ICS 35.020
L 09

GA

中华人民共和国公共安全行业标准

GA/T 387—2002

计算机信息系统安全等级保护 网络技术要求

Network technology requirement in computer information system classified security protection

2002-07-15 发布　　2002-07-15 实施

中华人民共和国公安部　发布

目　　次

此为试读,需要完整PDF请访问: www.ertongbook.com

前　言

GB 17859—1999《计算机信息系统安全保护等级划分准则》是我国计算机信息系统安全等级管理的重要标准，已于1999年9月13日发布。为促进安全等级管理工作正常有序地开展，特制定一系列相关的标准，包括：

——计算机信息系统安全等级保护技术要求系列标准；

——计算机信息系统安全等级保护管理要求；

——计算机信息系统安全等级保护工程实施要求；

——计算机信息系统安全等级保护评测系列标准。

其中，计算机信息系统安全等级保护技术要求系列标准由以下标准和其他相关标准组成：

GA/T 390—2002　计算机信息系统安全等级保护通用技术要求；

GA/T 387—2002　计算机信息系统安全等级保护网络技术要求；

GA/T 388—2002　计算机信息系统安全等级保护操作系统技术要求；

GA/T 389—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。

本标准是计算机信息系统安全等级保护技术要求系列标准的第2项。

本标准的附录A是资料性附录。

本标准由中华人民共和国公安部公共信息网络安全监察局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：江南计算技术研究所。

本标准主要起草人：刘广明、吉增瑞、景乾元、张文元、徐良华。

引　言

本标准是计算机信息系统安全等级保护技术要求系列标准的重要组成部分，用以指导设计者如何设计和实现具有所需要的安全等级的网络系统，主要从对网络系统的安全保护等级进行划分的角度来说明其技术要求，即主要说明为实现 GB 17859—1999 中每一个安全保护等级的安全要求对网络系统应采取的安全技术措施，以及各安全技术要求在不同安全保护等级中具体差异。

本标准按 GB 17859—1999 五个安全保护等级的划分，对每一个安全保护等级的安全功能技术要求和安全保证技术要求做了详细描述。本标准中有关概念的说明见附录 A。本标准参考的主要文件列在参考文献中。

计算机信息系统安全等级保护网络技术要求

1 范围

本标准规定了按 GB 17859—1999 对网络系统进行安全保护等级划分所需要的详细技术要求。

本标准适用于按 GB 17859—1999 的要求所进行的网络系统的设计和实现。按 GB 17859—1999 的要求对网络系统进行的测试、管理也可参照使用。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单(不包括勘误的内容)或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GA/T 390—2002 计算机信息系统安全等级保护通用技术要求

3 术语和定义

GB 17859—1999 和 GA/T 390—2002 中确立的术语和定义适用于本标准。

4 网络安全组成与相互关系

根据 idt ISO 7498-2:1989 的参考模型和 GB 17859—1999 所规定的安全保护等级和安全要素，网络安全的组成与相互关系如表 1 所示。

对于网络系统的每个协议层，如物理层、链路层、网络层、会话层、表示层、以及应用层，都可按 GB 17859—1999的要求进行设计。

在各层中，安全要素的实现方法应有所不同，本标准分别从物理层、链路层、网络层、会话层、表示层及应用层对 GB 17859—1999 中的各项安全要素在每个安全保护等级中应采用的安全技术和机制提出要求。对于每一个安全要素，则根据其提供的安全功能和安全保证来区分各个安全保护等级的差别。

表 1 安全等级、网络层次与安全要素的相互关系

安全等级、网络层次		安全要素											
		身份鉴别	自主访问控制	标记	强制访问控制	客体重用	审计	数据完整性	隐蔽信道分析	可信路径	可信恢复	抗抵赖	密码支持
用户自主保护级	物理层							☆					☆
	链路层	☆	☆					☆					☆
	网络层	☆	☆					☆					☆
	传输层	☆	☆					☆					☆
	会话层	☆	☆					☆					☆
	表示层	☆	☆					☆					☆
	应用层	☆	☆					☆					☆

表 1(续)

