第3章 信息系统的安全评价标准

随着信息技术的发展，信息技术的安全问题变得越来越严重。面对一个信息系统（包括各种软、硬件以及系统集成），用户们的首要担忧就是，这个系统安全吗？所以，计算机系统的提供者需要对他们的产品的安全特性进行说明，而用户则需要验证这些安全特性的可靠性。

然而，普通的用户和系统购买者都不是安全专家，他们难以对产品的安全性进行准确和充分的验证，难以判断系统提供者所提供的安全证明的有效性，或者以任何方式来确定这些系统确实是实现了应该实现的安全策略。

因而，独立的第三方计算机安全评价是非常必要的。因为独立的计算机安全专家能够对系统的安全需求、设计、实现和保证证据等进行审查。对于非安全专家的用户来说，独立安全专家的评价是最合适的。国际上有多种为计算机安全系统构筑独立审查措施的安全评价体系，这些评价标准能够完善而准确地表达信息系统的安全性以及评价信息系统安全性的方法和准则，是信息安全技术的基础，其内容和发展深刻地反映了对信息安全问题的认识程度。了解其现状和发展对信息安全技术的研究十分重要，也是研究、开发和评测各种信息安全技术的基石。

3.1 可信计算机系统评价标准

在计算机应用的早期，由于计算机的应用领域越来越广泛，尤其是大型机被应用到政府、军事、金融等重要部门，计算机系统的可靠性、安全性逐渐得到了人们的重视。如何评价计算机系统的安全成为各国政府和计算机用户所关心的问题。1970 年美国国防部在国家安全局建立了计算机安全评估中心，开始了计算机安全评估的理论与技术的研究，研究的核心问题是计算机操作系统的安全问题。1985 年 12 月美国国防部公布了评价安全计算机系统的六项标准。这套标准的文献名称即为“可信计算机系统评价标准”（Trusted Computer System Evaluation Criteria，TCSEC），又称为橘皮书。“可信”，即可信赖，安全可靠。该标准旨在提供一种标准，使用户可以对其计算机系统内敏感信息安全操作的可信程度作出评估，同时给计算机行业的制造商提供一种可循的指导规则，使其产品能够更好地满足敏感应用的安全需求。

TCSEC 标准是计算机系统安全评估的第一个正式标准，具有划时代的意义。TCSEC 最初只是军用标准，后来延至民用领域。

3.1.1　TCSEC的主要概念

1. 考核标准

为了阐述对可信计算机的考核标准，TCSEC首先提出了主体与客体的概念。

主体(subject)，即计算机系统的主动访问者，如用户(包括入侵者)，用户运行的程序(包括入侵者的恶意程序)，用户的复制、删除、修改等操作都是主体。被访问或被使用的对象称为客体(object)。对资源的访问控制抽象为主体集合对客体集合的监视与控制。在主体与客体的概念体系下，TCSEC提出了评价安全计算机系统的六项标准。

1) 安全策略(security policy)

必须有一项明确的由计算机系统实施的安全策略。系统中必须有可供系统使用的访问规则的集合，以便决定是否允许某主体对特定客体的访问。这些访问规则包括阻止未授权用户对敏感信息的访问。支持自主访问控制，保证只有指定的用户或用户组才能获得对数据的访问权。必须根据安全策略，在可信计算机系统中实现这些访问规则。

2) 标识(identification)

必须能够对系统中的每个主体进行标识，使它们都可以唯一地和可靠地被辨识。为了能够让系统检验每个主体/客体的访问请求，这种标识是必需的。系统必须对每个主体识别后，才允许它对客体进行访问。在系统中每次对客体的访问，都需要识别主体的身份、安全级别和对应的有权访问的客体，对主体的识别与授权信息必须由计算机系统秘密进行，并与完成某些安全有关动作的每个活动元素结合起来。

3) 标记(marking)

对每个客体都要作一个敏感性标记(sensitivity labels)，用于规定该客体的安全等级，并且保证每次对客体访问时都能得到该客体的标记，以便在访问之前可以进行核查。对每个客体进行标记也是为了支持强制访问控制的安全策略。客体的标记既要包含敏感级别，也包括允许哪些主体可以对本客体进行访问的方式。

