GJB

中华人民共和国国家军用标准

FL 0133　　GJB 3433－98

军用计算机网络安全体系结构

Security architecture of military computer networks

广东省网络空间安全协会受控资料

1998－07－27 发布　　1999－01－01 实施

中国人民解放军总装备部　批准

前　言

本标准等效采用国际标准 ISO 7498－2:1989《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》。

根据军队指挥自动化系统的安全要求,增加了可用性服务和可用性管理,补充了附录 A(补充件)“军用报文处理系统的安全服务与安全机制的配置实例”。

附录 B(参考性)介绍的有关 OSI 安全问题的背景材料有助于理解本标准。

广东省网络空间安全协会受控资料

目　次

1　主题内容和适用范围 …… (1)
2　引用文件 …… (1)
3　定义 …… (1)
3.1　术语 …… (1)
3.2　缩写词 …… (5)
4　表示方法 …… (5)
5　安全服务与安全机制的一般描述 …… (5)
6　安全服务、安全机制与层的关系 …… (12)
6.1　安全分层原则 …… (12)
6.2　受保护的(N)服务的调用、管理和使用模型 …… (13)
7　安全服务与安全机制的配置 …… (15)
7.1　物理层 …… (16)
7.2　数据链路层 …… (16)
7.3　网络层 …… (16)
7.4　运输层 …… (18)
7.5　会话层 …… (18)
7.6　表示层 …… (18)
7.7　应用层 …… (19)
7.8　安全服务与层的关系说明 …… (21)
8　安全管理 …… (22)
8.1　概述 …… (22)
8.2　开放系统互连安全管理的分类 …… (22)
8.3　系统安全管理活动 …… (24)
8.4　安全机制管理功能 …… (24)
附录 A　军用报文处理系统的安全服务与安全机制的配置实例(补充件) …… (26)
附录 B　有关开放系统互连安全问题的背景材料(参考件) …… (30)
附录 C　安全服务与安全机制的配置理由(参考件) …… (39)
附录 D　加密位置的选取(参考件) …… (42)

广东省网络空间安全协会受控资料

中华人民共和国国家军用标准

军用计算机网络安全体系结构

Security architecture of military computer networks

GJB 3433－98

1 主题内容和适用范围

本标准给出了军用计算机安全服务和安全机制的一般描述，并规定了这些服务和机制由开放系统互连基本参考模型（见 GB 9387.1）中的哪些层来提供。另外，还说明了安全服务和安全机制与开放系统互连参考模型间的体系结构关系。

在端系统、设备和组织结构中可能需要附加的安全措施，这些措施适用于各种不同的应用上下文。附加措施所需要的安全服务不属于本标准范围。

本标准适用于军用计算机网络端系统之间需要通信安全保护的各种场合，可以为军用计算机网络安全系统的论证、研制、开发和应用提供指导。

2 引用文件

GB 9387.1　信息处理系统　开放系统互连　基本参考模型

3 定义

下列术语适用于本标准。

3.1 术语

3.1.1 访问控制　access control

防止未经授权使用（含以未授权方式使用）某资源。

3.1.2 访问控制表　access control list

实体及其访问权限的列表，这些实体有权访问某资源。

3.1.3 可确认性　accountability

确保实体的活动可以被唯一地跟踪到该实体的特性。

3.1.4 主动威胁　active threat

对系统状态进行故意的、未经授权的修改。例如：更改消息、重发消息、插入伪消息、冒充授权实体及拒绝服务。

3.1.5 审计　audit

见“安全审计”。

3.1.6 审计跟踪　audit trail

见“安全审计跟踪”。

广东省网络空间安全协会受控资料

总装备部 1998－07－27 发布　　1999－01－01 实施

3.1.7 鉴别 authentication

见“数据源点鉴别”和“对等实体鉴别”。

注：本标准在涉及数据完整性时不使用“鉴别”这一术语，而是用“数据完整性”。

3.1.8 鉴别信息 authentication information

用于确定声称的身份是否有效的信息。

3.1.9 鉴别交换 authentication exchange

一种通过信息交换保证实体身份的机制。

3.1.10 授权 authorization

授予权限，包括基于访问权允许访问。

3.1.11 可用性 availability

应授权实体的请求可被访问与使用的特性。

3.1.12 权力 capability

作为资源标识符使用的权标，拥有它便有权访问该资源。

3.1.13 信道 channel

信息传送通路。

3.1.14 密文 ciphertext

经过加密处理所产生的数据，其语义内容是不可用的。密文本身也可以是加密处理的输入，这样就产生超加密输出。

3.1.15 明文 cleartext

可懂数据，其语义内容是可用的。

3.1.16 保密性 confidentiality

信息不泄露给未授权的个人、实体或进程且不为其所用的特性。

3.1.17 凭证 credentials

为了鉴别实体身份而传送的数据。

3.1.18 密码分析 cryptanalysis

为得到保密变量和/或包括明文在内的敏感性数据而对密码系统和/或它的输入输出进行的分析。

3.1.19 密码检验值 cryptographic checkvalue

通过对数据单元进行密码变换而得到的信息。

注：密码检验值可经一步或多步操作后得出，并且是密钥与数据单元的函数，通常用于检验数据单元的完整性。

3.1.20 密码术 cryptography

一门关于数据变换的原理、手段和方法的学科，其目的是隐藏数据的内容，防止对它作了修改而不被识破和/或未经授权使用。

注：密码术确定加密和解密的方法，对密码原理、手段或方法的攻击就是密码分析。

3.1.21 数据完整性 data integrity

数据没有遭受以未授权方式所作的篡改或破坏的特性。

3.1.22 数据源点鉴别 data origin authentication

广东省网络空间安全协会受控资料

证实所接收的数据来自于声称的数据源。

3.1.23 解密 decipherment

在密钥控制下，将密文变成明文的过程，又称解密处理。

3.1.24 解密处理 decryption

见“解密”。

3.1.25 拒绝服务 denial of service

阻止对资源的授权访问或推迟对时间敏感操作的响应。

3.1.26 数字签名 digital signature

附加在数据单元上的数据，或对数据单元进行的密码变换，以使数据单元的接收者能够证实数据单元的来源及其完整性并保护数据，防止被人（例如该接收者）伪造。

3.1.27 加密 encipherment

对数据进行密码换码以产生密文。

3.1.28 加密处理 encryption

见“加密”。

3.1.29 端对端加密 end-to-end encipherment

数据在源端系统内或系统上加密，并只允许在目的端系统内或系统上解密。

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

基于用户/用户群的身份和/或属性，或基于代表用户和被访问资源和/或客体进行活动的实体的安全策略。

3.1.31 完整性 integrity

见“数据完整性”。

3.1.32 密钥 key

控制加密和解密操作的符号序列。

3.1.33 密钥管理 key management

依据安全策略，生成、存储、分发、删除、归档和应用密钥。

3.1.34 逐链加密 link-by-link encipherment

对通信系统的每段链路传送的数据分别加密。逐链加密意味着数据在中继实体中是明文形式。

3.1.35 操纵检测 manipulation detection

用于检测数据单元是否已被修改（偶然的或蓄意的）的一种机制。

3.1.36 冒充 masquerade

一个实体伪装成别的实体。

3.1.37 公证 notarization

由可信赖的第三方对数据进行登记，以保证数据特征（如内容、源点、时间和交付）的准确性。

3.1.38 被动威胁 passive threat

未经授权泄漏信息但不改变系统状态的威胁。

广东省网络空间安全协会受控资料

3.1.39 口令 password

保密的鉴别信息，通常由一串字符组成。

3.1.40 对等实体鉴别 peer-entity authentication

证实连接中的对等实体是所声称的实体。

3.1.41 物理安全 physical security

为防止蓄意和意外威胁，而对资源提供物理保护的措施。

3.1.42 策略 policy

见“安全策略”。

3.1.43 隐私权 privacy

一种个人权力，它控制或影响搜集和存储哪些信息、这些信息可被谁泄露或泄露给谁。

注：由于该术语涉及个人权力，因而不可能很精确。如果不是为了安全保护，应避免使用该术语。

3.1.44 抵赖 repudiation

在通信中涉及到的某个实体否认参与了该通信的全部或一部分。

3.1.45 路由选择控制 routing control

在路由选择过程中使用一些规则来选择通过或绕过特定网络、链路或中继。

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

基于强加给所有用户的总体规则的安全策略。这些规则通常取决于将被访问资源的敏感性和用户、用户群或代表用户进行活动的实体的相应属性进行比较的结果。

3.1.47 安全审计 security audit

对系统记录和活动进行独立的评估和考核，以测试系统控制的完备程度，确保与已建立的策略和操作规程相一致，检测违反安全的行为，介绍对控制、策略和规程中被指出的任何变化。

3.1.48 安全审计跟踪 security audit trail

为安全审计而收集的数据。

3.1.49 安全标记 security label

以显式或隐式形式命名或指定某资源(可以是数据单元)的安全属性的标记。

3.1.50 安全策略 security policy

为安全服务规定的一套准则(见基于身份安全策略和基于规则安全策略)。

注：一种完备的安全策略势必涉及开放系统互连范围以外的许多事项。

3.1.51 安全服务 security service

由正在通信的开放系统的某一层提供的服务，以确保该系统或数据传送的安全。

3.1.52 选择字段保护 selective field protection

对将要传送的消息中的特定字段实施保护。

3.1.53 敏感性 sensitivity

资源所具有的表明其价值或重要性、也可能包括其脆弱性的特性。

3.1.54 签名 signature

见“数字签名”。

3.1.55 威胁 threat

对安全的潜在侵害。

3.1.56 通信业务流分析 traffic analysis

通过观察通信业务流的出现、消失、总量、方向和频率推断信息的过程。

3.1.57 通信业务流保密性 traffic flow confidentiality

抵制通信业务流分析的一种保密性服务。

3.1.58 通信业务量填充 traffic padding

产生虚假通信、虚假数据单元和/或数据单元中的虚假数据的过程。

3.1.59 可信功能 trusted functionality

按某些准则(如由安全策略确定的准则)来衡量认为正确的功能。

3.2 缩写词

3.2.1 ACL Access Control List

访问控制表

3.2.2 AU Access Unit

访问单元

3.2.3 MHS Message Handling System

报文处理系统

3.2.4 MIB Management Information Base

管理信息库

3.2.5 MS Message Store

报文存储

3.2.6 MTA Message Transfer Agent

报文传送代理

3.2.7 MTS Message Transfer System

报文传送系统

3.2.8 SDU Service Data Unit

服务数据单元

3.2.9 SMIB Security Management Information Base

安全管理信息库

3.2.10 UA User Agent

用户代理

4 表示方法

层的表示方法按 GB 9387.1 执行。

除非特别说明,“服务”就是指“安全服务”。

5 安全服务与安全机制的一般描述

5.1 概述

广东省网络空间安全协会受控资料

本章讨论军用计算机网络安全体系结构中的安全服务以及实现这些服务的安全机制。它们是基本的安全服务，实际上在适当的层中和以适当的组合被调用，通常还要与通信网络的可用性服务和机制结合起来使用，以满足安全策略和/或用户要求。一些特定的安全机制可以同时实现几种安全服务，为了便于直接引用，实际建立的系统可以执行安全服务的某些特定组合。

5.2 安全服务

5.2.1 鉴别

鉴别服务可鉴别通信中的对等实体及其数据来源。鉴别服务需要存储本地的鉴别信息和为了鉴别而传送的数据(凭证)。

5.2.1.1 对等实体鉴别

当由(N)层提供时，对等实体鉴别服务将使(N＋1)实体确信与之打交道的对等实体正是所声称的(N＋1)实体。

这种服务在连接建立时或数据传送阶段使用，以证实一个或多个连接实体的身份。它仅在使用时方可确认一实体是否试图冒充或未授权重演前一次连接。对等实体鉴别可以是单向的也可以是双向的，可以带有效值检验也可以不带。它可以提供各种程度的保护。

5.2.1.2 数据源点鉴别

由(N)层提供时，这种服务将使(N＋1)实体确信数据来源正是所声称的对等(N＋1)实体。

数据源点鉴别服务证实数据单元的来源，但它不能防止数据单元的重复或修改。

5.2.2 访问控制

访问控制可为通过开放系统互连访问的资源提供保护，以免对其进行未授权使用。这些资源可能是通过开放系统互连协议访问的开放系统互连资源或非开放系统互连资源。访问控制服务适用于对一种资源进行的不同类型的访问(例如：使用通信资源、读、写或删除信息资源、运行资源)也适用于对一种资源进行的所有访问。

