阶段来执行。

7.7 应用层

7.7.1 服务

应用层可以提供以下基本安全服务中的一个或多个服务，无论是单独提供还是组合提供，如下所示：

a) 对等实体身份验证；

b) 数据来源身份验证；

c) 访问控制服务；

d) 连接机密性；

e) 无连接机密性；

f) 选择性字段机密性；

g) 流量流机密性；

h) 带恢复功能的连接完整性；

j) 不带恢复功能的连接完整性；

k) 选择性字段连接完整性；

m) 无连接完整性；

n) 选择性字段无连接完整性；

p) 带来源证明功能的不可否认；以及

q) 带交付证明功能的不可带来。

在真正的开放系统中，预期通信合作伙伴的身份验证支持对 OSI 和非 OSI 资源（如文件、软件、终端、打印机）的访问控制。

通信实例中的特定安全需求，包括数据机密性、完整性和身份验证，可基于 SMIB 中的信息以及应用过程提出的请求，通过 OSI 安全管理或应用层管理来确定。

7.7.2 机制

应用层的安全服务通过以下机制方式来提供：

a) 对等实体身份验证服务可通过在应用实体之间对身份验证信息进行转换来提供，通过表示层或较低层加密机制来保护；

b) 数据来源身份验证服务可通过签名机制或较低层加密机制来支持；

c) 一个真正的开放系统其访问控制服务问题与 OSI 相关，例如，与特定系统或远程应用实体进行通信的能力，可通过组合应用层和较低层中的访问控制机制来提供。

d) 连接机密性服务可通过较低层加密机制来支持；

e) 无连接机密性服务可通过较低层加密机制来支持；

f) 选择性字段机密性服务可通过表示层上的加密机制来支持；

g) 有限的流量流机密性服务可通过应用层上的流量填充机制并结合更低层上的机密性服务来支持；

h) 带恢复功能的连接完整性服务可通过较低层的数据完整性机制（有时结合加密机制）来支持；

j) 不带恢复功能的连接完整性服务可通过较低层的数据完整性机制（有时结合加密机制）来支持；

k) 选择性字段连接完整性服务可通过数据完整性机制（有时结合加密机制）来支持；

m) 无连接完整性服务可通过较低层的数据完整性机制（有时结合加密机制）来支持；

n) 选择性字段无连接完整性服务可通过数据完整性机制（有时结合加密机制）来支持；

p) 带来源证明功能的不可否认服务可通过适当组合签名和较低层的数据完整性机制可能并结合第三方公证来支持；以及

q) 带交付证明功能的不可否认服务可通过适当组合签名和较低层的数据完整性机制可能并结合第三方公证来支持。

如果公证机制用于提供不可否认服务，那么它将作为一个可信的第三方。它可以以转换形式来中继一个数据单元记录（即转换语法），以便解决争议。它可以从较低层来使用保护服务。

7.7.3 非 OSI 安全服务

应用程序本身基本上可以提供所有的服务，并使用相同类型的机制，它们在本建议书进行描述，可适当地置于体系结构的各层中。此类使用超出了 OSI 服务、协议定义和 OSI 体系结构的范围，但与之是一致的。

7.8 对安全服务与层关系的说明

表 2/X.800 对参考模型的各层进行了说明，在这些层上，提供特定的安全服务。可在第 5.2 节中找到有关安全服务的描述。为何在某个特定层上放置某项服务的理由在附件 B 中进行描述。

表 2/X.800

对安全服务与层关系的说明

服务	层						
	1	2	3	4	5	6	7*
对等实体身份验证	·	·	Y	Y	·	·	Y
数据来源身份验证	·	·	Y	Y	·	·	Y
访问控制服务	·	·	Y	Y	·	·	Y
连接机密性	Y	Y	Y	Y	·	Y	Y
无连接机密性	·	Y	Y	Y	·	Y	Y
选择性字段机密性	·	·	·	·	·	Y	Y
流量流机密性	Y	·	Y	·	·	·	Y
带恢复功能的连接完整性	·	·	·	Y	·	·	Y
不带恢复功能的连接完整性	·	·	Y	Y	·	·	Y
选择性字段连接完整性	·	·	·	·	·	·	Y
无连接完整性	·	·	Y	Y	·	·	Y
选择性字段无连接完整性	·	·	·	·	·	·	Y
不可否认来源	·	·	·	·	·	·	Y
不可否认交付	·	·	·	·	·	·	Y

Y 是。作为提供商的一个选项，服务应纳入各层标准中。

· 未提供。

* 对第 7 层，应注意：应用过程本身可提供安全服务。

注 1 － 表 2/X.800 无意指明各入口具有同等权重或重要性；反之，在表入口内存在相当多的层级。

注 1 － 网络层内安全服务的布局如第 7.3.2 节所述。网络层内安全服务的位置将在很大程度上影响待提供之服务的性质和范围。

注 3 － 表示层包含众多安全设施，用于支持应用层提供安全服务。

8 安全管理

8.1 概述

8.1.1 OSI 安全管理关注的是那些相对 OSI 和 OSI 管理安全的安全管理问题。OSI 安全管理方面关注的是那些在正常通信实例之外的操作，但需要它们来支持和控制这些通信的安全问题。

注 — 通信服务的可用性取决于网络设计与/或网络管理协议。需要对这些问题做出适当选择，以便免遭拒绝服务攻击。

8.1.2 分布式开放系统管理部门可以提出很多安全策略，OSI 安全管理建议书应支持此类策略。受制于某个单一安全策略、受管于某个单一主管部门的实体，有时被纳入所谓的“安全域”。安全域及其相互作用是未来扩展的一个重要领域。