4) 可记账性(accountability)或责任

系统必须能够记录所有影响系统安全的各种活动。这些活动包括有新用户登录到系统中，发生了修改主体或客体的安全级别的事件，发生了拒绝访问的事件，发生了多次注册失败的事件。对与系统信息安全有关的事件应该有选择地记录与保存，即审计，以便对影响系统安全的活动进行追踪，确定责任者。系统对审计信息必须妥善保护，防止对审计信息的恶意篡改或未经授权的毁坏。

5) 保障机制(assurance)

为了实现上述各种安全能力与机制，在系统中必须提供相应的硬件与软件的保障机制与设施，并且能够对这些机制进行有效的评价。这些机制可以嵌入在操作系统内，并以秘密的方式执行指定的任务。还应该在文档中写明，这些机制是否能够独立考察、评估和检验其结果是否充分。

6) 连续性保护(continuous protection)

系统的上述安全机制必须受到连续性的保护，防止未经许可的中途修改或损坏。如果

实现了上述策略的硬件和软件本身是客体，那么这些安全机制的可靠性就受到威胁，进而威胁到计算机系统的可信性。

2. 主要概念

在 TCSEC 中提出了以下主要概念，以描述计算机系统的安全问题。

1）安全性概念

包括安全策略、策略模型、安全服务和安全机制等内容，其中安全策略是为了软件系统的安全而制定的有关管理、保护和发布敏感信息的规定与实施细则；策略模型是指实施安全策略的模型；安全服务是指根据安全策略和安全模型提供的安全方面的服务；安全机制是实现安全服务的方法。

2）可信计算基概念（Trusted Computing Base，TCB）

TCB 是软件、硬件与固件的有机集合，它根据访问控制策略处理主体集合对客体集合的访问，TCB 中包含了所有与系统安全有关的功能。

3）自主访问控制（Discretionary Access Control，DAC）

DAC 是指资源的所有者（即主体）可以自主地确定别人对其资源的访问权。具有某类权限的主体能够将其对某资源（客体）的访问权直接或间接地按照需要动态地转让给其他主体或回收转让给其他主体的访问权限。

4）强制访问控制（Mandatory Access Control，MAC）

MAC 是比自主访问更为严格的一种访问控制方式。在这种访问方式中，客体的访问权限不能由客体的拥有者自己确定，而是由系统管理者强制规定的。系统管理者为主体与客体规定安全属性（安全级别、权限等），系统安全机制严格按照主体与客体的安全属性控制主体对客体的访问，对于系统管理员确定的安全属性，任何主体都不能修改与转让。

5）隐蔽信道

隐蔽信道是指一个进程利用违反系统安全的方式传输信息。有两类隐蔽信道：存储信道与时钟信道。存储信道是一个进程通过存储介质向另一个进程直接或间接传递信息的信道；时钟信道是指一个进程通过执行与系统时钟有关的操作把不该泄露的信息传递给另一个进程的通信信道。例如，一个文件的读写属性位可以成为隐蔽存储信道。

此外，还有认证、加密、授权与保护等概念。

3. 系统模型

评估准则中采用的可信计算机系统的安全模型采用了 Roger Sehell 提出的访问监控器概念。访问监控器映射计算机系统的可信计算基 TCB，即安全核，它的作用是负责实施系统的安全策略，在主体和客体之间对所有的访问操作实施监控，访问监控器的作用参见图 3-1。图中的主体表示系统中访问操作的发起者，可以是用户，或者代表用户意图的进程等；客体是访问操作的对象，包括文件、目录、内存区或进程等；监视器数据基主要存放用户权限和对

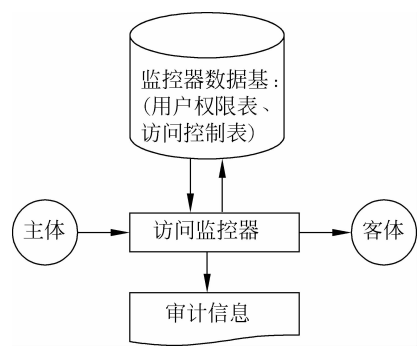

图 3-1　基于访问监控器的系统安全模型

客体的访问关系等信息；访问监控器是实现系统安全策略的机制，是系统的可信计算基。它对于主体提出的每一次访问请求，根据访问监控数据基中定义的访问关系与访问权决定是否同意这次访问的执行，并进行相应的审计记录。