安全等级、网络层次		安全要素											
		身份鉴别	自主访问控制	标记	强制访问控制	客体重用	审计	数据完整性	隐蔽信道分析	可信路径	可信恢复	抗抵赖	密码支持
系统审计保护级	物理层							☆					☆
	链路层	☆	☆			☆		☆					☆
	网络层	☆	☆			☆	☆	☆					☆
	传输层	☆	☆			☆	☆	☆					☆
	会话层	☆	☆			☆	☆	☆					☆
	表示层	☆	☆			☆	☆	☆					☆
	应用层	☆	☆			☆	☆	☆				☆	☆
安全标记保护级	物理层							☆					☆
	链路层	☆	☆	☆	☆	☆		☆					☆
	网络层	☆	☆	☆	☆	☆	☆	☆				☆	☆
	传输层	☆	☆	☆	☆	☆	☆	☆				☆	☆
	会话层	☆	☆	☆	☆	☆	☆	☆				☆	☆
	表示层	☆	☆	☆	☆	☆	☆	☆				☆	☆
	应用层	☆	☆	☆	☆	☆	☆	☆				☆	☆
结构化保护级	物理层							☆					☆
	链路层	☆	☆	☆	☆	☆		☆					☆
	网络层	☆	☆	☆	☆	☆	☆	☆	☆	☆		☆	☆
	传输层	☆	☆	☆	☆	☆	☆	☆	☆	☆		☆	☆
	会话层	☆	☆	☆	☆	☆	☆	☆	☆	☆		☆	☆
	表示层	☆	☆	☆	☆	☆	☆	☆	☆	☆		☆	☆
	应用层	☆	☆	☆	☆	☆	☆	☆	☆	☆		☆	☆
访问验证保护级	物理层							☆					☆
	链路层	☆	☆	☆	☆	☆		☆					☆
	网络层	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
	传输层	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
	会话层	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
	表示层	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
	应用层	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆

注：“☆”号表示具有该要求。每个安全等级的具体要求可能不同，详见第 7 章描述。

5 网络基本安全技术

5.1 身份鉴别

5.1.1 用户标识

此为试读，需要完整PDF请访问：www.ertongbook.com

a) 基本标识：应在 TSF 实施所要求的动作之前，先对提出该动作要求的用户进行标识。

b) 唯一性标识：应确保所标识用户在计算机信息系统生命周期内的唯一性，并将用户标识与审计相关联。

c) 标识信息管理：应对用户标识信息进行管理、维护，确保其不被非授权地访问、修改或删除。

5.1.2 用户鉴别

a) 基本鉴别：应在 TSF 实施所要求的动作之前，先对提出该动作要求的用户成功地进行鉴别。

b) 不可伪造鉴别：应检测并防止使用伪造或复制的鉴别数据。一方面，要求 TSF 应检测或防止由任何别的用户伪造的鉴别数据；另一方面，要求 TSF 应检测或防止当前用户从任何其他用户处复制的鉴别数据的使用。

c) 一次性使用鉴别：应能提供一次性使用鉴别数据操作的鉴别机制，即 TSF 应防止与已标识过的鉴别机制有关的鉴别数据的重用。

d) 多机制鉴别：应能提供不同的鉴别机制，用于鉴别特定事件的用户身份，并且 TSF 应根据所描述的多种鉴别机制如何提供鉴别的规则，来鉴别任何用户所声称的身份。

e) 重新鉴别：应有能力规定需要重新鉴别用户的事件，即 TSF 应在需要重鉴别的条件表所指示的条件下，重新鉴别用户。例如，用户终端操作超时被断开后，重新连接时需要进行重鉴别。

5.1.3 用户-主体绑定

在 TCB 安全功能控制范围之内，对一个已标识和鉴别的用户，为了要求 TSF 完成某个任务，需要激活另一个主体(如进程)，这时，要求通过用户-主体绑定将该用户与该主体相关联，从而将用户的身份与该用户的所有可审计行为相关联。

5.1.4 鉴别失败处理

要求 TSF 为不成功的鉴别尝试次数(包括尝试数目和时间的阈值)定义一个值，以及明确规定达到该值时所应采取的动作。鉴别失败的处理应包括检测出现相关的不成功鉴别尝试的次数与所规定的数目相同的情况，并进行预先定义的处理。

5.2 自主访问控制

5.2.1 访问控制策略

TSF 应按确定的自主访问控制安全策略进行设计，实现对策略控制下的主体与客体间操作的控制。可以有多个自主访问控制安全策略，但它们必须独立命名，且不能相互冲突。常用的自主访问控制策略包括：访问控制表访问控制、目录表访问控制、权能表访问控制等。