8.1.3 OSI 安全管理关注的是 OSI 安全服务和机制的管理。此类管理需要分发管理信息给这些服务和机制，并收集与这些服务和机制运作有关的信息。例子包括：加密密钥的分布、行政管理强制要求的安全选择参数设置、正常和异常安全事件的报告（审计跟踪）以及服务激活和灭活。安全管理不在协议中解决安全相关信息的传递问题，它们需要特定的安全服务的协议（例如，在连接请求中的参数）。

8.1.4 安全管理信息库（SMIB）是有关开放系统所需之全部安全相关信息的概念性库。该概念不建议任何形式的存储信息或其实施方案。不过，各个端系统都必须包含必要的本地信息，以使其能够执行适当的安全策略。就需在一组（逻辑的或物理的）端系统中执行一致的安全策略而言，SMIB 是一个分布式信息库。在实践中，部分 SMIB 可能会或可能不会与 MIB 集成。

注 — SMIB 可以有多种实现方式，例如：

a) 一个数据表；

b) 一个文件

c) 嵌入于实际开放系统软件或硬件中的数据或规则。

8.1.5 管理协议尤其是安全管理协议以及承载管理信息的通信信道，是潜在的脆弱环节。因此，应采取特别措施，确保管理协议和信息得到妥善保护，从而使为正常通信实例提供的安全保护免遭削弱。

8.1.6 安全管理可能要求在各系统管理部门之间交换安全相关的信息，以便建立或扩展 SMIB。在某些情况下，安全相关信息将通过非 OSI 通信路径进行传递，本地系统管理者将通过未由 OSI 标准化的方法来更新 SMIB。在其它情况下，可能需要通过 OSI 通信路径来交换此类信息，在这种情况下，信息将在运行于真实开放系统中的两个安全管理应用之间进行传递。安全管理应用将使用传递的信息来更新 SMIB。对 SMIB 所做的此类更新可能需要适当安全管理者的事先授权。

8.1.7 为在 OSI 通信信道上交换安全相关的信息，将定义应用协议。

8.2 OSI 安全管理类别

有三种类别的 OSI 安全管理行为：

a) 系统安全管理；

b) 安全服务管理；以及

c) 安全机制管理。

此外，必须虑及 OSI 管理自身的安全（参见第 8.2.4 节）。这些安全管理类别执行的关键功能概述如下。

8.2.1 系统安全管理

系统安全管理涉及整体 OSI 环境方方面面安全问题的管理。以下所列是属于此类安全管理的典型行为：

a) 总体安全策略管理，包括一致性更新和维护；

b) 与其它 OSI 管理功能的相互作用；

c) 与安全服务管理和安全机制管理的相互作用；

d) 事件处置管理（参见第 8.3.1 节）；

e) 安全审计管理（参见第 8.3.2 节）；

f) 安全恢复管理（参见第 8.3.3 节）。

8.2.2 安全服务管理

安全服务管理涉及特定安全服务的管理。以下所列是在管理特定安全服务中可执行的典型行为：

a) 确定和分配服务的目标安全保护；

b) 分配和维护选择（当存在可选项时）特定安全机制（用于提供请求的安全服务）的规则；

c) 商定（在本地和在远程）可用的安全机制，这需要事先管理协议；

d) 通过适当的安全机制管理功能，调用特定的安全机制，例如，为提供行政管理强制要求的安全服务；以及

e) 与其它安全服务管理功能的相互作用以及安全机制管理功能。

8.2.3 安全机制管理

安全机制管理涉及特定安全机制的管理。以下所列安全机制管理功能是典型的但不是全部的：

a) 密钥管理；

b) 加密管理；

c) 数字签名管理；

d) 访问控制管理；

e) 数据完整性管理；

f) 身份验证管理；

g) 流量填充管理；

h) 路由控制管理；以及

j) 公证管理。

对所列的各安全机制管理功能，在第 8.4 节中有更详尽论述。

8.2.4 OSI 管理的安全性

所有 OSI 管理功能以及 OSI 管理信息通信的安全是 OSI 安全的重要组成部分。为确保 OSI 管理协议和信息得到充分保护，该类安全管理将调用所列 OSI 安全服务和机制中的适当选项（参见第 8.1.5 节）。例如，涉及管理信息库的、管理实体之间的通信，通常需要某种形式的保护。