访问监控器支持的安全策略是由 BLP 模型所抽象形式化处理的 DoD 的安全策略。该模型是用数学和集合论的工具精确地定义保密状态、基本的访问方式和为了授予主体对客体进行特殊访问所需要的规则，再用基本的安全理论去证明规则能够保证安全操作的。基本安全理论认为，对于处于保密状态的系统，任何规则子集的使用将导致系统进入一个新的状态，只要规则子集本身是安全的，这个新状态也将是保密的。

BLP 模型在主体的签证级与系统客体的保密级之间定义了一种关系，称为控制系。根据这种定义，基本的访问模型在主体与客体之间定义了只读、只写和读写等访问操作。模型把控制授予某主体可以读某一客体的权利称为简单安全条件，而把控制授予某主体可以写某一客体的权利称为 *-特权。根据主体签证级与客体保密级之间的控制关系，简单安全条件和 *-特权两者都包含强制安全措施。在状态转换时，为了授予某主体以特殊的访问方式，也需要定义自主安全访问方式。在主体代表一用户进程进行处理时，模型需要对可信主体与非可信主体加以区别。

3.1.2　计算机系统的安全等级

TCSEC 将可信计算机系统的评价规则划分为四类，即安全策略、可记账性、安全保证措施和文档。

安全策略包括自主存取控制、客体重用、标记、标记完整性、标记信息的扩散、主体敏感度标记、设备标记、强制存取控制等规则；

可记账性包括标识与认证、可信路径、审计等规则；

安全保障措施包括系统体系结构、系统完整性、隐蔽信道分析、可信设施管理、可信恢复、生命周期保证、安全测试、设计规范和验证、配置管理、可信分配等规则；

文档包括安全特性用户指南、可信设施手册、测试文档、设计文档等规则。

根据计算机系统对上述各项指标的支持情况及安全性相近的特点，TCSEC 将系统划分为四类(division)七个等级，依次是 D；C(C1,C2)；B(B1,B2,B3)；A(A1)。其系统可靠或可信程度逐渐增高，如表 3-1 所示。

表 3-1　TCSEC 安全级别划分

安 全 级 别	定　　义
A1	验证设计(verified design)
B3	安全域(security domains)
B2	结构化保护(structural protection)
B1	标记安全保护(labeled security protection)
C2	受控的存取保护(controlled access protection)
C1	自主安全保护(discretionary security protection)
D	最小保护(minimal protection)

在 TCSEC 中建立的安全级别之间具有一种偏序向下兼容的关系，即较高安全性级别提供的安全保护要包含较低级别的所有保护要求，同时提供更多或更完善的保护能力。

1. D 安全级

D 级是最低级别。保留 D 级的目的是将一切不符合更高标准的系统，统统归于 D 组。如 DoS 就是操作系统中安全标准为 D 的典型例子。它具有操作系统的基本功能，如文件系统、进程调度等，但在安全性方面几乎没有什么专门的机制来保障。

2. C1 安全级

C1 级系统只提供了非常初级的自主安全保护。能够实现对用户和数据的分离，进行自主存取控制(DAC)，保护或限制用户权限的传播。现有的商业系统往往稍作改进即可满足要求。

C1 级系统称为自主安全保护系统。此类系统是针对多个协作用户在同一敏感级别上处理数据的工作环境。其最主要的特点是把用户与数据隔离，提供自主访问控制功能，使用户可以对自己的资源自主地确定何时使用或不使用控制，以及允许哪些主体或组进行访问。通过用户拥有者的自主定义和控制，可以防止自己的数据被别的用户有意或无意地读取、篡改、干涉或破坏。该安全级要求在进行任何活动之前，通过 TCB 去确认用户身份(如密码)，并保护确认数据，以免未经授权对确认数据的访问和修改。这类系统在硬件上必须提供某种程度的保护机制，使之不易受到损害；用户必须在系统注册建立账户并利用通行证让系统能够识别他们。C1 级要求较严格的测试，以检测该类系统是否实现了设计文档上说明的安全要求。另外还要进行攻击性测试，以保证不存在明显的漏洞让非法用户攻破或绕过系统的安全机制进入系统。另外，C1 级系统要求完善的文档资料。