5.2.2 访问控制功能

TSF 应明确指出采用一条命名的访问控制策略所实现的特定功能，说明策略的使用和特征，以及该策略的控制范围。

无论采用何种自主访问控制策略，TSF 应有能力提供：

——在安全属性或命名的安全属性组的客体上，执行访问控制 SFP；

——在基于安全属性的允许主体对客体访问的规则的基础上，允许主体对客体的访问；

——在基于安全属性的拒绝主体对客体访问的规则的基础上，拒绝主体对客体的访问。

5.3 标记

5.3.1 主体标记

应为主体指定敏感标记，这些敏感标记是等级分类和非等级类别的组合，是实施强制访问控制的依据。

5.3.2 客体标记

应为客体指定敏感标记，这些敏感标记是等级分类和非等级类别的组合，是实施强制访问控制的依据。

5.3.3 标记完整性

敏感标记应能准确地表示特定主体或客体的安全等级，主体和客体应以此发生关联。当数据从TCB输出时，根据需要，敏感标记应能准确地和明确地表示输出数据的内部标记，并与输出的数据相关联。

5.3.4 有标记信息的输出

TCB应对每个通信信道和I/O设备标明单级或多级。这个标志的任何变化都应由授权用户实现，并可由TCB审计。TCB应维持并且能够对安全等级的任何变化进行审定，或对与通信信道或I/O设备有关的安全等级进行审计。

a) 向多级安全设备的输出：当TCB将一客体信息输出到一个具有多级安全的I/O设备时，与该客体有关的敏感标记也应输出，并以与输出信息相同的形式(如机器可读或人可读形式)驻留在同一物理媒体上。当TCB在多级通信信道上输出或输入一客体信息时，该信道使用的协议应在敏感标记和被发送或被接收的有关信息之间提供明确的配对关系。

b) 向单级安全设备的输出：单级I/O设备和单级通信信道不需要维持其处理信息的敏感标记，但TCB应包含一种机制，使TCB与一个授权用户能可靠地实现指定的安全级的信息通信。这种信息经由单级通信信道或I/O设备输入/输出。

c) 人可读标记的输出：TCB应标记所有人可读的、编页的、具有人可读的敏感标记的硬拷贝输出(如行打印机输出)的开始和结束，以适当地表示输出敏感性。TCB应按默认值标记人可读的、编页的、具有人可读的敏感标记的硬拷贝输出(如行打印机输出)每页的顶部和底部，以适当地表示该输出总的敏感性，或表示该页信息的敏感性。TCB应该按默认值，并以一种适当方法标记具有人可读的敏感标记的其他形式的人可读的输出(如图形)，以适当地表示该输出的敏感性。这些标记默认值的任何滥用都应由TCB审计。

5.3.5 主体敏感标记显示

在终端用户交互对话期内，与该用户有关的敏感标记的各种变化，TCB应立即通知该用户，并在需要时显示完整的主体敏感标记。

5.3.6 设备标记

对各种附加物理设备，TCB应能支持最小和最大安全等级的分配。TCB应利用这些安全等级来实施对该设备安放的物理环境所强加的约束。

5.4 强制访问控制

5.4.1 访问控制策略

TSF应按确定的强制访问控制安全策略进行设计，并按需要确定访问控制策略的控制范围，包括策略控制下的主体、客体，及由策略覆盖的被控制的主体与客体间的操作。可以有多个访问控制安全策略，但它们必须独立命名，且不能相互冲突。按访问控制的覆盖范围，访问控制策略分为：

a) 子集访问控制：要求TSF的每个确定的基于敏感标记的访问控制，TSF应对属性所覆盖的主体、客体及其之间的操作，执行访问控制安全功能策略。

b) 完全访问控制：要求TSF的每个确定的基于敏感标记的访问控制，TSF应对属性所覆盖的主体、客体及其之间的操作，执行访问控制安全功能策略，并要求TSF应确保TSC内的任意一个主体和任意一个客体之间的所有操作将至少被一个确定的访问控制SFP覆盖。

常用的强制访问控制策略为多级安全模型。该模型要求TCB控制范围内的所有主体对客体的直接或间接的访问应满足：

——向下读原则——仅当主体敏感标记中的等级分类高于或等于客体敏感标记中的等级分类，且主体敏感标记中的非等级类别包含了客体敏感标记中的全部非等级类别，主体才能读该客体；