8.3 特定的系统安全管理行为

8.3.1 事件处置管理

OSI 中可见的事件处置管理问题，是远程报告明显的破坏系统安全企图，并修改用于触发事件报告的阈值。

8.3.2 安全审计管理

安全审计管理可包括：

a) 选择需记录与/或远程收集的事件；

b) 使之具备/不具备审计跟踪选定事件记录的能力；

c) 远程收集选定审计记录；以及

d) 准备安全审计报告。

8.3.3 安全恢复管理

安全恢复管理可包括：

a) 维护规则，以响应真实的或有嫌疑的安全冲突；

b) 远程报告明显的系统安全冲突；

c) 安全管理者互动。

8.4 安全机制管理功能

8.4.1 密钥管理

密钥管理可能涉及：

a) 以要求之安全水平相称的间隔，生成合适的密钥；

b) 依据访问控制要求，确定哪些实体应收到一份各密钥的拷贝；以及

c) 以安全的方式，向实际开放系统中的实体实例提供或分发密钥。

据了解，某些密钥管理功能将在 OSI 环境外执行，包括以可信的方式物理分发密钥。

交换工作密钥以供交往中使用是一种正常的层协议功能。选择工作密钥也可通过访问密钥分发中心或者经由管理协议进行预分发来实现。

8.4.2 加密管理

加密管理可能涉及：

a) 与密钥管理的相互作用；

b) 建立密码参数；以及

c) 密码同步。

加密机制的存在意味着将使用密钥管理和共同方法来引用加密算法。

对加密提供的保护区分到何种程度取决于 OSI 环境中拥有独立密钥保护的实体。进而这通常取决于安全体系结构、尤其是密钥管理机制。

对加密算法的共同引用可通过注册密码算法或实体间的先期协议来实现。

8.4.3 数字签名管理

数字签名管理可能涉及：

a) 与密钥管理的相互作用；

b) 建立密码参数与算法；以及

c) 在通信实体与可能的第三方之间使用协议。

注 — 通常，在数字签名管理与加密管理之间存在很大的相似性。

8.4.4 访问控制管理

访问控制管理可能涉及安全属性的分发（包括口令）或者更新访问控制列表或性能列表，它还可能涉及在通信实体与提供访问控制服务的其它实体之间使用某种协议。

8.4.5 数据完整性管理

数据完整性管理可能涉及：

a) 与密钥管理的相互作用；

b) 建立密码参数与算法；以及

c) 在通信实体之间使用协议。

注 — 当为了数据完整性而使用加密技术时，在数据完整性管理与加密管理之间存在很大的相似性。

8.4.6 身份验证管理

对需要执行身份验证的实体而言，身份验证管理可能涉及描述信息分发、口令或密钥（利用密钥管理），它还可能涉及在通信实体与提供身份验证服务的其它实体之间使用某种协议。

8.4.7 流量填充管理

流量填充管理可包括维护用于流量填充的规则。例如，这可包括：

a) 预先规定数据率；

b) 规定随机的数据率；

c) 规定消息特性，如长度；以及

d) 变动规范，可能依据时间与/或日历。

8.4.8 路由控制管理

路由控制管理可能涉及链路或子网定义，依据特定的准则，认为它们是安全的或可信的。

8.4.9 公证管理

公证管理可包括：

a) 公证相关信息的分发；

b) 公证与通信实体之间协议的使用；以及

c) 与公证的相互作用。

附件 A

开放系统互连（OSI）安全性背景信息

（本附件不是本建议书的组成部分）

A.1 背景

本附件提供：

a) 有关 OSI 安全性的信息，以便给出有关本建议书的一些观点；以及

b) 有关体系结构对各种各样安全特性和要求影响的背景信息。

OSI 环境中的安全性问题只是数据处理/数据通信安全性问题的一个方面。如果要使之有效，那么 OSI 环境中使用的保护措施还需要有 OSI 之外的配套措施。例如，可以对在系统之间流动的信息进行加密，但如果没有任何针对系统自身访问的物理安全限制，那么加密可能是徒劳的。此外，OSI 只关心系统互连。为使 OSI 安全措施有效，它们应结合 OSI 之外的措施来使用。

A.2 安全需求

A.2.1 安全指的是什么?

术语“安全”指的是尽可能减少资产和资源的脆弱性。一件资产指的是有价值的某件东西。一个弱点指的是某种劣势，它可能被用来侵犯系统或系统包含的信息。一个威胁指的是对安全的一种潜在侵犯。

A.2.2 开放系统中的安全动机

CCITT 已确定需要一系列建议书，以加强开放系统互连体系结构内的安全性。这源于：

a) 社会越来越依赖计算机，通过数据通信来访问或链接计算机，并需采取保护措施来抵御各种各样的威胁；

b) 在一些国家出现了“数据保护”方面的法律，要求供应商演示验证系统的完整性和私密性；以及

c) 各种各样的组织机构希望使用 OSI 建议书，并根据现有和未来安全系统的需要，提出更高要求。

A.2.3 要保护的是什么?

一般来说，以下内容可能需要保护：

a) 信息和数据（包括软件和安全措施相关的被动数据，如口令）；

b) 通信和数据处理服务；以及

c) 设备和设施。

A.2.4 威胁

对数据通信系统的威胁包括以下内容：

a) 破坏信息与/或其它资源；

b) 损坏或修改信息；

c) 窃取、删除或丢失信息与/或其它资源；

d) 透露信息；以及

e) 中断服务。

威胁可以分为意外的或故意的以及主动的或被动的。

A.2.4.1 无意威胁

无意威胁指的是那些没有预谋之意图的威胁。实现的无意威胁的例子包括系统故障、操作失误和软件缺陷。

A.2.4.2 有意威胁

有意威胁的范围可以从利用可方便得到的监控工具进行的随意检查，到利用专门的系统知识进行的精细攻击。如果实现，有意威胁可被认为是“攻击”。

A.2.4.3 被动威胁

被动威胁指的是那些如果实现，将不会对系统中包含的任何信息造成任何修改以及不会对系统操作和状态造成任何改变的威胁。通过被动窃听来观测通信线路上传输的信息就是被动威胁的一种实现方式。

A.2.4.4 主动威胁

对系统的主动威胁涉及修改系统中包含的信息，或者改变系统的状态或操作。未经授权的用户恶意更改系统的路由表就是主动威胁的一个例子。

A.2.5 一些特定类型的威胁

下面简要回顾了一些在数据处理/数据通信环境中受到特别关注的攻击类型。在下面的章节中，将出现术语“授权”和“未经授权”。“授权”指的是“授予权限”。该定义隐含两件事：权限指的是执行某活动的权利（如访问数据）；它们被授予某实体、人类代理或过程。那么，授权行为指的是执行经授权（并且未撤权）的活动。有关授权概念的更多信息，请参见第 A.3.3.1 节。

A.2.5.1 冒充

冒充指的是一个实体假装是另一个不同的实体。冒充通常与一些其它形式的主动攻击一起使用，尤其是重播和修改消息。例如，在有效的身份验证序列后，身份验证序列可被捕获和重播。只拥有很少特权的某授权实体，可以通过冒充一个拥有较多特权的实体，来获得额外的特权。

A.2.5.2 重播

当重复消息或消息的一部分而产生某未经授权的效应时，认为发生了重播。例如，包含身份验证信息的某有效消息，可由另一实体进行重播，以获得对其身份的验证（而实际上它不具备某些身份特征）。