3. C2 安全级

C2 安全级称为可控安全保护级，是安全产品的最低档次，提供受控的存取保护，即将 C1 级的 DAC 进一步细化，保护粒度要达到单个用户和单个客体一级，以个人身份注册，负责并实施审计和资源隔离。它通过注册过程、与安全相关事件的审计和资源隔离，使得用户的操作具有可追踪性。C2 级增加了审计功能，审计粒度必须能够跟踪每个主体对每个客体的每一次访问，审计功能是 C2 较 C1 新增加的安全要求。在安全策略方面，除了具备 C1 级所有功能外，还提供授权服务、对访问权限扩散的控制。C2 级还提供客体再用功能，即要求在一个过程运行结束后，要消除该过程残留在内存、外存和寄存器中的信息，在另一个用户过程运行之前必须清除或覆盖这些客体的残留信息。C2 系统的 TCB 必须保存在特定区域中，以防止外部人员的篡改。

很多商业产品已得到该级别的认证。达到 C2 级的产品在其名称中往往不突出“安全”(Security)这一特色，如操作系统中 Microsoft 的 Windows NT 3.5，数字设备公司的 Open VMS VAX 6.0 和 6.1。数据库产品有 Oracle 公司的 Oracle 7，Sybase 公司的 SQL Server 11.0.6 等。

4. B1 安全级

B 类安全包含三个级别(B1、B2、B3 级)，都采用强制保护控制机制。B1 级又称为带标记的访问控制保护级，其在 C2 级的基础上增加了或加强了标记、强制访问控制、审计、可记

账性和保障等功能。

在 B1 级中标记起着重要的作用，是强制访问控制实施的依据。每个主体和存储客体有关的标记都要由 TCB 维护。B1 级时标记的内容与适用有以下要求：

(1) 主体与客体的敏感标记的完整性：当 TCB 输出敏感标记时，应准确对应内部标记，并输出相应的关联信息。

(2) 标记信息的输出：人工制定每个 I/O 信道与 I/O 设备是单(安全)级的还是多(安全)级的，TCB 应能知道这种输出，并能对这种指定活动进行审计。

(3) 多级设备输出：当 TCB 把一个客体输出到多级 I/O 设备时，敏感标记也应同时输出，并与输出信息一起留存在同一物理介质上。当 TCB 使用多级 I/O 信道通信时，协议应能支持多敏感标记信息的传输。

(4) 单级设备的输出：虽然不要求对单级 I/O 设备和单级信道所处理的信息保留敏感标志，但要求 TCB 提供一种安全机制，允许用户利用单级设备与单级 I/O 信道安全地传输单级信息。

(5) 对人可读输出的标记输出：系统管理员应该能够指定与输出敏感标记相关联的可打印标记名，这些敏感标记可以是秘密、机密和绝密的。TCB 应能标识这些敏感标记输出的开始与结束。

B1 级能够较好地满足大型企业或一般政府部门对于数据的安全需求，这一级别的产品才被认为是真正意义上的安全产品。满足此级别的产品前一般多冠以“安全”(Security)或“可信的”(Trusted)字样，作为区别于普通产品的安全产品出售。例如，操作系统方面，典型的有数字设备公司的 SEVMS VAX Version 6.0，惠普公司的 HP-UX BLS release 9.0.9+。数据库方面则有 Oracle 公司的 Trusted Oracle 7，Sybase 公司的 Secure SQL Server version 11.0.6，Informix 公司的 Incorporated INFORMIX-OnLine/Secure 5.0 等。

5. B2 安全级

B2 安全级称为结构化保护级。该级系统的设计中把系统内部结构化地划分成明确而大体上独立的模块，并采用最小特权原则进行管理。B2 级不仅要求对所有对象加标记，而且要求给设备(磁盘或终端)分配一个或多个安全级别(实现设备标记)。必须对所有的主体与客体(包括设备)实施强制性访问控制保护，必须要有专职人员负责实施访问控制策略，其他用户无权管理。通过建立形式化的安全策略模型并对系统内的所有主体和客体实施自主访问控制和强制访问控制。