——向上写原则——仅当主体敏感标记中的等级分类低于或等于客体敏感标记中的等级分类，且主体敏感标记中的非等级类别包含于客体敏感标记中的非等级类别，主体才能写该客体。

5.4.2 访问控制功能

TSF 应明确指出采用一条命名的访问控制策略所实现的特定功能，说明策略的敏感标记的使用和特征，以及该策略的控制范围。按访问控制的覆盖范围，访问控制功能分为：

a） 子集访问控制：由相应子集访问控制策略实现的访问控制功能，能对 TSF 的敏感标记所覆盖的主体、客体及其之间的操作进行控制。

b） 完全访问控制：由相应的完全访问控制策略实现的访问控制功能，能对 TSF 的敏感标记所覆盖的主体、客体及其之间的操作进行控制，并要求 TSF 应确保 TSC 内的任意一个主体和任意一个客体之间的所有操作至少被一个确定的访问控制功能覆盖。

无论子集访问控制还是完全访问控制，TSF 应有能力提供：

——在敏感标记或命名的敏感标记组的客体上，执行访问控制 SFP；

——使用在受控客体上的受控操作所管理的受控主体和受控客体之间的访问规则，来决定受控主体与受控客体之间的操作是否被允许；

——在基于敏感标记的拒绝主体对客体访问的规则的基础上，实现拒绝主体对客体的访问。

5.5 客体重用

在对资源进行动态管理的系统中，客体资源（寄存器、内存、磁盘等记录介质）中的剩余信息不应引起信息的泄露。剩余信息保护分为：

a） 子集信息保护：要求对 TCB 安全控制范围之内的某个子集的客体资源，在将其分配给某一用户或代表该用户运行的进程时，应不会泄露该客体中的原有信息。

b） 完全信息保护：要求对 TCB 安全控制范围之内的所有客体资源，在将其分配给某一用户或代表该用户运行的进程时，应不会泄露该客体中的原有信息。

c） 特殊信息保护：对于某些需要特别保护的信息，应采用专门的方法对客体资源中的残留信息做彻底清除，如对剩磁的清除等。

5.6 安全审计

5.6.1 安全审计的响应

安全审计 TSF 应按以下要求响应审计事件：

a） 记审计日志：当检测到可能有安全侵害事件时，将审计数据记入审计日志。

b） 实时报警生成：当检测到可能有安全侵害事件时，生成实时报警信息。

c） 违例进程终止：当检测到可能有安全侵害事件时，将违例进程终止。

d） 服务取消：当检测到可能有安全侵害事件时，取消当前的服务。

e） 用户账号断开与失效：当检测到可能有安全侵害事件时，将当前的用户账号断开，并使其失效。

5.6.2 安全审计数据产生

TSF 应按以下要求产生审计数据：

a） 为下述可审计事件产生审计记录：

——审计功能的启动和关闭；

——使用身份鉴别机制；

——将客体引入用户地址空间（例如：打开文件、程序初始化）；

——删除客体；

——系统管理员、系统安全员、审计员和一般操作员所实施的操作；

——其他与系统安全有关的事件或专门定义的可审计事件。

b） 对于每一个事件，其审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功，及其他与审计相关的信息。

c） 对于身份鉴别事件，审计记录应包含请求的来源（例如：终端标识符）。

d） 对于客体被引入用户地址空间的事件及删除客体事件，审计记录应包含客体名及客体的安全等级。

e) 将每个可审计事件与引起该事件的用户相关联。

5.6.3 安全审计分析

安全审计分析应包括：

a) 潜在侵害分析：应能用一系列规则去监控审计事件，并根据这些规则指出 TSP 的潜在侵害。这些规则包括：

——由已定义的可审计事件的子集所指示的潜在安全攻击的积累或组合；

——任何其他的规则。

b) 基于异常检测的描述：应维护用户所具有的质疑等级——历史使用情况，以表明该用户的现行活动与已建立的使用模式的一致性程度。当用户的质疑等级超过门限条件时，TSF 应能指出将要发生对安全性的威胁。

c) 简单攻击探测：应能检测到对 TSF 实施有重大威胁的签名事件的出现。为此，TSF 应维护指出对 TSF 侵害的签名事件的内部表示，并将检测到的系统行为记录与签名事件进行比较，当发现两者匹配时，指出一个对 TSF 的攻击即将到来。

d) 复杂攻击探测：在上述简单攻击探测的基础上，要求 TSF 应能检测到多步入侵情况，并能根据已知的事件序列模拟出完整的入侵情况，还应指出发现对 TSF 的潜在侵害的签名事件或事件序列的时间。