访问控制要与各种安全策略一致(见 6.2.1.1 条)。

5.2.3 数据保密性

数据保密性服务防止数据的未授权泄露。

5.2.3.1 连接保密性

连接保密性服务保证一次(N)连接上的所有(N)用户数据的保密性。

注：根据使用和层次的情况，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 无连接保密性

无连接保密性服务保证单个无连接(N)－SDU 中所有(N)用户数据的保密性。

5.2.3.3 选择字段保密性

选择字段保密性服务保证一次(N)连接上或单个无连接(N)－SDU 中的(N)用户数据中选定的字段的保密性。

5.2.3.4 通信业务流保密性

这种服务对信息实施保护，以防通过对通信业务流的侦察推断出保密信息。

广东省网络空间安全协会受控资料

5.2.4 数据完整性

数据完整性服务抵制主动威胁，以保证接收者收到的信息与发送者发送的信息完全一致。数据完整性服务有五种形式：可恢复的连接完整性、无恢复的连接完整性、选择字段连接完整性、无连接完整性和选择字段无连接完整性。

注：在一次连接上，可以将连接的开始时使用的对等实体鉴别服务和整个连接的存活期使用的数据完整性服务组合起来，以证实该连接上传输的所有数据单元的来源和完整性，并且还可检测出数据单元是否重复，例如通过使用顺序号。

5.2.4.1 可恢复的连接完整性

这种服务保证一次(N)连接上的所有(N)用户数据的完整性，并且检测整个 SDU 序列中的数据所遭到的任意修改、插入、删除或重演(可恢复)。

5.2.4.2 无恢复的连接完整性

同 5.2.4.1 条，但无法恢复。

5.2.4.3 选择字段连接完整性

这种服务保证在一次连接上传送的(N)－SDU 的(N)用户数据中所选字段的完整性，并且所采取的形式是确定所选字段是否已被修改、插入、删除或重演。

5.2.4.4 无连接完整性

由(N)层提供时，这种服务可保证发出请求的(N＋1)实体的完整性。

这种服务保证单一无连接 SDU 的完整性，而且可以确定所选字段是否已被修改，在一定程度上也能提供对重演的检测。

5.2.4.5 选择字段无连接完整性

保证单一无连接 SDU 内选择字段的完整性，采用的方式是确定选择字段是否已被修改。

5.2.5 抗抵赖

用于防止发送者发送数据后否认自己发送过的数据或数据的内容，或接收者收到数据后否认自己收到过数据或数据内容。抗抵赖服务有两种形式：带源点证明的抗抵赖和带交付证明的抗抵赖。

5.2.5.1 带源点证明的抗抵赖

为数据接收者提供数据来源证明，以防数据发送者否认发送过这些数据或数据的内容。

5.2.5.2 带交付证明的抗抵赖

为数据发送者提供数据交付证明，以防数据接收者事后否认接收过这些数据或数据的内容。

5.2.6 可用性

这种服务用来保护系统资源和防止拒绝服务，包括弱化导致传输延迟、误传或不传输保护信息的故障和防止偶然或有意的破坏。其主要目的是减少传送数据的延迟和尽量避免数据交付不到以确保需要时就能得到数据。通信网络的可靠性、灵活性、应急措施管理和预防性维护是支持可用性服务的重要机制。可用性服务有两种形式：检测和通告及安全性恢复。

5.2.6.1 检测和通告

它确保系统有能力识别出受到攻击、可能已进入不能使用的状态、已损坏或已发生故障等情况，并通告已检测出来的安全性临界状态以及应该实施何种正确操作。

广东省网络空间安全协会受控资料

5.2.6.2 安全性恢复

它规定授权的管理人员修理或清除安全性故障的起因、隔离使系统失效的部分以及使运行重新有效，从而回到安全的运行状态。

5.3 特定安全机制

为了提供5.2条所述服务，可在适当的(N)层中设置下列机制。

5.3.1 加密机制

5.3.1.1 加密机制可保证数据和通信业务流信息的保密性，可作为数字签名机制、访问控制机制、数据完整性机制、鉴别交换机制、通信业务量填充机制、路由选择控制机制和公证机制的一部分或它们的补充。

5.3.1.2 加密算法可以是可逆的，也可以是不可逆的，可逆加密算法可分为二种：

a. 对称(即秘密密钥)加密，知道了加密密钥就意味着知道了解密密钥，反之亦然；

b. 非对称(即公开密钥)加密，知道了加密密钥并不意味着知道了解密密钥，反之亦然。系统的这两种密钥有时被称作“公开密钥”和“秘密密钥”。

不可逆加密算法可使用密钥，也可以不使用密钥。使用密钥时，密钥可以是公开的也可以是秘密的。

5.3.1.3 除了某些不可逆加密算法外，加密机制的存在意味着要使用密钥管理机制，密钥管理方法的一些准则见8.4条。

5.3.2 数字签名机制

数字签名机制规定了两个过程：

a. 对数据单元签名；

b. 验证已签名的数据单元。

前者使用签名者的私有(唯一的和秘密的)信息；后者使用公开的规程和信息，但不能从中推断出签名者的私有信息。

5.3.2.1 签名过程是指用签名者的私有信息作为秘密密钥对数据单元进行加密或产生数据单元的密码校验值。

5.3.2.2 验证过程是指用公开规程和信息来验证签名是否使用签名者的私有信息产生的。

5.3.2.3 签名机制的本质特征是只能使用签名者私有信息鉴名。因此，当验证签名时，可在事后的任何时候向第三方(例如：审查员或仲裁人)证实只有私有信息的唯一持有者才能产生这个签名。

5.3.3 访问控制机制

访问控制机制是从计算机系统的处理能力方面对信息提供保护。它是信息保护的前端屏障。访问控制机制是按照事先确定的规则决定主体对客体的访问是否合法。

5.3.3.1 为了确定和实施实体的访问权，这种机制可以使用该实体已鉴别的身份，或使用有关该实体的信息(例如：它与一个已知的实体集的从属关系)，或使用该实体的权力。若该实体试图使用未授权资源或以不正当的访问方式使用授权资源，则访问控制功能将予以拒绝，同时告警和/或作为安全审计跟踪的一部分记录下来。对于无连接数据传输，给发送者拒绝访问的任何通知，只能作为强加在源点访问控制的结果来提供。

广东省网络空间安全协会受控资料

5.3.3.2 访问控制机制可基于下列一种或多种方法来实现：

a. 存放对等实体访问权的访问控制信息库。这些信息可以由授权中心或由正被访问的实体保存，信息的形式可以是一个访问控制表也可以是等级结构或分布结构的矩阵。这里预先假定对等实体的鉴别已得到保证；

b. 鉴别信息(如口令)。拥有和出示这一信息，便证明正在进行访问的实体已被授权；

c. 权力。拥有和出示它，便证明有权访问由该权力规定的实体或资源；

注：权力应是不可伪造的，并以可信赖的方式传递。

d. 安全标志。当与一个实体相关联时，这种安全标志可以用于表示同意或拒绝访问，通常依安全策略而定；

e. 试图访问的时间；

f. 试图访问的路由；

g. 访问的持续时间。

5.3.3.3 访问控制机制可应用于通信联系的端点和/或任一中间点。

加在源点或任一中间点的访问控制可用来确定发送者是否被授权与指定的接收者进行通信，和/或是否被授权使用所要求的通信资源。

在无连接数据传输目的端上的对等级访问控制机制的要求在源点必须事先知道，并录入安全管理信息库中(见 6.2 条和 8.1 条)。

5.3.4 数据完整性机制

5.3.4.1 数据完整性可分为单个数据单元或字段的完整性和数据单元流或字段流的完整性。尽管没有第一类完整性服务，无法提供第二类完整性服务，但是这两种完整性服务通常还是由不同机制提供的。

5.3.4.2 确定单个数据单元的完整性包括两个过程，一个在发送端，一个在接收端。发送实体附加给数据单元一个量值，这个量值是数据本身的函数。这个量值可以是象分组校验码那样的追加信息，也可以是一个密码校验值，并且它本身可被加密。接收实体产生一个对应的量值，并与收到的量值相比较，以检测数据是否在传输过程中被修改过。单靠这种机制不能防止单个数据单元重演。在网络体系结构的适当层上，操纵检测可在该层或高层进行恢复活动(例如，通过重传或纠错)。

5.3.4.3 对于连接方式数据传送，保护数据单元序列的完整性(即：防止乱序和数据的丢失、重演、插入或修改)，还需要某些显示的序列形式，例如序列号、时标或密码链。

5.3.4.4 对于无连接数据传送，时标可提供一定的保护，以防止单个数据单元重演。

5.3.5 鉴别交换机制

鉴别交换是以交换信息的方式来确认实体身份的一种机制。

5.3.5.1 可用于鉴别交换的技术有：

a. 使用鉴别信息，例如，由发送实体提供、由接收实体验证的口令；

b. 密码技术；

c. 使用该实体的特征和/或拥有物。

5.3.5.2 这种机制可设置到(N)层，以提供对等实体鉴别。若这种机制在鉴别实体时得到否

广东省网络空间安全协会受控资料

定，将拒绝或终止连接，同时在安全审计跟踪中产生一个记录和/或报告给安全管理中心。

5.3.5.3 采用密码技术时，这些技术可与“握手”协议相结合以防止重演(即确保存活期)。

5.3.5.4 鉴别交换技术的选用取决于其使用环境。有时，它们必须与下列技术结合使用：

a. 时标和同步时钟；

b. 双方“握手”和三方“握手”(分别对应于单方鉴别和相互鉴别)；

c. 由数字鉴名和/或公证机制实现的抗抵赖服务。

5.3.6 通信业务量填充机制

这种机制主要是防止非法者在线路上监听数据并对其进行流量分析。采用的方法一般由保密装置在无信息传输时，连续发出伪随机序列，使得非法者不知哪些是有用信息，哪些是无用信息。这种机制仅在通信业务量填充受到保密性服务的保护时才有效。

5.3.7 路由选择控制机制

这种机制可使信息发送者选择特殊的路由，以保证数据完全。

5.3.7.1 路由可以动态选取也可以预定，以便仅使用物理上安全的子网络、中继或链路。

5.3.7.2 检测到持续的操纵攻击时，端系统可能会通知网络服务提供者另选路由建立连接。

5.3.7.3 安全策略可能禁止携带安全标记的数据通过某些子网络、中继或链路。连接的发起者(或无连接数据单元的发送者)可以提出有关路由选择的警告，要求回避某些特定的子网络、链路或中继。

5.3.8 公证机制

在两个或多个实体间通信的数据特性(如完整性、源点、时间和目的地)可以由公证机制加以保证，这种保证由第三方公证人提供。公证人为通信实体所信任，并掌握必要的信息，以可证实方式提供所需要的保证。根据公证人提供的服务，每个通信实例可采用数字签名、加密和完整性机制。当调用上述机制时，数据可通过受保护的通信实例和公证人在各通信实体之间进行通信。

广东省网络空间安全协会受控资料

5.4 普遍安全机制

普遍安全机制不是为任何特定服务而设的。因此，第7章在任意特定层上均未对其加以明确的说明。有些普遍安全机制属于安全管理问题(见第8章)。这些机制的重要性通常与要求的安全级直接相关。

5.4.1 可信功能

5.4.1.1 为了扩充其它安全机制的范围或建立其有效性，必须使用可信功能。直接提供安全机制或访问安全机制的任意功能都应是可信赖的。

5.4.1.2 用于保证对这些硬件和软件信赖的手段不属于本标准讨论的范围，而且这些手段总是随着已观察到的威胁的等级和被保护信息的价值而变化。

5.4.1.3 通常，这些手段代价高且难于实现。解决办法是：选择一个允许安全功能在一些模块中实现的体系结构，这些模块可以与非安全功能分开制作，并由非安全的相关功能提供。

5.4.1.4 在受保护层的上层，相关的任何保护必须由另外的手段提供，例如通过适当的可信功能。

5.4.2 安全标记

包含数据项的资源可能具有与这些数据相关联的安全标记，例如：指明安全敏感等级的标记。通常，传送数据时需要同时传送适当的安全标记。安全标记可以是与被传送的数据相关的附加数据，也可以是隐含的信息，例如通过使用一个特定密钥加密数据来隐含或由数据上下文（例如数据源点或路由）来隐含。显示安全标记必须能清晰地标识出来，以便验证。另外，它们必须安全可靠地依附于与之相关联的数据。