B2 级较 B1 级有一项更强的设计要求，B2 级系统的设计与实现必须经得起更彻底的测试和审查，必须给出可验证的顶级设计(Top-Level Design)，并且通过测试确保该系统实现了这一设计。还需要对隐蔽信道进行分析，确保系统不存在各种安全漏洞。实现中必须为安全系统自身的执行维护一个保护域，必须确保该域的安全性不受外界的破坏，进而保护整个系统的目标代码和数据的完整性不受外界破坏。

目前，经过认证的 B2 级以上的安全系统非常稀少。例如，符合 B2 标准的操作系统只有 Trusted Information Systems 公司的 Trusted XENIX 一种产品，符合 B2 标准的网络产品只有 Cryptek Secure Communications 公司的 LLC VSLAN 一种产品，而数据库方面则没有符合 B2 标准的产品。

6. B3 安全级

B3 安全级又称为安全域保护级。该级的 TCB 必须满足访问监控器的要求，审计跟踪能力更强，并提供系统恢复过程。B3 安全级要求系统有主体/客体的区域，有能力实现对每个目标的访问控制，使每次访问都受到检查。用户程序或操作被限定在某个安全域内，安全域间的访问受到严格控制。这类系统通常采用硬件设施来加强安全域的安全，例如，内存管理硬件用于保护安全域免受无权主体的访问或防止其他域的主体的修改。该级别要求用户的终端必须通过可信的信道连接在系统上。

为了能够确实进行广泛而可信的测试，B3 级系统的安全功能应该是短小精悍的。为了便于理解与实现，系统的高级设计(High Level Design)必须是简明而完善的，必须组合使用有效的分层、抽象和信息隐蔽等原则。所实现的安全功能必须是高度防突破的，系统的审计功能能够判断出何时能避免一种破坏安全的活动。为了使系统具备恢复能力，B3 系统增加了一个安全策略。

(1) 安全策略：采用访问控制列表进行控制，允许用户指定和控制对客体的共享，也可以指定命名用户对客体的访问方式。

(2) 可记账性：系统能够监视安全审计事件的发生与积累，当超出某个安全阈值时，能够立刻报警，通知安全管理人员进行处理。

(3) 保障措施：只能完成与安全有关的管理功能，对其他完成非安全功能的操作要严格限制。当系统出现故障与灾难性事件后，要提供一种过程与机制，保证在不损坏保护的条件下，使系统得到恢复。

7. A1 安全级

A1 安全级又称为可验证设计保护级，即提供 B3 级保护的同时给出系统的形式化设计说明和验证以确信各安全保护真正实现。A1 类与 B3 类相似，对系统的结构和策略不作特别要求。A1 系统的显著特征是，系统的设计者必须按照一个正式的设计规范来分析系统。对系统进行分析后，设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求：系统管理员必须从开发者那里接收到一个安全策略的正式模型；所有的安装操作都必须由系统管理员进行；系统管理员进行的每一步安装操作都必须有正式文档。

A1 安全级的设计要求非常严格，达到这种要求的系统很少。目前已获得承认的此类系统有 Honeywell 公司的 SCOMP 系统。A1 安全级标准是安全信息系统的最高安全级别，一般信息系统很难达到这样的安全要求。

3.2 计算机网络安全等级评价标准

计算机网络由两部分组成：一是由多个独立的计算机系统组成的资源子网；二是由通信系统组成的通信子网。因此，网络的安全评价问题要比计算机系统的安全评价更加复杂。美国国防部计算机安全评估中心在制定可信计算机系统评价标准的基础上，又成立了专门的研究组来研究可信计算机网络的评估准则，并于 1987 年 6 月发表了可信计算机网络安全说明，在可信计算机系统评价标准的基础上增加了网络安全评价的内容。

在可信网络安全说明中借用了可信计算机系统安全评估中的可信计算基 TCB 的概念，建立了网络可信计算基 NTCB 的概念，它是由所有与网络安全相关的部分组成的，而不考虑网络信道的脆弱性和网络部件的同步和异步操作。可信网络安全说明要求任何被喷灌的网络系统必须具有清晰的网络安全结构与设计，网络安全结构中要包括对安全策略、目标与协议的说明。网络安全策略包括自主访问控制、强制访问控制、支撑策略（加密、认证与审计）和应用策略（如 DBMS 的支持及其安全策略）。为了作为一个可信实体来评价，网络安全设计要说明网络提供的接口与服务。