A.2.5.3 修改消息

当数据传输内容被改变而未被检测到且产生了某未经授权的效应时，认为发生了消息修改。例如，当消息“允许‘约翰史密斯’读取机密文件账号”被改为“允许‘弗雷德布朗’读取机密文件帐户”时，认为发生了消息修改。

A.2.5.4 拒绝服务

当某实体未能履行其适当功能或行为并防止其它实体履行其对应功能时，认为发生了拒绝服务。攻击可以是一般性的，如当某实体压制所有消息时，或者当存在某个特定目标而某实体压制所有指向特定目的地的所有消息时，如安全审计服务。攻击可能涉及压制流量，如本例中所述，或者可能产生额外的流量。也可能产生旨在破坏网络操作的消息，特别是当网络有中继实体时，这些中继实体基于来自其它中继实体的状态报告来决定路由。

A.2.5.5 内部攻击

当系统的合法用户以非预期的方式或未授权的方式行使职能时，就认为发生了内部攻击。大部分已知的计算机犯罪均涉及内部攻击，破坏系统的安全。可以用于抵御内部攻击的保护方法包括：

a) 仔细审查工作人员；

b) 检查硬件、软件、安全策略和系统配置，从而在一定程度上保证它们将正确运行（称为可信的功能）；以及

c) 审计跟踪，以增加检测出此类攻击的可能性。

A.2.5.6 外部攻击

外部攻击可以采用的技术包括：

a) 窃听（主动的和被动的）；

b) 拦截辐射；

c) 伪装成系统的授权用户或系统组件；以及

d) 绕过身份验证或访问控制机制。

A.2.5.7 陷门

当对系统的一个实体进行修改，以使攻击者能够对命令或者预定事件或事件序列产生未经授权的效应，那么其结果被称为一个陷门。例如，修改口令验证，从而使在正常的效应之外，也能验证通过攻击者的口令。

A.2.5.8 特洛伊木马

当引入到系统中时，除了其经授权的功能之外，特洛伊木马还拥有未经授权的功能。另将消息拷贝给一个未经授权信道的中继，就是一种特洛伊木马。

A.2.6 威胁、风险与对抗措施评估

安全特性通常会增加系统的成本，并可能使之更难使用。因此，在设计一个安全系统之前，应确定需要什么样的保护来应对特定的威胁。这就是所谓的威胁评估。系统在很多方面是脆弱的，但由于攻击者缺乏机会，或者由于结果并不能证明所做的努力和检测的风险，因此只有其中一些是可利用的机会。尽管威胁评估的细节问题超出了本附件的讨论范围，但它们大体上包括：

a) 确定系统漏洞；

b) 分析旨在利用这些漏洞的威胁的可能性；

c) 评估后果，若每个威胁都被成功实施；

d) 估计每个攻击的成本；

e) 成本潜在对策；以及

f) 选择合理的安全机制（可能通过成本效益分析）。

非技术措施，如保险覆盖，可能是高效费比的非技术性安全措施。完善的技术安全，就像完美的物理安全，是不可能的。因此，目标应是使攻击的成本足够高，足以将风险降低至可接受的水平。

A.3 安全策略

本节讨论安全策略：需要适当地定义安全策略、其作用、在用的策略方法，以及改进策略使之适用于特定情况。而后将概念用于通信系统。

A.3.1 安全策略的需求与目的

整个安全领域既复杂又深远。任何合理而完整的分析都将产生数量惊人的细节。一个适当的安全策略应主要关注最高主管部门认为应关注的安全问题。本质上，一般来说，安全策略要指明的是在所议系统通常操作期间允许和不允许的安全问题。策略通常是不明确的；指出什么是最重要的，但不明确指出如何获得所需的结果。策略设定安全规范的最高等级。

A.3.2 策略定义的影响：细化过程

由于策略是高度概括的，因此一开始并不清楚策略如何与某个特定的应用相匹配。通常，最好的实现方式是后续对策略进行细化，在各个阶段依据应用添加更多的细节。为了了解需要哪些细节，需依据通用策略，对应用领域进行详细研究。这种研究应确定因试图施加策略条件于应用上而引起的问题。细化过程将产生以非常精确的术语重新描述的通用策略，这些术语直接来自应用。重新经过描述的策略将使确定实施方案细节变得更容易。

A.3.3 安全策略构成

现有的安全策略存在两个方面的问题。二者均依赖于授权行为的概念。

A.3.3.1 授权

已做讨论的威胁均涉及授权或未授权行为的概念。构成授权的声明包含在安全策略中。一个通用的安全策略可能会指明“未经适当授权者不得访问信息、不得对信息进行推断，也不得使用任何资源。”授权的本性是区分各种各样不同的策略。依据涉及之授权的性质，策略可分为两个独立的组件，即基于规则的策略或者基于身份的策略。第一个策略基于少数通用属性或灵敏度等级来使用规则；普遍执行之。第二个策略涉及基于特定的、个性化的属性来授权。假定一些属性永久地与其适用的实体相关联；其它属性（如能力）可传递给其它实体。也可对管理部门提供的授权服务和动态选择的授权服务进行区分。安全策略将确定常用的系统安全要素（例如，如果有的话，基于规则的和基于身份的安全策略组件），以及用户选择的、认为适合使用的系统安全要素。

A.3.3.2 基于身份的安全策略

基于身份的安全策略部分地对应称为“须知”的安全概念。目标是过滤对数据或资源的访问。基本上，有两种基本方式来实现基于身份的策略，这取决于访问权限信息是由访问者持有，还是是所访问数据的一部分。前者的例子是权限或性能，提供给用户，由代表用户的过程来使用。后者的例子是访问控制列表（ACL）。在这两种情况下，数据项大小（从一个完整文件到一个数据元素）可能是非常易变的，数据项可在某性能中进行命名或者携带自身的 ACL。