5.4.3 事件检测

5.4.3.1 与安全有关的事件检测包括对安全明显侵害事件和“正常”事件（例如成功的访问或登录）的检测。与安全有关的事件可由包括安全机制的开放系统互连实体来检测。构成事件的技术规范由事件处置管理活动维护（见 8.3.1 条）。检测各种与安全有关的事件（例如：特定的安全侵害、特定的选择事件、总发生次数溢出）后可能产生下列动作：

a. 事件的本地报告；

b. 事件的远程报告；

c. 登录事件（见 5.4.3 条）；

d. 恢复动作（见 5.4.4 条）。

5.4.3.2 该领域的标准化将要考虑的问题是传送与事件报告和事件登录有关的信息，以及用于事件报告和事件登录传输的语法和语义。

5.4.4 安全审计跟踪

5.4.4.1 安全审计跟踪是一种有价值的安全机制，可通过事发后的安全审计来检测和调查安全遭到的破坏。安全审计是对系统记录和活动的独立评估和考核，以测试系统控制得是否充分，确保与既定策略和操作规程相一致，有助于进行侵害评估，并指出控制、策略和程序的变化。安全审计需要安全审计跟踪中与安全有关的记录信息和从安全审计跟踪中得来的分析和报告信息。登录或记录被视为一种安全机制，并在本条中描述。而分析和报告生成则被视为一种安全管理功能（见 8.3.2 条）。

5.4.4.2 通过指明所记录的与安全有关的事件的类别（例如明显侵害安全或完成成功操作），安全审计跟踪信息的收集可适应各种需要。

已知安全审计跟踪的存在可对潜在的安全攻击源的攻击起到威慑作用。

5.4.4.3 开放系统互连安全审计跟踪将考虑选择哪些信息进行登录，在什么条件下对信息进行登录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

安全恢复机制可应事件处理和管理功能等机制的请求，在应用一组规则后采取恢复动作。恢复动作可分为下述三种：

a. 立即的；

b. 暂时的；

c. 长期的。

立即动作就是立即放弃操作（如断开），暂时动作就是使实体暂时无效，而长期动作则是把实体列入“黑名单”或更改密钥。

5.4.5.1 标准化问题包括恢复动作协议与安全恢复管理协议（见 8.3.3 条）。

全国信息安全标准化技术委员会资料

5.5 安全服务与安全机制的关系

安全服务是由一种或多种安全机制提供，而有的安全机制又可以用于多种服务，表1仅列出了它们的对应关系，更详细的描述见第6章。

表1 安全服务与安全机制的关系

机制 / 服务	加密	数字签名	访问控制	数据完整性	鉴别交换	通信业务量填充	路由选择控制	公证
对等实体鉴别	Y	Y	·	·	Y	·	·	·
数据源点鉴别	Y	Y	·	·	·	·	·	·
访问控制服务	·	·	Y	·	·	·	·	·
连接保密性	Y	·	·	·	·	·	Y	·
无连接保密性	Y	·	·	·	·	·	Y	·
选择字段保密性	Y	·	·	·	·	·	·	·
通信业务流保密性	Y	·	·	·	·	Y	Y	·
可恢复的连接完整性	Y	·	·	Y	·	·	·	·
无恢复的连接完整性	Y	·	·	Y	·	·	·	·
选择字段连接完整性	Y	·	·	Y	·	·	·	·
无连接完整性	Y	Y	·	Y	·	·	·	·
选择字段无连接完整性	Y	Y	·	Y	·	·	·	·
带源点证明的抗抵赖	·	Y	·	Y	·	·	·	Y
带交付证明的抗抵赖	·	Y	·	Y	·	·	·	Y

注："Y"表示这种机制可单独或与其它机制组合提供此项安全服务；
"·"表示这种机制不提供此项安全服务。

广东省网络空间安全协会受控资料

6 安全服务、安全机制与层的关系

6.1 安全分层原则

6.1.1 确定各层的安全服务以及在这些层中配置安全机制时应遵循下列原则：

a. 减少实现一种服务的可选方案；
b. 允许通过在多个层上提供安全服务来建立安全系统；
c. 安全性所需的附加功能不应重复现有的开放系统互连功能；
d. 避免破坏层的独立性；
e. 减少可信功能的总量；

f. 当实体依赖于下层实体提供的安全机制时，应以不破坏安全的方式构造中间各层；

g. 定义层的附加安全功能时，应允许这些附加功能作为自容模块来实现；

h. 本标准适用于由包括所有七层在内的端系统组成的开放系统和中继系统。

6.1.2 各层的服务的定义可能需要修改，以满足安全服务的请求，无论要求的安全服务由该层提供还是由下层提供。

6.2 受保护的(N)服务的调用、管理和使用模型

本条应结合第8章“安全管理”来阅读。管理实体可以通过管理接口和/或服务调用来激活安全服务与安全机制。

6.2.1 确定通信实例保护特点

6.2.1.1 概述

本条阐述面向连接和无连接通信实例保护的调用。在面向连接通信时，请求和获准保护服务通常是在连接时刻建立；在无连接服务调用时，请求和获准保护是对每个单元数据请求进行的。

为了简化下列说明，“服务请求”指连接建立或单元数据请求。可以通过请求选择字段保护来完成被选数据的保护调用，例如可以通过建立几个具有不同的保护类型或等级的连接来完成。

这种安全体系结构适应多种安全策略，基于规则的安全策略、基于身份的安全策略或两者兼有之。这种安全体系结构还适应多种保护，行政强加的、动态选择的及两者兼有之。

6.2.1.2 服务请求

对于每个(N)服务请求，(N+1)实体可以请求所需要的目标安全保护。(N)服务请求将指明安全服务、参数以达到目标安全保护。

在每次通信前，(N)层必须访问安全管理信息库(SMIB)(见8.1条)。SMIB存有与(N+1)实体相关联的行政管理强制保护所需要的信息。还需要可信功能来实施这些行政管理强制的安全要求。

提供面向连接通信实例的安全特点，需要与要求的安全服务进行协商，机制和参数的协商过程可作为一个单独的过程实现，或作为正常连接建立过程的组成部分。

当协商作为一个单独过程实现时，协商的结果(即提供这种安全服务所需的安全机制的类型和安全参数)存入SMIB。

当协商作为正常连接建立过程的组成部分实现时，(N)实体间的协商结果将暂存于SMIB中。在协商之前，(N)实体将访问SMIB以获得协商所需要的信息。

若服务请求违反了记录在SMIB中为该(N+1)实体所作的行政管理强加的要求时，(N)层将拒绝这一服务请求。

(N)层也将给被请求的保护服务添加上安全服务，这些安全服务在SMIB中定义为强制控制，以达到目标安全保护。

若(N+1)实体不指明目标安全保护，那么N层将遵循与SMIB相一致的安全策略，在SMIB中为(N+1)实体所定义的区段内使用默认安全保护，使通信能够继续进行。

6.2.2 保护服务的提供

全国信息网络与空间安全协会受控资料

在确定了行政管理强加的与动态选取的安全要求的组合之后(见 6.2.1 条),(N)层将试图最低限度达到目标保护,可采用下述方法实现:

a. 在(N)层中直接调用安全机制;

b. 从(N－1)层请求保护服务,这时通过(N)层中可信功能和/或特定安全机制的组合,使保护范围必须扩展到(N)服务。

注:这并不一定意味着(N)层中所有的功能必须是可信赖的。

因此,(N)层决定能否达到受请求的目标保护。若不能,就不进行任何通信。

6.2.2.1 受保护 N 连接的建立

本条讨论(N)层内提供的服务(与之相对的是对(N－1)服务的依赖)。

在某些协议中,为得到满意的目标保护,操作顺序是至关重要的。

6.2.2.1.1 出访问控制

(N)层可实施出访问控制,即可以在本地由 SMIB 确定能否建立受保护的(N)连接。

6.2.2.1.2 对等实体鉴别

若目标保护包插对等实体鉴别,或者根据 SIBM 得知目的地(N)实体要求对等实体鉴别,则就必须进行鉴别交换。这可以利用双方或三方握手来提供所需要的单向或相互鉴别。

有时,鉴别交换可以合并到正常的(N)连接建立规程中,在其它情况下,鉴别交换可以与(N)连接建立分开进行。

6.2.2.1.3 访问控制服务

目的地(N)实体或中间实体可以强加访问控制约束。若远程访问控制机制要求特定信息,那么(N)始发实体在(N)层协议中或通过管理信道提供。

6.2.2.1.4 保密性

若选定了全保密性服务或选择保密性服务,就必须建立一个受保护的(N)连接,这必须包括建立适当的工作密钥和协商用于此次连接的密码参数。这可在鉴别交换中预定或通过一个单独的协议来完成。

6.2.2.1.5 数据完整性

若选定了可恢复或无恢复的所有(N)用户数据的完整性或选择字段的完整性,则必须建立一个受保护的(N)连接。这可能与为提供保密性服务而建立的连接相同,并且它可提供鉴别。同样的考虑适用于受保护(N)连接的保密性服务。

6.2.2.1.6 抗抵赖服务

若选择了带源点证明的抗抵赖,则必须建立适当的密码参数或建立带公证实体的受保护连接。

若选择了带交付证明的抗抵赖,则必须建立适当的参数(与带源点证明的抗抵赖所要求的参数不同)或建立带有公证实体的受保护连接。

注:由于密码参数未协商好(可能没有适当的密钥),或遭受访问控制机制的拒绝,受保护(N)连接的建立可能失败。

6.2.3 受保护(N)连接的操作

6.2.3.1 在受保护(N)连接的数据传送阶段,必须提供经协商的保护服务。

在(N)服务范围内,下列服务是可用的:

广东省网络空间安全协会受控资料

a. 对等实体鉴别(间隔进行)；

b. 选择字段保护；

c. 主动攻击报告(例如：若正在提供的服务为"无恢复的连接完整性"时，发生了对数据的操纵时。参见5.2.4.2条)。

另外，还可能需要：

a. 安全审计跟踪记录；

b. 事件检测与处理。

6.2.3.2 适用于选择性应用的服务有：

a. 保密性；

b. 数据完整性(可能与鉴别一起)；

c. 抗抵赖(接收者抵赖或发送者抵赖)。

注：①推荐两种标记选定服务应用数据项目的技术。一是使用粗体，假定表示层可以识别出哪种字体需要保护；二是给需要特定保护服务的数据项加上某种形式的标志。

②提供有选择的抗抵赖服务可能是基于下述情况：在两个(N)实体就数据项最后版本取得相互认可之前，已进行过某种形式的协商对话。这时，预定的接收者会要求发送者把抗抵赖服务(带源点证明的和带交付证明的)加到数据项的最后认可的版本中。发送者请求并获得这些服务，发送数据项，随即可收到接收者已收到数据项并已确认的通知。抗抵赖服务向发送者和接收者保证已收到成功传送的数据项。

③带源点证明的抗抵赖和带交付证明的抗抵赖服务均由发送者调用。

6.2.4 受保护无连接数据传输的提供

并非所有用于面向连接协议的安全服务都能用于无连接协议。例如，防止删除、插入和重演攻击的保护就必须由面向连接的更高的层次提供。对重演攻击的有限保护可由时标机制提供。此外，其它很多安全服务无法提供与面向连接协议所能达到的同等的安全强度。

适用于无连接数据传输的保护服务有：

a. 对等实体鉴别(见5.2.1.1条)；

b. 数据源点鉴别(见5.2.1.2条)；

c. 访问控制服务(见5.2.2条)；

d. 无连接保密性(见5.2.3.2条)；

e. 选择字段保密性(见5.2.3.3条)；

f. 无连接完整性(见5.2.4.4)条；

g. 选择字段无连接完整性(见5.2.4.5条)；

h. 带源点证明的抗抵赖(见5.2.5.1条)。

这些服务由加密机制、数字签名机制、访问控制机制、路由选择机制、数据完整性机制、公证机制和/或鉴别交换机制提供(见5.3条)

无连接数据传输的发送者必须保证他的每个SDU中均含有使SDU到达目的地所需要的全部信息。

7 安全服务与安全机制的配置

本章定义了开放系统互连基本参考模型框架内提供的安全服务，并概述了实现方法。安

产品信息安全协会受控资料

全服务均是按需求可选择的。

本章所指一个特定层任意选定的安全服务，如不另作说明，则由设置在该层的安全机制提供。如第6章所述，多个层将提供特定的安全服务，这些安全服务不一定总是由这些层本身提供，也可以利用下层提供的相应的安全服务。即使某一层不提供安全服务，该层的服务定义也可能需要修改，以允许安全服务的请求传递到下层。