5.6.4 安全审计查阅

安全审计查阅工具应具有：

a) 审计查阅：提供从审计记录中读取信息的能力，即要求 TSF 为授权用户提供获得和解释审计信息的能力。当用户是人时，必须以人类可懂的方式表示信息；当用户是外部 IT 实体时，必须以电子方式无歧义地表示审计信息。

b) 有限审计查阅：在上述审计查阅的基础上，审计查阅工具应禁止具有读访问权限以外的用户读取审计信息。

可选审计查阅：在上述有限审计查阅的基础上，审计查阅工具应具有根据准则来选择要查阅的审计数据的功能，并根据某种逻辑关系的标准提供对审计数据进行搜索、分类、排序的能力。

5.6.5 安全审计事件选择

应根据以下属性选择可审计事件：

a) 客体身份、用户身份、主体身份、主机身份、事件类型。

b) 作为审计选择性依据的附加属性。

5.6.6 安全审计事件存储

应具有以下创建并维护安全的审计踪迹记录的能力：

a) 受保护的审计踪迹存储：要求审计踪迹的存储受到应有的保护，能检测或防止对审计记录的修改。

b) 审计数据的可用性确保：要求在意外情况出现时，能检测或防止对审计记录的修改，以及在发生审计存储已满、存储失败或存储受到攻击时，确保审计记录不被破坏。

c) 审计数据可能丢失情况下的措施：要求当审计跟踪超过预定的门限时，应采取相应的措施，进行审计数据可能丢失情况的处理。

d) 防止审计数据丢失：要求在审计踪迹存储记满时，应采取相应的防止审计数据丢失的措施，可选择“忽略可审计事件”、“阻止除具有特殊权限外的其他用户产生可审计事件”、“覆盖已存储的最老的审计记录”和“一旦审计存储失败所采取的其他行动”等措施，防止审计数据丢失。

5.7 数据完整性

5.7.1 存储数据的完整性

应对存储在 TSC 内的用户数据进行完整性保护，包括：

此为试读，需要完整PDF请访问：www.ertongbook.com

a) 完整性检测：要求 TSF 应对基于用户属性的所有客体，对存储在 TSC 内的用户数据进行完整性检测。

b) 完整性检测和恢复：要求 TSF 应对基于用户属性的所有客体，对存储在 TSC 内的用户数据进行完整性检测，并且当检测到完整性错误时，TSF 应采取必要的恢复措施。

5.7.2 传输数据的完整性

当用户数据在 TSF 和其他可信 IT 产品间传输时应提供完整性保护，包括：

a) 完整性检测：要求对被传输的用户数据进行检测，及时发现以某种方式传送或接收的用户数据被篡改、删除、插入等情况发生。

b) 数据交换恢复：由接收者 TCB 借助于源可信 IT 产品提供的信息，或由接收者 TCB 自己无须来自源可信 IT 产品的任何帮助，能恢复被破坏的数据为原始的用户数据。