A.3.3.3 基于规则的安全策略

基于规则的安全策略中的授权通常取决于灵敏度。在安全系统中，数据与/或资源应用安全标签做出标记。代表人类用户的过程可以获得适于其发起者的安全标签。

A.3.4 安全策略、通信与标签

在数据通信环境中，标记的概念很重要。承载属性的标签扮演诸多角色。有在通信期间移动的数据项；有发起通信和响应通信的过程和实体；有在通信期间使用的信道和其它系统资源。所有都有可能被其属性以一种方式或另一种方式标记。安全策略必须指明如何使用每个的属性来提供必要的安全。为给特定的标记属性建立

适当的安全重要性，可能需要进行谈判。当安全标签附于访问过程和被访问数据时，应用基于身份的访问控制所需的额外信息应处于相关标签中。当安全策略是基于访问数据的用户身份时，不论是直接的还是通过一个过程，安全标签都应包括有关用户身份的信息。应在安全管理信息库（SMIB）的安全策略中对特定标签的规则进行描述，与/或根据需要，与端系统进行谈判。标签可以通过属性添加后缀，用于限定其灵敏度、规范处理和分发警告、约束时序和配置、指明端系统的特定要求。

A.3.4.1 过程标签

在身份验证中，完整识别那些发起和响应通信实例的过程或实体以及所有适当的属性，往往是最重要的。因此，SMIB 将充分包含关于这些属性的信息，这些属性对管理部门提出的任何策略而言都至关重要。

A.3.4.2 数据项标签

当数据项在通信实例期间移动时，每个数据项都将紧密地绑定于其标签上。（这种绑定是重要的，在某些基于规则的策略情况下，在提交给应用之前，要求标签是数据项的一个特殊组成部分。）用于保护数据项完整性的技术还将维护标签的准确性和耦合性。通过 OSI 基本参考模型数据链路层中的路由控制功能，可以使用这些属性。

A.4 安全机制

可以使用各种各样的机制来实现安全策略，单独使用或组合使用，取决于所用的策略目标和机制。一般来说，一种机制将属于以下三种机制中的一种（重叠）：

a) 预防；

b) 检测；以及

c) 恢复。

适用于数据通信环境的安全机制将在下面讨论。

A.4.1 密码术与加密

密码术是许多安全服务和机制的基础。加密函数可作为加密、解密、数据完整性、身份验证交换、口令存储和校验等的一部分，以帮助实现机密性、完整性与/或身份验证。用于机密性的加密服务，将敏感数据（即待保护数据）转换为不敏感的形式。当用于完整性或身份验证时，加密技术用于计算无法执行的功能。

加密最初在明文上进行，以产生密文。解密的结果或者是明文，或者是在某种掩护下的密文。计算上，为通用目的之处理而使用明文是可行的；其语义内容是可访问的。除了以指定的方式，（例如，主要是解密或精确匹配），在计算上，处理密文是不可行的，原因是隐藏了其语义内容。当不希望导出初始明文（如口令）时，有时有意使加密是不可逆的（如通过截断或丢失数据）。

加密函数使用加密变量并对字段、数据单元与/或数据单元流进行运算。两个加密变量作为密钥，引导特定的转换，并对变量进行初始化，在某些加密协议中要求这么做，以便保证密文明显的随机性。密钥通常必须保密，加密函数和初始化变量都可能增加延迟并消耗带宽。这将复杂化现有系统的“透明式”或“插入式”加密附件。

对加密和解密而言，加密变量可以是对称的或不对称的。不对称算法中所用的密钥，在数学上是相关的；一个密钥不能从另一个密钥计算得到。这些算法有时被称为“公钥”算法，原因是一个密钥可以公开，而另一个密钥要保密。

当无需知晓密钥即可通过计算恢复明文时，认为对密文是可进行加密分析的。如果使用了脆弱的或有缺陷的加密函数，那么就有可能发生这种事情。拦截和流量分析可导致对密码系统的攻击，包括消息/字段插入、删除和更改、回放先前有效的密文并进行冒充。

因此，密码协议旨在抵御攻击，有时也用于抵御流量分析。特定的流量分析对抗措施－－流量流机密性，旨在隐藏数据存在或不存在的状况及其特点。如果对密文进行中继，那么在中继和网关中，地址是公开的。如果只在各个链路上对数据进行加密，并且在中继或网关中进行解密（因此而变得脆弱），那么认为体系结构用的是“逐个链路加密”。如果在中继或网关中只有地址（以及类似的控制数据）是公开的，那么认为体系结构用的是“端到端加密”。从安全角度来看，端到端加密较为可取，但在体系结构上认为要复杂得多，特别当包括带内电子密钥分发（一种密钥管理功能）时。可对逐个链路加密和端到端加密进行组合，以实现多重安全目标。数据完整性常常通过计算加密校验值来实现。校验值可以通过一个或多个步骤获得，是加密变量和数据的一个数学函数。这些校验值与要保护的数据相关。加密校验值有时被称为操作检测码。

加密技术可以提供或有助于提供针对以下威胁的保护：

a) 消息流观测与/或修改；

b) 流量分析；

c) 否认；

d) 伪造

e) 未经授权的连接；以及

f) 消息修改。

A.4.2 密钥管理问题

使用加密算法牵涉到密钥管理。密钥管理包括生成、分发和控制密钥。密钥管理方法的选择基于各参与方对其使用环境所做的评估。对环境，需要考虑的要素包括：需要采取保护措施保护抵御的威胁（包括组织内部的威胁和组织外部的威胁）、所用的技术、体系结构和提供加密服务的位置、物理结构和加密服务提供方所处的位置。