注：①普遍安全机制不在本章讨论，参见5.4条；

②各种加密机制的应用场合见附录C(参考件)。

7.1 物理层

7.1.1 服务

物理层单独或组合提供下述两种安全服务：

a. 连接保密性；

b. 通信业务流保密性。

通信业务流保密性服务采取全通信业务流保密性和有限通信业务流保密性两种形式。前者只能为双向同时、同步、点对点等传输类型提供；后者可为异步传输等其它传输类型提供。

这些安全服务只能对付被动威胁，可用于点对点或多个对等实体通信。

7.1.2 机制

数据流总加密是物理层的主要安全机制。

一种只用于物理层的、特定加密形式是传输安全(即扩频安全)。

物理层保护是由一种操作透明的加密装置提供的，物理层保护的目标是保护整个物理服务数据比特流，并且提供通信业务流保密性。

广东省网络空间安全协会受控资料

7.2 数据链路层

7.2.1 服务

数据链路层仅提供连接保密性和无连接保密性两种安全服务。

7.2.2 机制

加密机制提供数据链路层的安全服务，参见附录C(参考件)。

链路层附加的安全保护功能是在正常的层传输功能之前和正常的层接收功能之后执行。即安全机制是在所有这些正常的层功能之上建立并使用的。

数据链路层的加密机制对于链路层协议是敏感的。

7.3 网络层

网络层在内部组织起来，提供执行下列操作协议：

a. 子网访问；

b. 与子网相关的收敛；

c. 与子网无关的收敛；

d. 中继与路由选择。

7.3.1 服务

执行与开放系统互连网络服务相关的子网络访问功能的协议可以提供下列安全服务：

a. 对等实体鉴别；

b. 数据源点鉴别；

c. 访问控制服务；

d. 连接保密性；

e. 无连接保密性；

f. 通信业务流保密性；

g. 无恢复的连接完整性；

h. 无连接完整性。

这些安全服务可以单独提供或组合提供。由执行与提供从端系统到端系统的开放系统互连网络服务相关的中继和路由选择操作的协议所提供的安全服务，与由执行子网络访问操作的协议所提供的安全服务是相同的。

7.3.2 机制

7.3.2.1 执行与提供从端系统到端系统的开放系统互连网络服务相关联的子网络访问操作和中继与路由选择操作的协议均使用相同的安全机制。路由选择在这一层上执行，因此，路由选择控制也在这层执行。上述安全服务列举如下：

a. 对等实体鉴别服务由密码导出的或受保护的鉴别交换、受保护的口令交换和签名机制的适当组合提供；

b. 数据源点鉴别服务由加密或签名机制提供；

c. 访问控制服务由适当使用特定访问控制机制提供；

d. 连接保密性服务由加密机制和路由选择控制提供；

e. 无连接保密性服务由加密机制和路由选择控制提供；

f. 通信业务流保密性服务由通信业务量填充机制并配以网络层或网络层以下的一种保密性服务或路由选择控制而获得；

g. 无恢复的连接完整性服务由数据完整性机制，有时结合加密机制提供；

h. 无连接完整性服务由数据完整性机制，有时结合加密机制提供。

7.3.2.2 协议中的机制提供横贯单个子网络的服务，协议则执行与提供从端系统到端系统的开放系统互连网络服务相关的子网络访问操作。

由子网络管理机构施加的子网络保护将在子网络访问协议的支配下实施，但发送时通常在正常子网络功能之前实施，接收时通常用在正常子网功能之后实施。

7.3.2.3 由协议规定的机制横贯一个或多个互联网络提供服务。协议执行与提供从端系统到端系统的开放系统互连网络服务相关的中继和路由选择操作。

这些机制当发送时是在中继和路由选择功能之前，接收时是在中继和路由选择功能之后调用。在路由选择控制机制情况下，从 SMIB 导出适当的约束信息，然后将数据与这些必要的路由选择约束一并传给中继与路由选择功能。

7.3.2.4 网络层中的访问控制有多种用途，例如，它允许端系统控制网络连接的建立，拒绝无用呼叫，它还允许一个或多个子网络去控制网络层资源的使用。在某些情况下，这后一用途与使用网络的费用有关。

注：网络连接的建立通常要收取子网络行政管理费，通过控制访问和选取反向付费或其它网络特定参数可使费用降到

广东省密码管理局全部会受控资料

最低程度。

7.3.2.5 特定子网络要求可能对执行与提供从端系统到端系统的开放系统互连网络服务相关的子网络访问操作的协议施加访问控制机制。当访问控制机制由执行与提供从端系统到端系统的开放系统互连网络服务相关的中继和路由选择操作协议时，可用中继实体方法控制子网络的访问，也可用控制对端系统的访问。显然，访问控制的这种隔离程度很低，只能在网络层实体之间区分。

7.3.2.6 若通信业务量填充机制与网络层加密机制(或物理层保密性服务)结合使用，则可获得适度的通信业务流保密性。

7.4 运输层

7.4.1 服务

运输层单独或组合提供的安全服务有：

a. 对等实体鉴别；

b. 数据源点鉴别；

c. 访问控制服务；

d. 连接保密性；

e. 无连接保密性；

f. 可恢复的连接保密性；

g. 无恢复的连接保密性；

h. 无连接完整性。

7.4.2 机制

上述安全服务由下列相应机制提供：

a. 对等实体鉴别服务由密码导出的或受保护的鉴别交换、受保护的口令交换与签名机制的适当组合提供；

b. 数据源点鉴别由加密或签名机制提供；

c. 访问控制服务由适当使用特定的访问控制机制提供；

d. 连接保密性服务由加密机制提供；

e. 无连接保密性服务由加密机制提供；

f. 可恢复的连接完整性服务由数据完整性机制提供，有时由加密机制与之配合；

g. 无恢复的连接完整性服务由数据完整性机制提供，有时由加密机制与之配合；

h. 无连接完整性服务由数据完整性机制提供，有时由加密机制与之配合。

保护机制的运行方式将保证安全服务可被个体运输连接所调用。这种保护的结果将个体运输连接同所有其它运输连接完全隔离。

7.5 会话层

7.5.1 服务

该层不提供安全服务。

7.6 表示层

7.6.1 服务

广东省网络空间安全协会受控资料

表示层将提供设施，以支持应用层对应用进程提供的下列安全服务：

a. 连接保密性；

b. 无连接保密性；

c. 选择字段保密性；

d. 通信业务流保密性；

e. 对等实体鉴别；

f. 数据源点鉴别；

g. 可恢复的连接完整性；

h. 无恢复的连接完整性；

j. 选择字段连接完整性；

k. 无连接完整性；

m. 选择字段无连接完整性；

n. 带源点证明的抗抵赖；

p. 带交付证明的抗抵赖。

注：表示层提供的设施将是那些依赖于只能在数据传送语法编码上操作的机制，包括那些诸如基于密码技术上的机制。

7.6.2 机制

下列安全服务和支持机制，可设置在表示层中，并同应用层安全机制相配合以提供应用层安全服务：

a. 对等实体鉴别服务由语法变换机制(例如加密)支持；

b. 数据源点鉴别服务由加密或签名机制支持；

c. 连接保密性服务由加密机制支持；

d. 无连接保密性服务由加密机制支持；

e. 选择字段保密性服务由加密机制支持；

f. 通信业务流保密性服务由加密机制支持；

g. 可恢复的连接完整性服务由数据完整性机制支持，有时由加密机制与之配合支持；

h. 无恢复的连接完整性服务由数据完整性机制支持，有时由加密机制与之配合；

j. 选择字段连接完整性服务由数据完整性机制支持，有时由加密机制与之配合；

k. 无连接完整性服务由数据完整性机制支持，有时由加密机制与之配合；

m. 选择字段无连接完整性服务可由数据完整性机制支持，有时由加密机制与之配合；

n. 带源点证明的抗抵赖服务由数据完整性、签名与公证机制适当组合支持；

p. 带交付证明的抗抵赖服务由数据完整性、签名和公证机制适当组合支持；

用于数据传送的加密机制设置在上层时，将包括在表示层中。

以上所列的某些安全服务也可以由设在应用层中的安全机制选择提供。

只有保密性安全服务可以由设在表示层的安全机制全部提供。

表示层中的安全机制在发送时作为传送语法变换的最后阶段运行，在接收时作为该变换进程的初始阶段运行。

7.7 应用层

广东省网络空间安全协会受控资料

7.7.1 服务

应用层可单独或组合提供下列安全服务：

a. 对等实体鉴别；

b. 数据源点鉴别；

c. 访问控制服务；

d. 连接保密性；

e. 无连接保密性；

f. 选择字段保密性；

g. 通信业务流保密性；

h. 可恢复的连接完整性；

j. 无恢复的连接完整性；

k. 选择字段连接完整性；

m. 无连接完整性；

n. 选择字段无连接完整性；

p. 带源点证明的抗抵赖；

q. 带交付证明的抗抵赖。

在实开放系统中，认定通信各方的鉴别支持开放系统互连和非开放系统互连资源（例如：文件、软件、终端、打印机）的访问控制。

在一次通信实例中的具体安全要求，包括数据保密性、完整性与鉴别，均可由开放系统互连安全管理或应用层管理根据 SMIB 中的信息以及应用进程提出的请求来确定。

7.7.2 机制

应用层中的安全服务由下列机制提供：

a. 对等实体鉴别服务由应用实体间传送的鉴别信息提供，这些信息受表示层或下层的加密机制的保护；

b. 数据源点鉴别服务由签名机制或下层的加密机制支持；

c. 对实开放系统这些方面的访问控制服务与开放系统互连有关，例如，与特定系统或远程应用实体进行通信的能力，可以由应用层与下层的访问控制机制组合提供；

d. 连接保密性服务由下层加密机制支持；

e. 无连接保密性服务由下层加密机制支持；

f. 选择字段加密机制服务由表示层的加密机制支持；

g. 有限的通信业务流保密性服务由应用层的通信业务量填充机制并配合一个与下层的保密性服务支持；

h. 可恢复的连接完整性服务由下层的数据完整性机制（有时加密机制与之配合）支持；

j. 无恢复的连接完整性服务由下层的数据完整性机制（有时加密机制与之配合）支持；

k. 选择字段连接完整性服务由表示层的数据完整性机制（有时加密机制与之配合）支持；

m. 无连接完整性服务由下层的数据完整性机制（有时加密机制与之配合）支持；

n. 选择字段无连接完整性服务由表示层的数据完整性机制（有时加密机制与之配合）支

广东省网络空间安全协会受控资料

持；

p. 带源点证明的抗抵赖服务由签名机制与下层数据完整性机制适当组合支持，并与第三方公证相配合；

q. 带交付证明的抗抵赖服务由签名机制与下层数据完整性机制适当组合支持，并与第三方公证相配合。

若公证机制用来提供抗抵赖服务，则可将其作为可信赖的第三方。为了解决纠纷，公证机制具有以传送形式(即传送语法)重放的数据单元记录。公证机制可以使用下层的保护服务。

7.7.3 非开放系统互连安全服务

应用进程本身基本上可以提供所有服务，并且使用与本标准在体系结构的各层上所描述的相应机制相同的机制。这种使用已超出开放系统互连服务、协议定义及开放系统互连体系结构的范围，但并不与之冲突。

7.8 安全服务与层的关系说明

表2示出了参考模型各层所提供的特定安全服务。在某一特定层上设置某种服务的理由见附录B(参考件)。

表2 安全服务与层的关系

层 / 安全服务	1	2	3	4	5	6	7[1)]
对等实体鉴别	·	·	Y	Y	·	·	Y
数据源点鉴别	·	·	Y	Y	·	·	Y
访问控制服务	·	·	Y	Y	·	·	Y
连接保密性	Y	Y	Y	Y	·	·	Y
无连接保密性	·	Y	Y	Y	·	·	Y
连接字段保密性	·	·	·	·	·	·	Y
通信业务流保密性	Y	·	Y	·	·	·	Y
可恢复的连接完整性	·	·	·	Y	·	·	Y
无恢复的连接完整性	·	·	Y	Y	·	·	Y
选择字段连接完整性	·	·	·	·	·	·	Y
无连接完整性	·	·	Y	Y	·	·	Y
选择字段无连接完整性	·	·	·	·	·	·	Y
带源点证明的抗抵赖	·	·	·	·	·	·	Y
带交付证明的抗抵赖	·	·	·	·	·	·	Y

广东省网络空间安全协会受控资料

注：①“Y”表示服务作为提供者的选项列入该层标准中，“·”表示不提供该服务；

②表 2 中各项并非同等重要，而是存在较大差别；

③网络层中安全服务的配置见 7.3.2 条。安全服务在网络层中的位置对所提供的服务的性能和范围的影响很大；

④表示层包含许多支持应用层提供安全服务的安全设施。

1)对第 7 层而言，应用进程本身即可提供安全服务。

8 安全管理

8.1 概述

8.1.1 开放系统互连安全管理包括开放系统互连安全管理和开放系统互连管理的安全两个方面。开放系统互连安全管理涉及这样一些操作，它们本身并非正常的通信情况，但却是支持和控制这些通信的安全必不可少的。