5.7.3 处理数据的完整性

a) 回退：对计算机信息系统中处理中的数据，应通过“回退”进行完整性保护，即要求 TSF 应执行访问控制 SFP，以允许对所定义的操作序列进行回退。

5.8 隐蔽信道分析

5.8.1 一般性的隐蔽信道分析

应通过对隐蔽存储信道的非形式化搜索，标识出可识别的隐蔽存储信道，并以文档形式说明以下情况：

a) 标识出隐蔽存储信道并估算它们的带宽。

b) 描述用于确定隐蔽存储信道存在的过程，以及进行隐蔽存储信道分析所需要的信息。

c) 描述隐蔽存储信道分析期间所作的全部假设。

d) 描述最坏的情况下对隐蔽存储信道带宽进行估算的方法。

e) 为每个可标识的隐蔽存储信道描述其最大可能的利用情形。

5.8.2 系统化的隐蔽信道分析

应通过对隐蔽信道的系统化搜索，标识出可识别的隐蔽信道，并以结构化、可重复的方式标识出隐蔽信道，并以文档形式说明以下情况：

a) 标识出隐蔽信道并估算它们的带宽。

b) 描述用于确定隐蔽信道存在的过程，以及进行隐蔽信道分析所需要的信息。

c) 描述隐蔽信道分析期间所作的全部假设。

d) 描述最坏的情况下对隐蔽信道带宽进行估算的方法。

e) 为每个可标识的隐蔽信道描述其最大可能的利用情形。

5.9 可信路径

用户与 TSF 间的可信路径应：

a) 提供真实的端点标识，并保护通信数据免遭修改和泄露。

b) 利用可信路径的通信可以由 TSF 自身、本地用户或远程用户发起。

c) 对原发用户的鉴别或需要可信路径的其他服务均使用可信路径。

5.10 可信恢复

a) 手动恢复：在发生失败或服务中断后，TSF 应进入维护方式，该方式将提供以手工方法将 TCB 返回到一个保护状态的能力。

b) 自动恢复：对失败或服务中断，TSF 应确保使用自动化过程使 TCB 返回到一个保护状态。当不能从失败或服务中断自动恢复时，TSF 应进入维护方式，该方式将提供以手工方法将 TCB 返回到一个保护状态的能力。

c) 无过分丢失的自动恢复：在自动恢复的基础上，要求 TSF 所提供的从失败或服务中断状态恢复的功能，应确保在 TSC 内的 TSF 数据或客体无超过限定量的丢失。

d） 功能恢复：对失败或服务中断，TSF 应确保安全功能或者被成功完成，或者对指定的情况恢复到一致的和安全的状态。

5.11 抗抵赖

5.11.1 抗原发抵赖

应确保信息的发送者不能成功地否认曾经发送过该信息。这就要求 TSF 提供一种方法，来确保接收信息的主体在数据交换期间能获得证明信息原发的证据，而且该证据可由该主体或第三方主体验证。

抗原发抵赖分为：

a） 选择性原发证明：要求 TSF 具有为主体提供请求原发证据信息的能力。即 TSF 在接到原发者或接收者的请求时，能就传输的信息产生原发证据，证明该信息的发送由该原发者所为。

b） 强制性原发证明：要求 TSF 在任何时候都能对传输的信息产生原发证据。即 TSF 在任何时候都能就传输的信息强制产生原发证据，证明该信息的发送由该原发者所为。

5.11.2 抗接收抵赖

应确保信息的接收者不能成功地否认对该信息的接收。这就要求 TSF 提供一种方法，来确保发送信息的主体在数据交换期间能获得证明该信息被接收的证据，而且该证据可由该主体或第三方主体验证。

抗接收抵赖分为：

a） 选择性接收证明：要求 TSF 具有为主体提供请求信息接收证据的能力。即 TSF 在接到原发者或接收者的请求时，能就接收到的信息产生接收证据，证明该信息的接收由该接收者所为。

b） 强制性接收证明：要求 TSF 总是对收到的信息产生接收证据。即 TSF 能在任何时候对收到的信息强制产生接收证据，证明该信息的接收由该接收者所为。

5.12 密码支持

应根据密码强度与信息系统安全等级匹配的原则，按国家密码主管部门的规定分级配置密码管理。

6 网络安全技术要求

6.1 身份鉴别技术要求

应按照用户标识和用户鉴别的要求进行身份鉴别安全机制的设计。

一般以用户名和用户标识符来标识一个用户，应确保在一个计算机信息系统中用户名和用户标识符的唯一性，严格的唯一性应维持在网络系统的整个生命周期都有效，即使一个用户的账户已被删除，他的用户名和标识符也不能再使用，并由此确保用户的唯一性和可区别性。

鉴别应确保用户的真实性。可以用口令进行鉴别，更严格的身份鉴别可采用智能 IC 卡、指纹、视网膜等特征信息进行身份鉴别，并在每次用户登录系统之前进行鉴别。口令应是不可见的，并在存储和传输时进行保护。智能 IC 卡身份认证应以密码技术为基础，并按用户鉴别中不可伪造鉴别所描述的要求进行设计。对于鉴别失败的情况，要求按鉴别失败所描述的要求进行处理。

用户在系统中的行为一般由进程代为执行，要求按用户-主体绑定所描述的要求，将用户与代表该用户行为的进程相关联。这种关联应体现在 TCB 安全功能控制范围之内各主、客体之间的相互关系上。比如，一个用户通过键入一条命令要求访问一个指定文件，计算机信息系统运行某一进程实现这一功能。这时，该进程应与该用户相关联，于是该进程的行为即可看作该用户的行为。