关于密钥管理，需要考虑的要点包括：

a) 对每个定义的密钥，隐性地或显性地，基于时间、使用或其它准则使用“生命周期”；

b) 依据其功能正确识别密钥，从而使之只能用于其功能，例如，计划用于机密性服务的密钥不得用于完整性服务，或者反之亦然；以及

c) 非 OSI 要素，如密钥的物理分发和密钥的存档。

关于对称密钥算法的密钥管理，需要考虑的要点包括：

a) 在密钥管理协议中使用机密性服务来传送密钥；

b) 使用密钥层次结构。应允许不同的情况，例如：

1) 只使用数据加密密钥的“扁平”密钥层次结构，隐性地或显性地选自密钥身份或索引集；

2) 多层密钥层次结构；以及

3) 密钥加密密钥不得用于保护数据，数据加密密钥不得用于保护密钥加密密钥；

c) 职责分工，从而使任何人都无法完全拥有一个重要密钥的副本。

关于不对称密钥算法的密钥管理，需要考虑的要点包括：

a) 在密钥管理协议中使用机密性服务来传送私钥；以及

b) 在密钥管理协议中使用机密性服务或者带来源证明功能的不可否认服务来传送公钥。可通过对称与/或不对称加密算法来提供这些服务。

A.4.3 数字签名机制

术语“数字签名”用于表示一种特定的技术，它可用于提供安全服务，如不可否认服务和身份验证服务。数字签名机制需要使用不对称加密算法。数字签名机制的本质特征是不使用私钥将无法创建经签名的数据单位。这意味着：

a) 除私钥持有者之外，任何个人都无法创建经签名的数据单元；以及

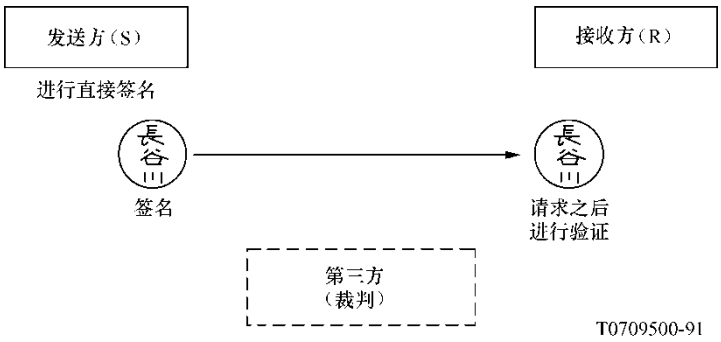
b) 接收方无法创建经签名的数据单位。

因此，只有使用公开可用的信息，才有可能唯一确定一个数据单元的签名者是私钥的所有者。在之后参与者之间出现冲突的情况下，它有可能向一个可靠的第三方证明数据单元签名者的身份，它要求判断经签名数据单元的真实性。这种类型的数字签名被称为直接签名方案（参见图 A-1/X.800)。 在其它情况下，可能需要额外的属性 c)：

c) 发送方无法否认发送过经签名的数据单元。

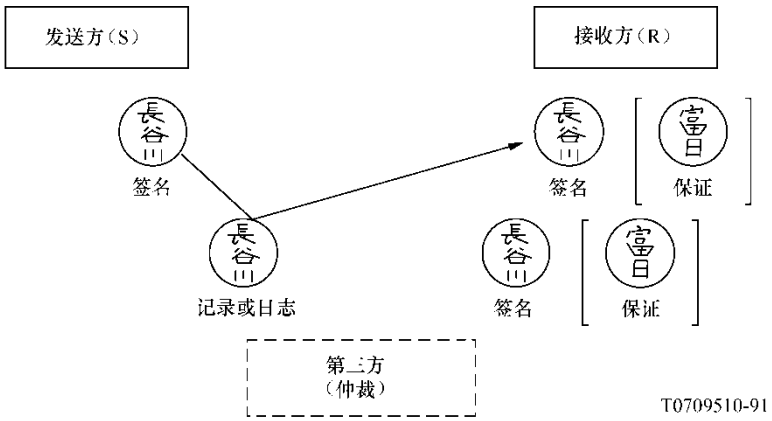
在这种情况下，一个可靠的第三方（仲裁者）向接收方证明信息的来源和完整性。这种类型的数字签名有时是经仲裁的签名方案（参见图 A-2/X.800）。

注 — 发送方可以要求接收方之后不能否认收到了经签名的数据单位。这可以通过不可否认服务来实现，通过数字签名、数据完整性和公证机制的适当组合来证明已经交付数据。



注—当参与方之间出现冲突时（S 可能是伪证方或者 R 可能是伪证方），对签名进行验证。

图 A-1/X.800 直接签名方案



注—由第三方对数据来源进行验证（并为接收方提供保证（即肯定的结果））。由第三方记录证明数据来源和完整性所需的信息。在这种情况下，S 之后无法否认曾发送过所签署的数据单元。

图 A-2/X.800 仲裁签名方案

A.4.4 访问控制机制

访问控制机制指的是以下机制，即用于执行某项策略，以限制只有授权用户才能访问某资源。技术包括：使用访问控制列表或矩阵（通常包含受控项目和授权用户的身份，如人或过程）、口令、能力、标签或令牌，拥有之则可用于指明访问权限。在使用能力时，它们应是无法实施的，并应以某种可信的方式来传达。

A.4.5 数据完整性机制

数据完整性机制有两种类型：一是用于保护单个数据单元的完整性；二是既用于保护单个数据单元的完整性，又用于保护某个连接上整个数据单元流的序列。

A.4.5.1 消息流修改检测

损坏检测技术通常与检测由通信链路和网络引入的比特错误、块错误和序列错误有关，也可用于检测对消息流所做的更改。不过，如果协议报头和报尾不受完整性机制保护，那么已知的入侵者可成功绕过这些检查。只有通过损坏检测技术并结合序列信息，才能成功检测对消息流所做的更改。这不能阻止对消息流的更改，但能发出发生攻击的通告。