注：通信服务的有效性取决于网络设计和/或网络管理协议，因此需要对网络设计和/或网络管理协议进行适当的选择，以防拒绝服务。

8.1.2 分布式开放系统的行政管理机构强加的安全策略可有多种，开放系统互连安全管理标准应支持这些策略。受单一安全策略支配的、由单个授权机构管理的多个实体构成的集合有时被称为“安全域”，安全域及其相互作用是一个有待进一步开拓的重要领域。

8.1.3 开放系统互连安全管理是指开放系统互连安全服务和安全机制的管理。这种管理要求为安全服务和安全机制分发管理信息，并搜集与这些服务与机制操作有关的信息。例如，密钥的分发、设置行政管理机构强加的安全选择参数，报告正常和异常的安全事件(审计跟踪)以及服务的激活与停止。安全管理并不强调在呼叫特定安全服务的协议(例如连接请求中的参数)中传递与安全有关的信息。

8.1.4 安全管理信息库(SMIB)是概念上的贮藏地，存放开放系统需要的与安全有关的全部信息，这个概念对信息的存储形式和实施方式不提出要求。但是，每个端系统必须包含必需的本地信息，以使它能够执行一个适当的安全策略。从(逻辑上或物理上)成组的端系统必须执行一致的安全策略的意义上讲，SMIB 是一个分布式信息库。实际上，SMIB 的某些部分可以与 MIB 结合成一体，也可以分开。

注：SMIB 可有多种实现办法，例如：

a. 数据表；

b. 文卷；

c. 嵌入实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)以及传送管理信息的通信信道可能很脆弱，因此要格外谨慎，以确保管理协议和信息受到保护，不致削弱对通常的通信所提供的安全保护。

8.1.6 安全管理要求各系统的行政管理机构间交换与安全有关的信息，以便于建立或扩充 SMIB。在有些情况下，与安全有关的信息经由非开放系统互连通信路径传递，此时本地系统管理员将采用尚未开放系统互连标准化的方法修改 SMIB。在另外一些情况下，与安全有关的信息需要在开放系统互连通信路径上交换，这时这些信息将在运行于实开放系统中的两个安全管理应用间传送。安全管理应用将利用这些信息修改 SMIB。这种修改可能需要事先对相应的安全管理员进行授权。

8.1.7 为了在开放系统互连通信信道上交换与安全有关的信息，应明确应用协议。

8.2 开放系统互连安全管理的分类

开放系统互连安全管理活动分三类：

a. 系统安全管理；

b. 安全服务管理；

c. 安全机制管理。

此外，还必须考虑开放系统互连管理本身的安全(见 8.2.4 条)。

8.2.1 系统安全管理

系统安全管理是指整个开放系统互连环境的安全管理方面，下面列举了属于这类安全管理的典型活动：

a. 安全策略的综合管理，包括一致性的修改与维护；

b. 与其它开放系统互连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. 事件处理管理(见 8.3.1 条)；

e. 安全审计管理(见 8.3.2 条)；

f. 安全恢复管理(见 8.3.3 条)。

8.2.2 安全服务管理

安全服务管理是指特定的安全服务管理，下面列出了管理某种特定安全服务时可能执行的典型活动：

a. 为该服务确定与指派安全保护目标；

b. 指定与维护选择规则(存在可选情况时)，用以选取为提供所需要的安全服务而使用的特定安全机制；

c. 协商(本地与远程的)那些需要事先取得管理同意的可用安全机制；

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，用来提供行政管理强加的安全服务；

e. 与别的安全服务管理功能和安全机制管理功能的相互作用。

8.2.3 安全机制管理

安全机制管理是指特定安全机制的管理。下面列出的仅是典型的安全机制管理功能，并非全部安全机制管理：

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. 鉴别管理；

g. 通信业务量填充管理；

h. 路由选择控制管理；

j. 公证管理。

广东省网络空间安全协会受控资料

以上安全机制管理功能详见 8.4 条。

8.2.4 开放系统互连管理的安全

所有开放系统互连管理功能和开放系统互连管理信息通信的安全均是开放系统互连安全的重要组成部分。这类安全管理选取适当的安全服务与安全机制，以使开放系统互连管理协议和信息获得足够的保护(见 8.1.5 条)。例如，管理信息库的管理实体间的通信通常需要某种形式的保护。

8.3 系统安全管理活动

8.3.1 事件处理管理

在开放系统互连中可看到的属于事件处理管理包括远程报告明显违反系统安全的企图以及修改触发事件报告的门限值。

8.3.2 安全审计管理

安全审计管理包括：

a. 选择将要记录和/或远程收集的事件；

b. 授予或取消对所选事件进行审计跟踪日志记录的能力；

c. 远程收集选定的审计记录；

d. 安全审计报告整理。

8.3.3 安全恢复管理

安全恢复管理包括：

a. 维护对已发生的或可能发生的违反安全事件作出反应的规则；

b. 远程报告明显违反系统安全的事件；

c. 安全管理者的相互作用。

8.4 安全机制管理功能

8.4.1 密钥管理

密钥管理包括：

a. 根据要求的安全级定时生成合适的密钥；

b. 根据访问控制要求，确定应由哪些实体接收密钥的拷贝；

c. 以安全的方式生成密钥，并将这些密钥分发给实开放系统中的实体实例。

需要说明的是，有些密钥管理功能将在开放系统互连环境之外执行，例如以可信赖方式分发密钥。

在联系中交换工作密钥属正常层协议功能。工作密钥的选取可以通过访问密钥管理中心来完成，也可以由管理协议预先分发。

8.4.2 加密管理

加密管理包括：

a. 与安全标志和密钥管理的相互作用；

b. 建立密码参数；

c. 密码同步。

加密机制的存在意味着密钥管理和采用共同方式调用密码算法的使用。

广东省网络空间安全协会受控资料

由加密提供的保护判别等级取决于开放系统互连环境内的哪些实体独立地使用密钥，通常还取决于安全体系结构，特别是密钥管理机制。

为获得密码算法的共同调用，可使用密码算法寄存器或在实体间事先协商。

8.4.3 数字签名管理

数字签名管理包括：

a. 与密钥管理的相互作用；

b. 建立密码参数和加密算法；

c. 在通信实体和可能的第三方之间使用协议。

注：数字签名管理和加密管理通常极为相似。

8.4.4 访问控制管理

访问控制管理包括：

a. 分发安全属性(含口令)；

b. 修改访问控制表或权力表；

c. 在通信实体和提供访问控制服务的其它实体间使用协议。

8.4.5 数据完整性管理

数据完整性管理包括：

a. 与密钥管理的相互作用；

b. 建立密钥参数和加密算法；

c. 在通信实体间使用协议。

注：当使用加密技术实现数据完整性时，数据完整性管理和加密管理极为相似 。

8.4.6 鉴别管理

鉴别管理包括：

a. 向需要鉴别的实体分发描述性信息、口令或密钥(利用密钥管理)；

b. 在通信实体和提供鉴别服务的其它实体间使用协议。

8.4.7 通信业务量填充管理

通信业务量填充管理包括通信业务量填充规则的维护，例如：

a. 预先指定数据速率；

b. 指定随机数据速率；

c. 指定报文特征(如长度)；

d. 可能按日时间或日历改变这些规定。

8.4.8 路由选择控制管理

路由选择控制管理包括确定就特定规范而言是安全、可信赖的链路或子网络。

8.4.9 公证管理

公证管理包括：

a. 分发公证人信息；

b. 在公证人和各通信实体间使用协议；

c. 与公证人的相互作用。

广东省网络空间安全协会受控资料

8.4.10 可用性管理

可用性管理包含在与提供通信网络的管理设施之间进行交互作用的上下文内，用于通知故障中断和通知替代服务信息。

广东省网络空间安全协会受控资料

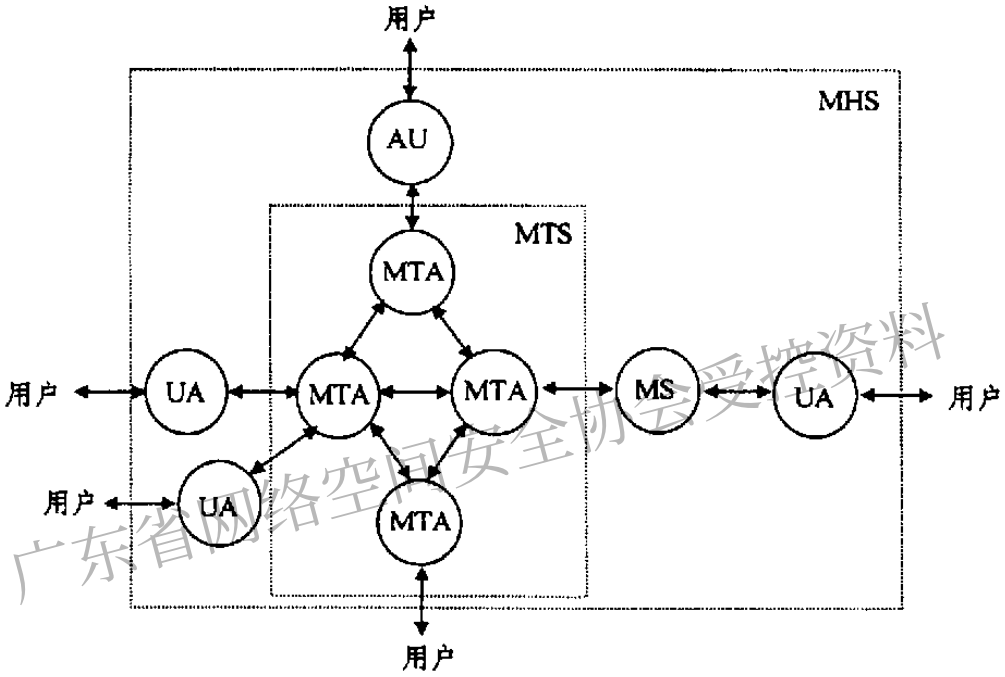
附 录 A
军用报文处理系统的安全服务与安全机制的配置实例
（补充件）

A1 概述

本实例规定了遵循开放系统互连应用层协议 MHS(报文处理系统)的军用报文的安全服务和安全机制的配置,以保证军用报文在传输应用中的完整性和真实性。

A2 MHS 功能模型

图 A1 示出了军用报文处理系统报文传输应遵循的 MHS 功能模型。



注:1)AU: 访问单元;
2)MS: 报文存储;
3)MTA: 报文传送代理;
4)MTS: 报文传送系统;
5)UA: 用户代理。

图 A1 MHS 的功能模型

A2.1 用户及其传输的报文

用户作为 MHS 客体的外围,可以是发送或接收报文的人,也可以是应用进程。报文由信封和内容组成。信封标识报文的发送者和接收者以及内容的特征(如指示它是私人报文通信还是事务公文通信)。信封还包含一些管理信息,以便将报文从发送者转交给一个或多个接收者。内容就是发送者想要传输到接收者那里的正文。

报文有三种类型:

a. 用户报文,含有内容;

广东省网络空间安全协会受控资料

b. 探询报文，不含有任何内容，用于帮助用户确定某一特定用户报文是否可以投递；

c. 投递报告报文，用于向报文发送者通知用户报文或探询报文投递的结果。

A2.2 功能客体

模型中的功能客体是用户代理(UA)、报文存储(MS)、访问单元(AU)和报文传送系统(MTS)。UA是一种应用进程，它与MTS或MS交互工作，替用户提交报文或把报文投递给用户。MS作为UA和MTS之间的中介实体，可为UA或MTS提供报文存储机制，其目的是存储并允许检索已传输过的报文。AU可使MHS的作用增值，即它可将非MHS的通信系统(如用户电报、通信系统、可视图文通信系统等)连到MHS上。MTS可由多个MTA组成，提供分布式和存储转发式报文传输服务。源MTA验证UA提交的报文并设法将其投递给接收者。若接收者是源MTA的用户，则投递是直接的，不涉及其他MTA；否则，源MTA需将报文转发给其他MTA。当报文有多个接收者时，报文的各个拷贝由各转发报文的MTA创建。MTS对报文内容不检查也不修改，但当报文内容中有多个报体，而每个报体的编码信息类型不同(如IA5文本、传真、声音、用户电传)时，MTA可提供编码信息类型的转换，以保证用户使用不同编码信息类型终端时的互通性。