身份鉴别应区分实体鉴别和数据起源鉴别：当身份是由参与通信连接或会话的远程实体提交时叫实体鉴别，它可以作为访问控制服务的一种必要支持；当身份信息是由数据项发送者提交时叫数据起源鉴别，它是确保部分完整性目标的直接方法，确保知道某个数据项的真正起源。

表 2 给出了从第一级到第五级对身份鉴别技术的不同要求。

表 2　身份鉴别技术要求

安全等级和网络层次		基本安全技术			
		5.1.1 用户标识	5.1.2 用户鉴别	5.1.3 用户-主体绑定	5.1.4 鉴别失败处理
用户自主保护级	物理层				
	链路层	☆	☆		☆
	网络层	☆	☆		☆
	传输层	☆	☆		☆
	会话层	☆	☆		☆
	表示层	☆	☆		☆
	应用层	☆	☆		☆
系统审计保护级	物理层				
	链路层	☆	☆		☆
	网络层	☆	☆		☆
	传输层	☆	☆		☆
	会话层	☆	☆		☆
	表示层	☆	☆		☆
	应用层	☆	☆		☆
安全标记保护级	物理层				
	链路层	☆	☆		☆
	网络层	☆	☆		☆
	传输层	☆	☆		☆
	会话层	☆	☆		☆
	表示层	☆	☆		☆
	应用层	☆	☆	☆	☆
结构化保护级	物理层				
	链路层	☆	☆		☆
	网络层	☆	☆		☆
	传输层	☆	☆		☆
	会话层	☆	☆		☆
	表示层	☆	☆		☆
	应用层	☆	☆	☆	☆
访问验证保护级	物理层				
	链路层	☆	☆		☆
	网络层	☆	☆		☆
	传输层	☆	☆		☆
	会话层	☆	☆		☆
	表示层	☆	☆		☆
	应用层	☆	☆	☆	☆
注：“☆”号表示具有该要求。每个安全等级的具体要求可能不同，详见第 7 章描述。					

6.2　自主访问控制技术要求

应按照对访问控制策略的要求，选择所需的访问控制策略，并按照对访问控制功能的要求，设计和

实现所需要的自主访问控制功能。

当使用文件、目录和网络设备时，网络管理员应给文件、目录等指定访问属性。访问控制规则应将给定的属性与网络服务器的文件、目录和网络设备相联系。网络上的资源都应预先标出一组安全属性。用户对网络资源的访问权限对应一张访问控制表，用以表明用户对网络资源的访问能力。自主访问控制应能控制以下权限：

a） 向某个文件写数据、拷贝文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。

b） 为每个命名客体指定用户名和用户组，以及规定他们对客体的访问模式。

表 3 给出了从第一级到第五级对自主访问控制技术的不同要求。

表 3 自主访问控制技术要求

安全等级和网络层次		基本安全技术	
		5.2.1 访问控制策略	5.2.2 访问控制功能
用户自主保护级	物理层		
	链路层	☆	☆
	网络层	☆	☆
	传输层	☆	☆
	会话层	☆	☆
	表示层	☆	☆
	应用层	☆	☆
系统审计保护级	物理层		
	链路层	☆	☆
	网络层	☆	☆
	传输层	☆	☆
	会话层	☆	☆
	表示层	☆	☆
	应用层	☆	☆
安全标记保护级	物理层		
	链路层	☆	☆
	网络层	☆	☆
	传输层	☆	☆
	会话层	☆	☆
	表示层	☆	☆
	应用层	☆	☆
结构化保护级	物理层		
	链路层	☆	☆
	网络层	☆	☆
	传输层	☆	☆
	会话层	☆	☆
	表示层	☆	☆
	应用层	☆	☆

表 3(续)

安全等级和网络层次		基本安全技术	
		5.2.1 访问控制策略	5.2.2 访问控制功能
访问验证保护级	物理层		
	链路层	☆	☆
	网络层	☆	☆
	传输层	☆	☆
	会话层	☆	☆
	表示层	☆	☆
	应用层	☆	☆
注：“☆”号表示具有该要求。每个安全等级的具体要求可能不同，详见第 7 章描述。			

6.3 标记技术要求

应按照主体标记和客体标记所描述的要求进行标记设计。

在网络环境中，带有特定标记的数据应能被安全策略禁止通过某些子络、链路或中继。连接的发起者(或无连接数据单元的发送者)可以指定路由选择说明，请求回避某些特定的子络、链路或中继。