3.2.1　网络系统的安全等级

与计算机系统一样，计算机网络系统的安全也划分为七个等级，总体上又分为四类，即无安全等级、自主安全等级、强制保护等级和验证设计等级，其中，无安全等级为 D 级，自主安全级包括 C1 和 C2 两个等级，强制保护级包括 B1、B2 和 B3 三个等级，验证设计级为 A1 等级。它们的安全要求与计算机系统的相应安全等级对应。

1. D 级

无安全等级，没有任何安全措施，整个系统是不可信赖的。

2. C1 级

自主访问控制的低安全等级。该等级允许用多种方法实现网络环境下的用户认证，可以利用网络地址来解决用户组的识别问题。在安全网络系统的设计与实现时，NTCB 的部分自主访问控制功能可以由可信监控器来完成，管理系统的所有资源，控制主体与客体分离。但 C1 级并不要求在全部的网络系统部件内都实现自主访问控制的安全机理。

3. C2 级

自主访问控制的高安全等级。C2 级在 C1 级的基础上增加了审计功能，审计跟踪的信息包括客体的删除、将客体引入用户的地址空间、确认和识别安全机制的使用、操作人员与系统管理员所进行的与安全有关的活动等。另外，与网络结构和网络安全策略有关的安全事件也应该进行审计记录。

4. B1 级

该等级在 C2 的全部功能基础上又增加了强制访问控制策略。B1 级的安全策略要求网络的拥有者在网络中定义自主与强制保护策略，防止未经授权的用户读取委托给网络处理的敏感信息。在进程（或设备）中控制着与主体和存储客体有关的敏感标记，这些标记应由 NTCB 来保存，并把它们作为强制访问的判断依据。

5. B2 级

B2 级要求把 B1 级中实施的强制访问和自主访问控制策略扩展到网络系统中的所有主体与客体。对于保存网络控制信息的客体和其他网络结构（如路由表）必须标有安全标记，

防止被未经授权的访问所修改。NTCB 应能保证信息从源点准确地传输到目的点，任何导致对信息流的修改的活动都被看做是对完整性策略的侵犯。因此，B2 级要求 NTCB 具备能够自动测试、检验、报告超出指定网络完整性要求的错误和威胁的能力。

6. B3 级

B3 级网络要求通信信道和部件必须标识为单级安全的或多级安全的，并规定单级设备只能连接到单级信道上。要求 NTCB 包含一种具有能够监视安全审计事件的发生和积累的机制，并且能够在积累到一定的阈值时立即通知安全管理人员。B3 级要求根据网络安全结构使用一种简单而精确的语法定义保护机理来设计和构造 NTCB，以便于验证。且与安全有关的功能都应该放在 NTCB 内。B3 级还要求 NTCB 和其他部分出现故障时，网络系统应提供一种恢复进程，用以隔离故障部分，并保证其他部分能够正常工作，同时系统还应具有防渗透能力。

7. A1 级

该等级的安全要求在 B1 级的基础上，要求给出系统设计的形式化说明，并利用形式化验证技术来验证系统的安全功能，确保 NTCB 是完全符合设计要求的。

3.2.2 网络系统的安全服务

各安全等级网络中需要满足的安全要求和需要提供的安全机制都是支持网络提供安全服务的。除此之外还要求提供特定安全服务和辅助网络安全服务。

特定安全服务包括为保证通信的完整性、防止发生拒绝服务和防止泄露而提供相应安全措施。

1. 通信完整性

通信完整性由一组安全服务共同完成，其中包括鉴别、通信域完整性和不可否认等安全服务。

鉴别主要指对等实体之间的鉴别，用于判断正在通信的双方是否是所希望的实体。鉴别的主要方法有实体已知的东西（如密码）、加密方法和实体具有的特征（如指纹信息），这些用于鉴别的信息必须受到网络的保护。

通信域完整性是指报文头信息（即协议信息）和用户的数据域完整性。通信完整性保护就是指在通信过程中对这些域的保护。一个协议数据单元（PDU）中必须包括协议信息，而用户数据域则是可选的。

不可否认服务提供数据的收发双方都不能伪造所收发数据的证明。这种服务能够向数据的接收方提供发送者事后不能否认已发送报文的证明；向发送方提供接受者是否进行过篡改或伪造来自发送者文件的证明。采用的方法通常是数字签名技术和可信第三方认证技术。