A2.3 MHS安全服务

MHS是按开放系统互连的应用层开发的，它提供的安全服务符合本标准的规定，但作为特定的应用系统，其内容更为具体。设置安全服务是为了对付可能受到的威胁，如表A1所示。MHS提供的安全服务，可以出现在MHS功能模型中有关功能客体的八种接口上，即：UA－UA、UA－MS、MS－MTA、UA－MTA、MTA－MS、MTA－MTA、MTA－UA和MS－UA，如表A2所示。

表A1 MHS安全威胁

威　胁	含　义
冒　充	未授权的某个MTS用户可能冒充另一个MTS用户。废弃MTS的合法用户报文虚假地声称发过一份报文。替代另一合法收信人作出接收认可。某个未授权的MTA，冒充MTS用户所在的MTA，虚假地声称用户报文已经投递。
报文失序	重新排序。改换时间。重复报文的一部分或全部。窃取、记录和事后重放报文。
报文修改	给收信人的报文内容、管理信息被未授权的故意修改或破坏
信息泄漏	偷听报文。非法访问存储在MHS客体中的信息。分析通信业务流量，根据业务流量的变化推断出确定的信息量。
抵　赖	报文源抵赖发送。抵赖提交过报文。抵赖接收了投递的报文。
其　它	修正路由信息，导致报文送入错误路由或未授权的不可靠路由。高密级报文传到低安全等级的用户。安全等级违章。

广东省网络空间安全协会资料

表 A2　MHS 安全服务

安全服务		UA－UA	UA－MS	MS－MTA	UA－MTA	MTA－MS	MTA－MTA	MTA－UA	MS－UA
源点鉴别	用户报文源点鉴别	Y	Y	·	Y	·	·	·	·
	探询报文源点鉴别	·	·	Y	Y	·	·	·	·
	提交报告报文源点鉴别	·	·	·	·	Y	Y	Y	·
	提交证明	·	·	·	·	·	·	Y	·
	投递证明	Y	·	·	·	·	·	·	·
安全访问管理	对等实体鉴别	Y	Y	Y	Y	Y	Y	Y	Y
	安全上下文	·	Y	Y	Y	Y	Y	Y	Y
报文保密性	连接保密性	·	Y	Y	Y	Y	Y	Y	Y
	内容保密性	Y	·	·	·	·	·	·	·
	报文流保密性	Y	·	·	·	·	·	·	·
报文完整性	连接完整性	·	Y	Y	Y	Y	Y	Y	Y
	内容完整性	Y	·	·	·	·	·	·	·
	报文顺序完整性	Y	·	·	·	·	·	·	·
抗抵赖	抗源点抵赖	Y	·	·	Y	·	·	·	·
	抗提交抵赖	·	·	·	·	·	·	Y	·
	抗投递抵赖	Y	·	·	·	·	·	·	·
报文安全标记		Y	Y	Y	Y	Y	Y	Y	Y
安全管理	改变凭证	·	Y	·	Y	Y	Y	Y	·
	登　　录	·	Y	·	Y	·	·	·	·

注："Y"表示提供此服务；"·"表示不提供此服务。

A3　军用报文的完整性、真实性的安全服务与安全机制配置

对军用报文完整性、真实性安全威胁所需要的安全服务与在应用层的机制配置如表 A3 所示。

广东省网络空间安全协会受控资料

表 A3　军用报文完整性、真实性的安全服务与安全机制配置

威　胁	安　全　服　务	安全机制			设　置　的　层						
		加密	鉴别与验证	审计	1	2	3	4	5	6	7
冒　充	用户报文源点鉴别	Y	Y	Y	·	·	·	·	·	·	Y
冒　充	探询报文源点鉴别	Y	Y	Y	·	·	·	·	·	·	Y
冒　充	投递报告报文源点鉴别	Y	Y	Y	·	·	·	·	·	·	Y
冒　充	提交证明	Y	Y	Y	·	·	·	·	·	·	Y
冒　充	投递证明	Y	Y	Y	·	·	·	·	·	·	Y
冒　充	对等实体鉴别	Y	Y	Y	·	·	·	·	·	·	Y
高密级报文传到低安全等级用户	安全上下文	Y	Y	Y	·		·	·	·	·	Y
报文修改	报文连接完整性	Y	Y	Y	·	·	·	·	·	·	Y
报文修改	报文内容完整性	Y	Y	Y	·	·	·	·	·	·	Y
报文失序	报文顺序完整性	Y	Y	Y	·	·	·	·	·	·	Y
抵　赖	抗源点抵赖	Y	Y	Y	·	·	·	·	·	·	Y
抵　赖	抗提交抵赖	Y	Y	Y	·	·	·	·	·	·	Y
抵　赖	抗投递抵赖	Y	Y	Y	·	·	·	·	·	·	Y
安全等级违　章	报文安全标记	Y	Y	Y	·	·	·	·	·	·	Y

注："Y"表示提供此服务；"·"表示不提供此服务。

广东省网络空间安全协会受控资料

附 录 B
有关开放系统互连安全问题的背景材料
（参考件）

B1 背景情况

本附录提供：

a. 有关开放系统互连安全的材料，以帮助理解本标准；

b. 各种安全功能与要求的体系结构含义的背景。

开放系统互连环境中的安全仅仅是数据处理/数据通信安全的一个方面。在开放系统互连环境中所采取的保护措施要有效，就需要有开放系统互连之外的某些措施予以支持。例如，可以对系统之间流通的信息进行加密处理，但若对这些系统本身的访问不设置物理上的安全限制，加密就可能是徒劳的。而开放系统互连只涉及系统的互连。为了使开放系统互连安全措施有效，就需将它们与开放系统互连范围以外的措施配合起来使用。

B2 对安全的要求

B2.1 安全的含义是什么

“安全”是指减少财富与资源的脆弱性。财富是指任何有价值的东西。脆弱性是指可利用的任何弱点，以达到侵害系统或系统内信息的目的。威胁即对安全的潜在侵害。

B2.2 开放系统中要求安全的原因

为加强开放系统互连体系结构中的安全，国际标准化组织（ISO）认为必须制定一系列标准。原因是：

a. 社会对计算机的依赖性日益增长，计算机是通过数据通信来访问或连接的，需对它们加以保护以抵御各种威胁；

b. 有些国家颁布了“数据保护”法规，迫使供应商表明系统的完整性与保密性；

c. 各种组织在现有的和将来的安全系统中使用开放系统互连标准的愿望日益增强。

B2.3 需要保护的内容

下列各项通常需要保护：

a. 信息与数据（包括软件以及与安全措施有关的被动数据，如口令）；

b. 通信和数据处理服务；

c. 设备与设施。

B2.4 威胁

对数据通信系统的威胁包括：

a. 对通信和/或其他资源的破坏；

b. 对信息的讹用或修改；

c. 信息和/或其他资源的失窃、删除或丢失；

d. 信息的泄露；

e. 服务的中断。

威胁可分为偶发威胁和故意威胁两类，也可分为主动威胁和被动威胁。

广东省网络空间安全协会受控资料

B2.4.1 偶发威胁

偶发威胁是指那些非预谋的威胁。例如：系统故障、操作失误和软件差错等。

B2.4.2 故意威胁

故意威胁包括从使用容易获得的监视工具进行随意检测到使用特别的系统知识进行精心的攻击。若故意威胁得逞就可视之为“攻击”。

B2.4.3 被动威胁

被动威胁是指：其得逞不修改系统的任何信息，系统的操作和状态也不发生改变。例如，通过消极的搭线窃听办法侦察通信线路上传送的信息。

B2.4.4 主动威胁

对系统的主动威胁包括修改系统中含有的信息、改变系统的状态或操作。例如，一个未经授权的用户恶意地改动路由选择表。

B2.5 几种特定类型的攻击

下面扼要介绍在数据处理/数据通信环境中特别值得关注的几种攻击。在下列各条中用到“授权”与“未授权”两个术语。“授权”是指授予权力。该定义有两层含义：权力是指进行某种活动的权力(例如访问数据)；这样的权力被授予某个实体、代理人或进程。于是，授权行为就是履行被授予权力(未被撤消)的那些活动。关于授权概念详见 B3.3.1 条。

B2.5.1 冒充

冒充就是一个实体伪装成别的实体。冒充常与某些别的主动攻击形式一起使用，特别是消息的重演与修改。例如，鉴别序列能够被截获，并在一个有效的鉴别序列发生之后被重演。特权很少的实体为了得到额外的特权，可能冒充成具有这些特权的实体。

广东省网络空间安全协会受控资料

B2.5.2 重演

当一消息或其中一部分被重复以便产生未授权效果时便出现重演。例如，含有鉴别信息的一个有效消息可能被另一个实体重演，其目的是鉴别它自己(把它当作其他实体)。

B2.5.3 消息更改

当数据传送的内容被改变而未发觉，并造成未授权后果时便出现消息更改。例如，消息“允许‘甲’读保密文卷‘帐目’”被改为“允许‘乙’读保密文卷‘帐目’”。

B2.5.4 服务拒绝

当一个实体不能执行它的正当功能，或它的动作妨碍了别的实体执行正当功能时便发生服务拒绝。这种攻击可能是泛泛的，比如一个实体抑制所有的消息；也可能是有具体目标的，例如一实体抑制所有送往某一特定目的端的消息，如安全审计服务。这种攻击包括抑制通信业务，如本例中所述，或产生额外的通信业务。它也可能制造出试图破坏网络操作的消息，特别是如果网络具有中继实体，而这些中继实体根据从别的中继实体那里接收到的状态报告来作出路由选择的决定。

B2.5.5 内部攻击

当系统的合法用户以非故意或未授权方式进行动作时便出现内部攻击。大多数计算机犯罪都与损害系统安全的内部攻击有密切的关系。防止内部攻击的保护方法包括：

a. 对工作人员进行仔细审查；

b. 仔细检查硬件、软件、安全策略和系统配制，以便在一定程度上保证它们运行的正确性（称为可信功能）；

c. 审计跟踪以增强对这种攻击的检测能力。

B2.5.6 外部攻击

外部攻击可能使用的办法有：

a. 搭线（主动的与被动的）；

b. 截取发射；

c. 冒充系统的授权用户或冒充系统的组成部分；

d. 绕过鉴别或访问控制机制。

B2.5.7 暗入口

当系统的实体被改变致使攻击者能对命令，或对预定的事件或事件序列产生未授权的效果时，其结果就称为暗入口。例如，口令的验证系统可能被修改，使得除了其正常效力之外也使攻击者的口令生效。

B2.5.8 特洛伊木马

当特洛伊木马侵入系统时，它不但具有自己的授权功能，而且还有未授权功能。一个未授权信道拷贝消息的中继就是一个特洛伊木马。

B2.6 对威胁、风险与抵抗措施的评估

系统安全功能通常会提高系统的成本和使用难度。所以，在设计安全系统之前，应明确具体威胁以便有针对性的提供保护，这叫做威胁评估。虽然一个系统易受攻击的地方很多，但是由于攻击者缺乏机会或者认为不值得冒被检测出来的风险，所以只有其中的几个是可被利用的，大致来说包括以下几种（威胁评估的详细论述不属本附录的范围）：

a. 找出系统的薄弱环节；

b. 分析有可能利用这些薄弱环节的威胁；

c. 评估每种威胁一旦得逞所产生的后果；

d. 估计每种攻击的代价；

e. 估算出可能的应付措施的费用；

f. 选取合理的安全机制（可能要使用价值效益分析）。

非技术性措施，例如交付保险，有可能比技术性安全措施更合算。技术上要做到完全安全是不可能的，正如不可能做到完全的物理保护一样。所以，目标应该是使攻击所花的代价足够高而把风险降低到可接受的程度。

B3 安全策略

本章讨论安全策略，问题包括：制定适当的安全策略的必要性；安全策略的作用；使用中的策略方法；和为了应用于具体情况而作的改进。然后将这些概念应用于通信系统。

B3.1 安全策略必要性和目的

整个安全领域既复杂又广泛。任何一个相当完备的分析都将产生种类繁多的细节，使人望而生畏。一个适当的安全策略应该把注意力集中到最高权力机关认为须得注意的那些方面。实质上，安全策略应当概括地说明在安全领域内哪些在相关系统的一般操作过程中是允

军标信息网络安全协会提供资料

许和不允许的策略。它通常不作具体规定，即只是提出什么是最重要的，而不具体地说明如何达到所希望的这些结果。策略建立起安全技术规范的最高一级。

B3.2 策略规定的含义：精确化过程

由于策略是很一般性的，因而开始时是不可能知道这一策略如何与某一具体应用结合在一起。最好的办法是经常让这一策略经受一个不断精确化的改进过程，在每个阶段加进从应用中来的更多的细节。为了知道这些细节应当是什么，就需要在总策略的指导下对该应用领域进行细致的考查和研究，这种考查应该弄清由于试图将策略的条件强加于应用而出现的问题。这一精确化过程将产生出用直接从应用中抽取来的确切语言重新表述的总策略，这个重新表述的策略使得制定实施方案细节的工作更容易些。