A.4.6 身份验证交换机制

A.4.6.1 机制选择

身份验证交换机制有许多种选择和组合，以适用于不同的情况。例如：

a) 当对等实体和通信手段都可信时，对等实体的识别可通过口令来确认。口令用于防止出现错误，但不能防止恶意行为（尤其是不能防止重播）。可以通过在各个方向上使用不同的口令来相互验证身份。

b) 当各个实体信任其对等实体但不信任通信手段时，防止主动攻击可以通过口令和加密的组合或者通过密码手段来实现。防止重播攻击需要双向握手（利用保护参数）或时间戳（利用可信时钟）。通过三路握手，可以实现利用重播保护的相互身份验证。

c) 当实体不信任（或者感觉未来可能会不信任）其对等实体或通信手段时，可使用不可否认服务。通过数字签名与/或公证机制，可以实现不可否认服务。这些机制可与上面 b)中所述的机制一起使用。

A.4.7 流量填充机制

生成虚假流量和填充协议数据单元，使之达到恒定长度，可以对流量分析攻击提供有限的保护。为成功实现之，虚假流量的水平必须接近真实流量的最高预期水平。此外，对协议数据单元的内容必须进行加密或伪装，从而不能从真实流量中识别和区分出虚假流量。

A.4.8 路由控制机制

针对数据传输的路由警告规范（包括整个路由的规范）可用于确保数据只经由物理上安全的路由来传送，或者确保敏感信息只经由具备适当保护等级的路由来传送。

A.4.9 公证机制

公证机制基于可信第三方（公证方）的概念，以确保在两个实体之间交换之信息的某些属性，如其来源、其完整性，或者其发送或接收的时间。

A.4.10 物理与人员安全

物理安全措施将总是必要的，以确保实现妥善保护。物理安全是昂贵的，常试图通过其它（较廉价的）技术来尽可能减少对它的需求。尽管所有的系统最终都将依赖某种形式的物理安全和值得信赖的系统操作人员，但物理和人员安全因素在 OSI 的讨论范围之外。应定义好操作程序，以确保正确的操作和人员责任的描述。

A.4.11 可信的硬件/软件

用于获得正确执行实体功能之信心的方法包括正式的证明方法、核查与验证、检测与记录已知攻击企图，以及在安全的环境中由可信的人来构建实体。也需要预防措施来确保实体不会被意外地或故意地更改，从而在其工作生命周期内就其安全性达成折中方案，例如，在维护或升级期间。如果需要保持安全性，那么系统中的某些实体也必须是可信的，以便工作正常。用于建立信任的方法超出了 OSI 的讨论范围。

附件 B

对第 7 节中安全服务与机制布局的说明

（本附件不是本建议书的组成部分）

B.1 概述

本附录描述了有关在各层内提供所确定之安全服务的一些理由，如第 7 节中所示。标准第 6.1.1 节中所确定的安全分层原则支配了本选择过程。

如果对通常的通信安全的影响可被看作是不同的（例如，第 1 层和第 4 层的连接机密性），那么可由多个层来提供某种特定的安全服务。不过，考虑到现有的 OSI 数据通信功能（例如，多链路程序、复用功能、用于增强为有连接服务提供无连接服务的不同方法），以及为了使这些传输机制能够发挥作用，可能需要允许在另一层上提供某种特定的服务，尽管对安全的影响不能被视作是不同的。

B.2 对等实体身份验证

- 第 1 层和第 2 层：否。在这些层中，对等实体身份验证不被认为是有用的。
- 第 3 层：是。经由单个子网和针对路由与/或经由互联网络。
- 第 4 层：是。在一个连接开始之前以及在该连接持续过程中，在第 4 层上的端系统对端系统身份验证可用于两个或多个会话实体的相互验证。
- 第 5 层：否。在第 4 层与/或更高层上提供该服务没有任何益处。

– *第 6 层*：否。但加密机制可支持在应用层上提供该服务。

– *第 7 层*：是。应由应用层来提供对等实体身份验证服务。

B.3 *数据来源身份验证*

– *第 1 层和第 2 层*：否。在这些层中，数据来源身份验证不被认为是有用的。

– *第 3 层和第 4 层*：在第 3 层与/或第 4 层的中继和路由角色中，可端对端地来提供数据来源身份验证服务，如下所述：

a) 在连接建立之时提供对等实体身份验证服务以及在整个连接过程中提供基于加密的、持续的身份验证服务，实际上就是提供数据来源身份验证服务；以及

b) 即使未提供 a），也可以以很小的额外开销，来为这些层中已有的数据完整性机制提供基于加密的数据来源身份验证服务。

– *第 5 层*：否。在第 4 层或第 7 层上提供该服务没有任何益处。

– *第 6 层*：否。但加密机制可支持在应用层上提供该服务。

– *第 7 层*：是。可能结合表示层上的机制。

B.4 *访问控制*

– *第 1 层和第 2 层*：对符合全部 OSI 协议要求的系统而言，不能在第 1 层或第 2 层上提供访问控制机制，原因是，对这种机制，没有任何可用的端设施。

– *第 3 层*：根据特定子网的要求，访问控制机制可施加于子网访问角色上。当通过中继和路由角色来执行时，网络层上的访问机制既可通过中继实体用于控制对子网的访问，也可用于控制对端系统的访问。显然，访问粒度是相当粗糙的，只在网络层实体间进行区别。