包含数据项的资源应具有与这些数据相关联的安全标记。安全标记可能是与被传送的数据相连的附加数据，也可能是隐含的信息，例如使用一个特定密钥加密数据所隐含的信息或由该数据的上下文所隐含的信息，可由数据源或路由来隐含。明显的安全标记必须是清晰可辨认的，以便对它们作适当的验证。此外，它们还必须安全可靠地依附于与之关联的数据。

对于在通信期间要移动的数据项，发起通信的进程与实体，响应通信的进程与实体，在通信时被用到的信道和其他资源等，都可以用各自的敏感信息来标记。安全策略应指明如何使用敏感信息以提供必要的安全性。当安全策略是基于用户身份时，不论直接或通过进程访问数据，安全标记均应包含有关用户身份的信息。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，如果需要，还应与端系统协商。标记可以附带敏感信息，指明其敏感性，说明处理与分布上的隐蔽处，强制定时与定位，以及指明对该端系统特有的要求。

采用的安全策略决定了标记所携带的敏感信息及其含义，不同的网络会有差异。

表 4 给出了从第三级到第五级对标记技术的不同要求。

表 4 标记技术要求

安全等级和网络层次		基本安全技术								
		5.3.1 主体标记	5.3.2 客体标记	5.3.3 标记完整性	5.3.4 有标记信息的输出	a)向多级安全设备的输出	b)向单级安全设备的输出	c)人可读标记的输出	5.3.5 主体敏感标记显示	5.3.6 设备标记
安全标记保护级	物理层									
	链路层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	网络层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	传输层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	会话层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	表示层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	应用层	☆	☆	☆	☆	☆	☆	☆	☆	☆

表 4(续)

安全等级和网络层次		基本安全技术								
		5.3.1 主体标记	5.3.2 客体标记	5.3.3 标记完整性	5.3.4 有标记信息的输出	a)向多级安全设备的输出	b)向单级安全设备的输出	c)人可读标记的输出	5.3.5 主体敏感标记显示	5.3.6 设备标记
结构化保护级	物理层									
	链路层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	网络层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	传输层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	会话层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	表示层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	应用层	☆	☆	☆	☆	☆	☆	☆	☆	☆
访问验证保护级	物理层									
	链路层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	网络层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	传输层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	会话层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	表示层	☆	☆	☆	☆	☆	☆	☆	☆	☆
	应用层	☆	☆	☆	☆	☆	☆	☆	☆	☆
注：“☆”号表示具有该要求。每个安全等级的具体要求可能不同，详见第 7 章描述。										

6.4 强制访问控制技术要求

应按照强制访问控制策略的要求，选择所需的访问控制策略，并按照对强制访问控制功能的要求，设计和实现所需要的强制访问控制功能。

强制访问控制应由专门设置的系统安全员统一管理系统中与该访问控制有关的事件和信息。为了防止由于系统管理人员或特权用户的权限过于集中所带来的安全隐患，应将系统的常规管理、与安全有关的管理以及审计管理，由系统管理员、系统安全员和系统审计员分别承担，并在三者之间形成相互制约的关系。

采用多级安全模型的强制访问控制应将 TCB 安全控制范围内的所有主、客体成分通过标记方式设置敏感标记(非等级分类)，这些敏感标记与访问规则一起确定每一次主体对客体的访问是否被允许。

这里所要求的对客体的控制范围除涉及系统内部的存储、处理和传输过程外，还应包括将信息进行输入、输出操作的过程，即无论信息以何种形式存在，都应有一定的安全属性与其相关联，并按强制访问控制规则对其进行控制。

第三级的强制访问控制应对 TCB 所定义的主体与客体实施控制。第四级以上的强制访问控制应扩展到计算机信息系统中的所有主体与客体。表 5 给出了第三级到第五级强制访问控制技术的不同要求。

6.5 客体重用技术要求

应按照剩余信息保护中子集信息保护/完全信息保护的要求进行设计。

当网络资源动态分配时，应确保曾在该资源中存放过的信息不因动态分配而泄露。在向一个主体初始转让、分配或重分配客体之前或回收客体资源以后，应确保其残留信息全部被清除。表 6 给出了从二级到第五级对客体重用技术的不同要求。

此为试读，需要完整PDF请访问：www.ertongbook.com