B3.3 安全策略的组成部分

现有安全策略包括两个方面，它们都建立在授权行为这一概念之上。

B3.3.1 授权

上面讨论的威胁都与授权行为或未授权行为的概念有关。在安全策略中包含有对“什么构成授权”的说明。在一般性的安全策略中可能写有“未经适当授权的实体，信息不可以给予、不被访问、不允许引用、任何资源也不得为其所用”，按授权的性质以区分不同的策略。根据所涉及的授权的性质可将策略分为两种：基于规则的安全策略和基于身份的安全策略，前者采用基于少量的一般属性或灵敏度类别的规则，它们通常是强加的。后者则涉及基于特定的、个体化属性的授权准则。某些属性被认为与被应用实体永久相关联；而其金属性可以是某种占有物（例如权力）。它们可传送给另外的实体。人们也可以将授权服务分为行政管理强加的与动态选取的两类。一个安全策略将确定哪些系统安全要素需要强制执行（例如，基于规则的安全策略与基于身份的安全策略，若存在），哪些是根据用户需要选择的。

B3.3.2 基于身份的安全策略

基于身份的安全策略，在一定程度上与“必需认识”的安全观念相当，其目的是对数据或资源的访问进行筛选，基本上有两种执行基于身份策略的基本方法，视有关访问权的信息为访问者所拥有，还是被访问数据的一部分而定。前者的例子为特权标识或权力，给予用户并为代表该用户进行活动的进程所使用，后者的例子为访问控制表（ACL）。在这两种情况中，数据项的大小可以有很大的变化（从完整的文卷到数据元素），这些数据项可以按权力命名，也可以带有它自己的 ACL。

B3.3.3 基于规则的安全策略

在基于规则的安全策略中，授权通常依赖于敏感性。在一个安全系统中，数据和/或资源应该标注安全标记，代表用户进行活动的进程可以得到与其原发者相适应的安全标记。

B3.4 安全策略、通信与标记

标记的概念在数据通信环境中是至关重要的。带有属性的标记发挥多种作用。有在通信期间要移动的数据项；有发起通信的进程与实体；有响应通信的进程与实体；还有在通信时被用到的系统本身的信道和其他资源。所有这些都可以设法用它们的属性来标记。安全策略必须指明属性如何能被使用以提供必要的安全。这了对那些特别标记的属性建立适当的安全含义，可能需要进行协商。当安全标记既附加给访问进程又附加给被访问的数据时，应用基于身

份访问控制所需要的附加信息应是有关的标记。当一个安全策略是基于直接的或通过进程访问数据的用户的身份时，安全标记应该包括有关该用户的身份信息。用于特定标记的那些规则应该表示在安全管理信息库中的一个安全策略中描述，和/或根据要求与端系统协商。标记可以附带属性，这些属性能够指明其敏感性，说明处理与分析上的隐蔽处强制定时与定位、以及指明对该端系统特有的要求。

B3.4.1 进程标记

在鉴别中，完全识别发起与响应一个通信实例的那些进程或实体以及适当的属性是至关重要的，所以，安全管理信息库将保存对任一行政管理强加策略来说极为重要的那些属性的足够信息。

B3.4.2 数据项标记

当通信实例中数据项在移动时，每一个都与它的标记紧紧地拴在一起。（这种约束是重要的，而且在某些基于规则的实例中，要求将此标记做成数据项的一个特殊部分，然后交付应用），保持数据项完整的技术也将保持准确性以及标记的耦合。这些属性能为开放系统互连基本参考模型数据链路层中的路由选择控制功能所使用。

B4 安全机制

一种安全策略可以使用不同的机制来实施，或单独使用，或组合使用，取决于该策略的目的以及使用的机制。通常有以下三种（有重叠的）机制：

a. 预防；

b. 检测；

c. 恢复。

下面讨论适合于数据通信环境的安全机制。

B4.1 密码技术与加密

密码技术是许多安全服务与机制的基础，密码函数可用来作为加密、解密、数据完整性，鉴别交换，口令存储与校验等功能的一部分，借以达到保密、完整性和/或鉴别的目的。用于保密性的加密把敏感数据（即要保护的数据）变换成敏感性较弱的形式。当用于完整性或鉴别时，密码技术被用来计算不可伪造的函数。

加密，首先是把明文转换成密文，解密的结果或是明文，或是在某种掩护下的密文。使用明文作通用的处理在计算上可行的，它的语义内容是可以理解的，除了在一些特定的情形时（例如本原解密或恰切匹配）处理密文在算法上是行不通的，这是因为它的语义内容已被隐藏起来，有时故意让加密是不可逆的（例如截短或数据丢失），这时不希望导出原来的明文，例如口令。

密码函数使用密码变量，并作用于字段、数据单元和/或数据单元流上。两个密码变量为：密钥与初始变量，前者指导具体的变换；后者是为了保持密文外表的随机性在某些密码协议中所需要的。密钥通常必须处于保密状态，而且加密函数与初始变量可能增加延迟带宽消耗，这样把“透明的”和“可选的”密码技术加到现有系统中就变得复杂了。

加密或解密使用的密码变量分为对称的与非对称的两种。用在非对称算法中的密钥在数学上是相关的；一个密钥不能从另一个计算出来。这种算法有时称为公开密钥算法，这是因为

广东省网络空间安全协会受控资料

可使用一个密钥公之于众而另一个保持秘密。

只要在算法上行得通，在没有密钥也可通过对密文加以分析而将其恢复为明文，这种情况的发生大多是因为使用了一个脆弱的或是有缺陷的密码函数。窃听和通信业务流分析可能导致对密码系统的攻击，包括消息/字段的插入、删除与更改、原来有效密文的重演以及冒充。所以密码协议的设计要抗攻击，有时还要抗通信业务流分析。抵御通信业务流分析的一种具体办法即“通信业务流保密性”，其目的是掩蔽数据的出现或不出现及其特征。如果密文被中继，那么中继站和网关上的地址必须是明文。如果数据只在每个链路上是加密的，而在中继或网关内被解密(因而易受攻击)，这种结构称为“逐链加密”。如果只有地址(及类似的控制数据)在中继或网关内是明文，这种结构称为“端对端加密”。从安全观点来看，端对端加密较好，但结构复杂，特别是采用带内电子密钥分发(一种密钥管理功能)时更是如此。可将逐链加密和端对端加密结合起来使用，以达到多种安全目的。数据完整性往往可通过计算密码校验值来实现，这种校验值可以分一步或多步导出，而且是密码变量与数据的函数，这些校验值与要受到保护的那些数据相关联。这种密码校验值有时称为操纵检测码。

密码技术能够提供，或有助于提供保护以防止：

a. 消息流量的观察和/或修改；

b. 通信业务流分析；

c. 抵赖；

d. 伪造；

e. 未授权连接；

f. 修改消息。

B4.2 密钥管理方面

密码算法的使用就意味着要进行密钥管理。密钥管理包括密码密钥的产生、分发与控制。密钥管理方法是根据参与者对使用该方法的环境所作的评价选取的。对这一环境的考虑包括要进行防范的威胁(组织内部的和外部的)，所使用的技术，所提供的密码服务的体系结构与位置，以及密码服务提供者的物理结构与定位等。

关于密钥管理需要考虑的事项包括：

a. 对于每一个显式或隐含定义的密钥，应根据时间、使用情况或其他准则使用其“存活期”。

b. 按密钥的功能适当地区分密钥以便可以按功能使用密钥，例如：打算用作保密性服务的密钥就不应该用于完整性服务，反之亦然；

c. 非开放系统互连的考虑，例如密钥的物理分发和密钥存档。

有关对称密钥算法的密钥管理要考虑的事项包括：

a. 使用密钥管理协议中的保密性服务以运送密钥；

b. 使用密钥体系。应该允许有各种不同情况，如：

1) 单层密钥体系，只使用加密数据密钥，从一个集合中按密钥的身份或索引隐含地或显示地进行选取；

2) 多层的密钥体系；

广东省网络空间安全协会受控资料

3) 加密密钥的密钥决不能用来保护数据，而加密数据的密钥亦不能用来保护加密密钥的密钥。

c. 将责任作分解使得没有一个人具有重要密钥的完整拷贝。

有关非对称密钥算法的密钥管理要考虑的事项包括：

a. 用密钥管理协议中的保密性服务运送秘密密钥；

b. 用密钥管理协议中的完整性服务或带数据源点证明的抗抵赖服务运送公开密钥。这些服务可以通过使用对称或非对称密码算法提供。

B4.3 数字签名机制

数字签名机制是用来提供诸如抗抵赖与鉴别等安全服务的特殊技术。数字签名机制要求使用非对称密码算法。数字签名机制的主要特征为：不使用秘密密钥就不能建立签名数据单元，这意味着：

a. 除了掌握秘密密钥的人以外，任何人都不能建立签名数据单元；

b. 接收者不能建立签名数据单元。

所以，只需使用公开可用的信息就能认定数据单元签名者只能是掌握秘密密钥的人。因而一旦当事人之间后来发生纠纷，就可能向一个可靠的第三方证明数据单元签名者的身份，这个第三方是被请来对签名的数据单元的鉴别作出判决的。这种类型的数字签名称为直接签名方案(见图 B1)。在别的情况下，可能需要再加一条特性(c)：

c. 发送者不能否认曾经发送过签名的数据单元。

在这一情形，一个可信赖的第三方(仲裁人)向接收者证明该信息的来源与完整性。这种类型的数字签名有时称为仲裁签名方案(见图 B2)。

广东省网络空间安全协会受控资料

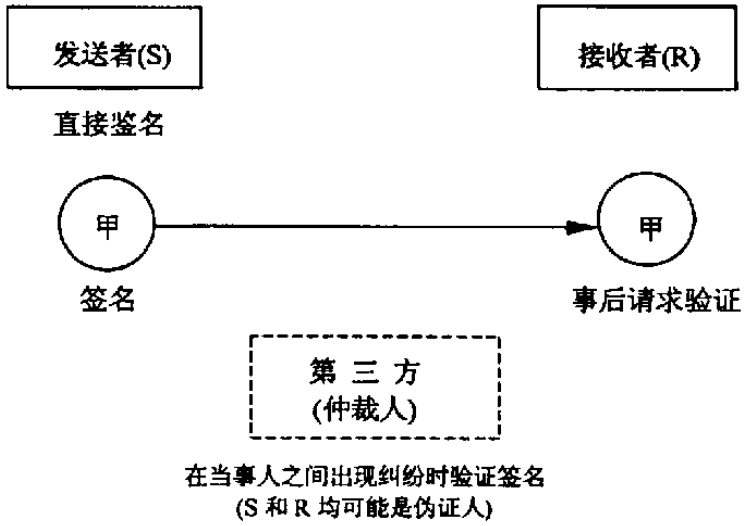
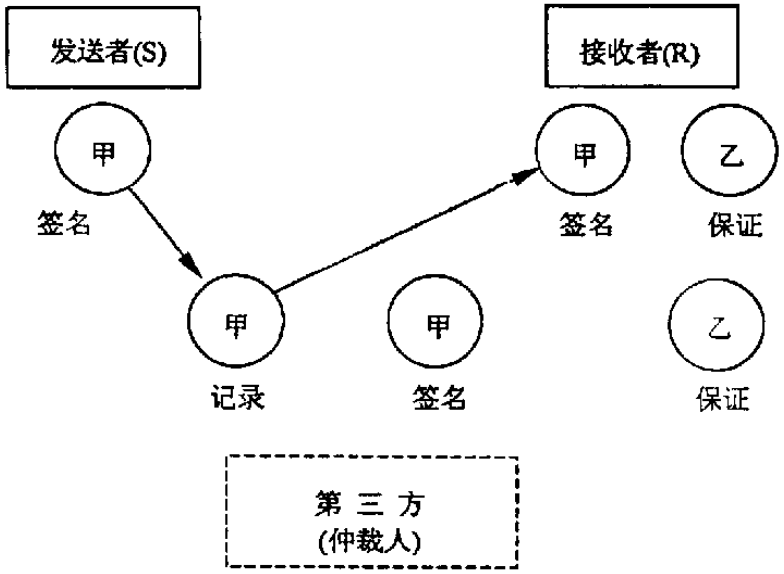