建立一个网络连接常常会导致子网管理部门收费。可以通过控制访问以及通过选择反向收费或其它网络或子网的具体参数，来尽可能降低成本。

– *第 4 层*：是。可在逐个传输连接端对端的基础上，部署应用访问控制机制。

– *第 5 层*：否。在第 4 层与/或第 7 层上提供该服务没有任何益处。

– *第 6 层*：否。在第 6 层上提供该服务是不恰当的。

– *第 7 层*：是。应用协议与/或应用过程可提供面向应用的访问控制设施。

B.5 *(N)－连接上所有(N)－用户－数据的机密性*

– *第 1 层*：是。由于电插入透明的转换设备对可以在物理连接上提供彻底的机密性，因此应提供该服务。

– *第 2 层*：是。但它不会对第 1 层或第 3 层上的机密性提供任何额外的安全益处。

– *第 3 层*：是。针对的是单个子网上的子网访问角色以及针对的是互联网络上的中继和路由角色。

– 第 4 层：是。原因是单个传输连接可提供端对端传输机制以及可隔离会话连接。

– 第 5 层：否。原因是它不会对第 3 层、第 4 层和第 7 层上的机密性提供任何额外的益处。它看起来不适于在本层上提供该服务。

– 第 6 层：是。原因是加密机制提供纯粹的语法转换。

– 第 7 层：是。结合较低层上的各种机制。

B.6 单个无连接(N)－SDU 中所有(N)－用户－数据的机密性

这针对的是所有(N)－用户－数据的机密性，第 1 层除外，其上没有任何无连接服务。

B.7 SDU(N)－用户－数据内选择性字段的机密性

本机密性服务通过表示层上的加密来提供，根据数据的语义，通过应用层上的机制来调用。

B.8 流量流机密性

完全的流量流机密性只能在第 1 层上实现。这可以通过在物理传输路径中物理插入一对加密设备来实现。假定传输路径将双向同时、同步，那么插入设备将在无法辨认的物理媒介上实现所有传输（并均衡其存在）。

在物理层以上，完全的流量流安全是不可能的。通过在某一层上使用完整的 SDU 机密性服务并在某一较高层上插入虚假的流量，可以部分地产生它的某些效应。这种机制是昂贵的，并可能消耗大量的载波和交换容量。

如果在第 3 层上提供流量流机密性服务，那么将使用流量填充与/或路由控制。通过不安全链路或子网周边的路由消息，路由控制可以提供有限的流量流机密性服务。不过，将流量填充纳入第 3 层可更好地实现对网络的利用，例如，通过避免不必要的填充和网络拥塞。

通过生成虚假流量，并结合防止虚假流量标识的机密性服务，可以在应用层上提供有限的流量流机密性服务。

B.9 (N)－连接（带错误恢复功能）上所有(N)－用户－数据的完整性

– 第 1 层和第 2 层：第 1 层和第 2 层无法提供该服务。第 1 层没有任何检测或恢复机制，第 2 层的机制只能以点对点而非端对端的方式执行，因此，不认为适于提供该服务。

– 第 3 层：否。原因是错误恢复不是普遍可用。

– 第 4 层：是。原因是这提供真正的端对端传输连接。

– 第 5 层：否。原因是第 5 层没有错误恢复功能。

– 第 6 层：否。但加密机制可支持应用层上的该服务。

– 第 7 层：是。结合表示层上的各种机制。

B.10 (N)－连接（不带错误恢复功能）上所有(N)－用户－数据的完整性

– 第 1 层和第 2 层：第 1 层和第 2 层无法提供该服务。第 1 层没有任何检测或恢复机制，第 2 层的机制只能以点对点而非端对端的方式执行，因此，不认为适于提供该服务。

– 第 3 层：是。针对的是经由单个子网的子网访问角色以及针对的是经由互联网络的路由和中继角色。

– 第 4 层：是。针对的是以下使用情况，即在检测到主动攻击后中止通信是可接受的。

– 第 5 层：否。原因是它不会对第 3 层、第 4 层或第 7 层上的数据完整性提供任何额外的益处。

– 第 6 层：否。但加密机制可支持应用层上的该服务。

– 第 7 层：是。结合表示层上的各种机制。

B.11 经由(N)－连接（不带恢复功能）转接之(N)－SDU(N)－用户－数据内选定字段的完整性

选定字段的完整性服务可以通过表示层的加密机制结合应用层的调用与校验机制来提供。

B.12 单个无连接(N)－SDU 中所有(N)－用户－数据的完整性

为了尽可能减少功能重复，对不带恢复功能的完整性，只应在相同的层上提供无连接传输的完整性，即在网络层、传输层和应用层上。这种完整性机制只有非常有限的有效性，而这必须实现。

B.13 单个无连接(N)－SDU 中选定字段的完整性

选定字段的完整性服务可以通过表示层的加密机制结合应用层的调用与校验机制来提供。

B.14 不可否认

来源和交付的不可否认服务可以通过公证机制来提供，它将涉及在第 7 层进行中继。

对不可否认服务使用数字签名机制需第 6 层和第 7 层间的密切合作。

附件 C

对应用加密位置的选择

（本附件不是本建议书的组成部分）

C.1 大多数应用不需要在多个层上进行加密。层的选择取决于一些重大问题，如下所述：

1) 如果流量流需要完全保密，那么将选择对物理层进行加密或采取传输安全措施（如采用适当的扩频技术）。适当的物理安全和可信的路由以及中继中类似的功能，可满足所有的保密要求。

2) 如果需要高粒度的保护（即可能需要为每个应用关联提供一个单独的密钥）以及需要提供不可否认或选择性字段保护功能，那么将选择对表示层进行加密。由于加密算法占用大量的处理能力，因此选择性字段保护非常重要。对表示层进行加密可以提供不带恢复功能的完整性、不可否认性以及全部的机密性。

3) 如果所有的端系统对端系统通信都需要简单的批量保护功能与/或需要外部的加密设备（例如，为了给算法和密钥提供物理保护或者提供针对错误软件的保护），那么选择对网络层进行加密。这可以提供机密性以及不带恢复功能的完整性。

注 — 虽然没有在网络层中提供恢复功能，但传输层的正常恢复机制可用于恢复网络层检测到的攻击。

4) 如果需要带恢复功能的完整性以及高粒度的保护，那么选择对传输层进行加密。这可以提供机密性以及带恢复功能或不带恢复功能的完整性。

5) 对未来的实施方案，不建议对数据链路层进行加密。

C.2 当需要关注这些关键问题中的两个或更多个问题时，可能需要在多层提供加密。