2. 拒绝服务

拒绝服务是指网络系统不能向用户提供正常应该提供的服务。产生拒绝服务的原因通

常是由于网络的吞吐量下降到一定的阈值，或者不能对远程实体进行访问而引起的，有时也可能因系统资源被耗尽而引起拒绝服务。

防止拒绝服务可以通过多种措施来实现，如保证操作的连续性（包括利用冗余机制使网络具有高可靠性，提供灵活的网络控制功能等）、采用基于拒绝服务保护机理的协议以及完善的网络管理。

3. 泄露保护

防止信息泄露需要采取物理、管理和技术的综合措施。在技术方面，为了防止信息在线路上被窃听，可以采用加密技术。加密措施会对信息的使用带来不便之处，需要对密钥的粒度进行合理的折中，适当的粒度是对每个敏感级别适用一种密钥。

网络还可能受到信息流分析攻击，防护的办法除采用加密机制外，还可以采用信息流填充技术，使攻击者无法辨别哪些信息是有效的。另外，通过路由选择也可以有效地控制信息的泄露。

3.3　我国信息系统安全评价标准

为了提高我国计算机信息系统安全保护水平，以确保社会政治稳定和经济建设的顺利进行，公安部提出并组织制定了强制性国家标准 GB-17859：1999《计算机信息安全保护登记划分准则》，该准则于 1999 年 9 月 13 日经国家质量技术监督局发布，并于 2001 年 1 月 1 日起实施。该标准是建立安全等级保护制度、实施安全等级管理的重要基础性标准。它将计算机信息系统安全保护等级划分为五个级别，通过规范、科学和公正的评定和监督管理，达到以下三个目的：一是为计算机信息系统安全等级保护管理法规的制定和执法部门的监督检查提供依据；二是为计算机信息系统安全产品的研制提供技术支持；三是为安全系统的建设和管理提供技术指导。之后，公安部于 2002 年 7 月 18 日还公布并实施了一系列计算机信息系统安全等级保护标准，包括 GA/T390-2002《计算机信息系统安全等级保护通用技术要求》、GA/T388-2002《计算机信息系统安全等级保护操作系统技术要求》、GA/T389-2002《计算机信息系统安全等级保护数据库管理系统技术要求》、GA/T387-2002《计算机信息系统安全等级保护网络技术要求》、GA/T391-2002《计算机信息系统安全等级保护管理要求》等，进一步完善了计算机信息系统安全等级保护的标准体系。

3.3.1　所涉及的术语

在公安部制定的信息系统安全评价标准中，为了清晰地阐述标准的详细内容，定义了一系列基本术语。这些术语与 TCSEC 中的相关术语基本相似。

1. 计算机信息系统（computer information system）

计算机信息系统是由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

2. 计算机信息系统可信计算基(trusted computing base of computer information system)

计算机系统内保护装置的总体,包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的保护环境并提供一个可信计算机系统所要求的附加用户服务。

3. 客体(object)

信息的载体。

4. 主体(subject)

引起信息在客体之间流动的人、进程或设备等。

5. 敏感标记(sensitivity label)

表示客体安全级别并描述客体数据敏感性的一组信息,可信计算基中把敏感标记作为强制访问控制决策的依据。

6. 安全策略(security policy)

有关管理、保护和发布敏感信息的法律、规定和实施细则。

7. 信道(channel)

系统内的信息传输路径。

8. 隐蔽信道(covert channel)

允许进程以危害系统安全策略的方式传输信息的通信信道。

9. 访问监控器(reference monitor)

监控主体和客体之间授权访问关系的部件。

10. 可信信道(trusted channel)

为了执行关键的安全操作,在主体、客体及可信 IT 产品之间建立和维护的保护通信数据免遭修改和泄露的通信路径。

11. 客体重用

在计算机信息系统可信计算基的空闲存储客体空间中,对客体初始制定、分配或再分配一个主体之前,撤销该客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时,当前主体不能获得原主体活动所产生的任何信息。

3.3.2 等级的划分及各等级的要求

《计算机信息系统安全保护等级划分准则》将信息系统划分为五个等级,分别是自主保