图 B1 直接签名方案



第三方鉴别信息源，并向接收者发出保证(即肯定的结果)。证明信息源与数据完整性的信息由第三方记录在案。因此，发送者 S 事后无法否认曾发过那个已鉴名的数据单元。

图 B2　仲裁签名方案

注：发送者可能要求接收者事后不能否认接受过该签名数据。这可用带交付证明的抗抵赖服务来完成。方法是将数字签名机制、数据完整性机制与公证机制作适当的结合。

B4.4　访问控制机制

访问控制机制是用来实施对资源访问加以限制策略的一种机制，这种策略只允许被授权用户访问资源。采用的技术包括使用访问控制表或矩阵〔通常包括被控制项与被授权用户(例如人群或进程)的身份〕、口令、权力、标记或标志。拥有这些东西的用户可用它指出自己的访问权。在使用权力的地方，权力应该是不可伪造的，而且用可靠的方式传递。

B4.5　数据完整性机制

数据完整性机制有两种类型：一种用来保护单个数据单元的完整性，另一种既保护单个数据单元的完整性，也保护一个连接上整个数据单元流序列的完整性。

B4.5.1　消息流的修改检测

通常用于对通信链路和网络所引入的对比特错、码组错与顺序错进行检测的讹误检测技术，也能用来检测消息流的修改。但如果协议的头标与尾标不受完整性机制的保护，那么一个知情的入侵者就可能成功地躲开这些检测。因而，检测消息流修改的有效方法只能通过使用讹误检测技术并配合以顺序信息实现，这不能防止对消息流的修改但能提供对攻击的检测通知。

B4.6　鉴别交换机制

B4.6.1　机制的选取

适合于各种不同场合的鉴别交换机制有多种选择与组合：

a. 当对等实体以及通信手段都可信任时，一个对等实体的身份可以通过口令来证实，该口令能防止出错，但不能防止恶意行为(特别是重演)。相互鉴别可在每个方向上使用不同的

广东省计算机信息系统安全协会受控资料

口令来完成。

b. 当每个实体信任其对等实体但不信任其通信手段时，抗主动攻击保护可由口令与加密组合提供，也可由密码手段提供。为了防止重演攻击需要双方握手（利用保护参数）或加上时标（利用可信时钟）。具有重演保护的相互鉴别，可通过三方握手予以实现。

c. 当实体不信任（或感到它们将来可能不信任）它们的对等实体或通信手段时，可以使用抗抵赖服务。使用数字签名机制和/或公证机制就能实现抗抵赖服务。这些机制可与 b 中所述的机制一起使用。

B4.7 通信业务量填充机制

制造伪通信业务和将协议数据单元填充到一个定长，能够为防止通信业务流分析提供有限的保护。为了使保护成功，伪通信业务级别必须接近实际通信业务量的最高预期等级。此外，必须对协议数据单元的内容进行加密或伪装，以便无法将伪通信业务与真正的通信业务区分开来。

B4.8 路由选择控制机制

传送数据的路由警告说明（包括一整条路径的说明）可用来保证数据只在物理上安全的路由上传输，或保证敏感数据只在具有适当保护级别的路由上传输。

B4.9 公证机制

公证机制建立在可信任的第三方（公证人）的概念之上，以确保在两个实体间交换的信息的某些性质不致变化，例如来源、完整性、发送时间或接收时间。

B4.10 物理安全与人员可靠

为了获得完善的保护，必须有物理安全措施。物理安全的代价高，往往要通过其他（廉价）技术降低对物理安全的要求。尽管所有系统将最终依靠某种形式的物理安全和对操作系统的人员的信赖，但对物理安全和人员可靠方面的考虑不属于开放系统互连的范围。应确定操作规程以保证操作正确、人员职责明确。

B4.11 可信任的硬件/软件

为了取得对一实体正常运转的信任，可采用形式证明法、验证与证实、检测和登录已知的试图进行的攻击以及由可信人员在安全环境中构造实体等方法。此外，还需要采取预防措施，以防止实体在其运行期内（例如在维护或升级过程中）被无意地或故意地修改，从而危害实体的安全。为了维护系统安全，系统中的有些实体必须是可信、能够正常工作的，但如何建立可信实体不属于开放系统互连的范围。

广东省测绘地理信息安全协会受控资料

附 录 C
安全服务与安全机制的配置理由
（参考件）

C1 概述

第7章已指明了各层所提供的相关安全服务，本附录将对此加以说明。6.1.1条所述的安全分层原则是选择上述服务的准则。

若某一特定安全服务由不同层提供时，对总的通信安全的影响不同，则这些层都应提供这种安全服务（例如，第1层和第4层均提供连接保密性）。但是，考虑到现有开放系统互连数据通信的机能（如多链路规程、多路复用功能、强化无连接服务使之成为面向连接服务的不同方法），并让这些传输机制得以运行，有可能需要在其他层上提供这种特定服务，尽管它对安全的影响没有什么不同。

C2 对等实体鉴别

第1层与第2层：无。在这些层上对等实体鉴别是无用的。

第3层：有。在一些单独的子网上，为了路由选择，和/或在互连网络上。

第4层：有。第4层中端系统到端系统的鉴别，能够在一个连接的开始前和持续过程中用来作为两个或多个会话实体的相互鉴别。

第5层：无。在第4层和/或更高层提供这一服务更好。

第6层：无。但加密机制能在应用层支持这种服务。

第7层：有。对等实体鉴别应该由应用层提供。

C3 数据源点鉴别

第1层与第2层：无。在这些层上数据源点鉴别是无用的。

第3层与第4层：在第3层和/或第4层的中继与路由选择功能中可端对端地提供数据源点鉴别，如下所述：

a. 在建立连接时所提供的对等实体鉴别及在连接存活期间所提供的基于加密的连续鉴别，事实上也提供了数据源点鉴别服务；

b. 即使不提供a项中的服务，通过对已经位于这些层中的数据完整性机制增加非常小的一点额外开销，也能提供基于加密的数据源点鉴别。

第5层：无。在第4层或第7层提供这一服务更好。

第6层：无。但加密机制能在应用层支持这一服务。

第7层：有。可能要与表示层中的机制相配合。

C4 访问机制

第1层与第2层：对一个遵守全部开放系统互连协议的系统，在第1层或第2层不能提供访问控制机制，这是因为没有可用于这样一种机制的端设备。

第3层：根据特定子网的要求，访问控制机制强加于子网访问作用之上。当由中继与路由选择作用执行时，在网络层中的访问机制既能用于控制中继实体对子网的访问，又能用于控制对端系统的访问。显然，如果这种访问粒度非常粗糙，那它仅在网络层的实体之间有所不同。

当建立一条网络连接时，子网的管理部门往往要收费。通常可通过访问控制、选用反向记

中关村网络空间安全协会受控资料

费、或选用其他网络或子网特定参数来使费用降低到最低限度。

第4层：有：访问控制机制可用于端至端传送连接上。

条5层：无。并不比第4层或第7层提供这一服务更好。

第6层：无。在第6层上这是不适宜的。

第7层：有。应用协议和应用进程能提供面向应用的访问控制业务。

C5 在(N)连接上所有(N)用户数据的保密性

第1层：有。由于成对插入的电气转换设备是透明的，它能提供物理连接上的完全保密性。所以应该提供。

第2层：有。但不给第1层或第3层的保密性提供更多的安全益处。

第3层：有。用于某些单个子网上的子网访问，以及互连网络上的中继与路由选择。

第4层：有。因为单个运输连接既能给出端对端运输机制又能提供会话连接的隔离。

第5层：无。因为在第3、4、7层的保密性上它不提供额外益处，所以不宜由这一层提供。

第6层：有。因为加密机制提供纯语法变换。

第7层：有。与下层的机制相配合。

C6 在单个的无连接(N)－SDU中全(N)用户数据的保密性

除第1层外，理由的说明与全用户数据的保密性相同。第1层没有无连接服务。

C7 SDU的(N)用户数据和选择字段保密性

这种保密性服务由表示层中的加密机制来提供，并且根据数据的语义由应用层中的机制调用。

C8 通信业务流保密性

全通信业务流保密性只能在第1层获得。在物理传输通路中插入一对加密设备即可。假定传输通路是双向同时同步的，这样插入加密设备就会在不可识别的物理媒体上提供全部传输(甚至传输的出现)。

在物理层之上不可能实现全通信业务流安全。在某一层上使用完整的SDU保密性服务，并在另一个高层上注入伪通信业务能部分地产生这种保密性的某些效果。这种机制代价高，要耗用大量的载波与交换能力。

如果在第3层提供通信业务流保密性，那么将使用通信业务量填充和/或路由选择控制。路由选择控制通过采用使消息绕过不安全的链路或子网，可提供有限通信业务流保密性。然而将通信业务量填充结合在第3层会使网络得到更好的利用，例如可避免不必要的填充和网络拥塞。

在应用层上通过制造伪通信业务，并与防止识别伪通信业务量的保密性相结合起来，可提供有限的通信业务流保密性。

C9 在(N)连接上(带差错恢复)全(N)用户数据的完整性

第1层与第2层：第1层与第2层不能提供这种服务。第1层没有检测或恢复机制，而第2层的机制是基于点对点的，而不是端对端的，因此不适于提供这种服务。

第3层：无。因为差错恢复不是普遍可用的。

第4层：有。因为这提供了真正的端对端运输连接。

广东省网络空间安全协会受控资料

第5层：无。因为差错恢复不是第5层的功能。

第6层：无。但加密机制能在应用层中支持这种服务。

第7层：有。与表示层中的机制相配合。

C10　在(N)连接上(无差错恢复)全(N)用户数据的完整性

第1层与第2层：第1层与第2层不能提供这种服务。第1层没有检测或恢复机制，第2层只能运行在点对点基础上而不是端对端的，所以不适宜提供这种服务。

第3层：有。起到单个子网的子网访问，以及链上的路由选择与中继作用。

第4层：有。对于在检测到主动攻击之后允许停止通信的情况。

第5层：无。因为在第3、4层或第7层的数据完整性，它不提供额外的好处。

第6层：无。加密机制能支持应用层中的这种服务。

第7层：有。与表示层中的机制相配合。

C11　在(N)连接上(无恢复)传送的(N)－SDU的(N)用户数据中选择字段完整性

通过将表示层中的加密机制与应用层中的调用及检测机制相配合，可提供选择字段完整性。

C12　单个无连接(N)－SDU中全(N)用户数据的完整性

为了减少功能重复，无连接传送的完整性应该只在提供无恢复完整性的层上提供，即网络层、运输层和应用层，但必须认识到这样的完整性机制可能只有非常有限的效用。

C13　单个无连接(N)－SDU中选择字段的完整性

表示层中的加密机制与应用层中调用及校验机制结合使用，可提供选择字段完整性。

C14　抗抵赖

数据源点与交付抗抵赖服务能够由一个涉及在第7层上作中继的公证机制提供。

使用对付抗抵赖的数字签名机制要求在第6层与第7层之间进行密切合作。

广东省网络空间安全协会受控资料

附 录 D
加密位置的选取
（参考件）

D1 大多数应用将不要求在多个层上加密，加密层的选取主要取决于下列主要因素：

1）若需要全通信业务流保密性，则选取物理层加密或传输安全手段（例如，适当的扩频技术），适当的物理安全、可信路由选择以及中继上的类似功能可满足所有的保密性要求。

2）若要求高粒度保护（即对每个应用联系可能提供不同的密钥）和抗抵赖或选择字段保护，则选取表示层加密。由于加密算法耗费大量的处理能力，所以选择字段保护可能是重要的。在表示层中的加密能提供无恢复的完整性、抗抵赖以及所有的保密性。

3）若想获得所有端系统到端系统通信的简单块保护和/或希望有一个外部的加密设备（例如为了给算法和密钥以物理保护，或防止错误软件），则选取网络层加密，以提供保密性与无恢复的完整性。

注：虽然网络层不提供恢复，但运输层的正常恢复机制能够恢复网络层检测到的攻击。

4）若既要求可恢复的完整性又要求具有高粒度保护，则应选取运输层加密。运输层加密能提供保密性、可恢复的完整性或无恢复的完整性。

5）在实施过程中，不推荐在数据链路层加密。

D2 当关系到这些主要问题中的两项或多项时，加密可能需要在多个层上提供。

广东省网络空间安全协会受控资料

附加说明：

本标准由总参通信部提出。

本标准由总参第六十一研究所归口。

本标准由总参第六十一研究所起草。

本标准主要起草人：李月芳、陈爱民、陈　影、蒋晓原、樊海宁、白小燕、尹　莉。

计划项目代号：6TX11。