SJ

中华人民共和国电子行业军用标准

FL 0137

SJ 20628—97

通用型军用计算机信息安全技术要求

Information security technical requirements for general military computers

1997-06-17 发布

1997-10-01 实施

中华人民共和国电子工业部 批准

目　次

中华人民共和国电子行业军用标准

通用型军用计算机信息安全技术要求

SJ 20628—97

Information security technical requirements for general military computers

1 范围

1.1 主题内容

本标准规定了军用计算机系统信息安全的通用技术要求。

本标准不涉及信息安全立法、行政管理和计算机系统工作场区、辅助设施以及计算机系统工作环境条件的安全保护要求。

1.2 适用范围

本标准适用于通用型军用计算机信息安全系统的研制、开发和应用。对有相应信息安全要求的其他系统亦可参照使用。

2 引用文件

GJB 1281—91 指挥自动化计算机网络安全要求

GJB 1894—94 指挥自动化系统数据加密要求

GJB 2256—94 军用计算机安全术语

GJB 2646—96 军用计算机安全评估准则

3 定义

3.1 术语

下列术语适用于本标准。

3.1.1 访问控制 access control

对用户、程序或进程访问系统资源进行授权与控制的过程。

同义词:受控访问 controlled access;受控访问性 controlled accessibility。

3.1.2 访问控制机制 access control mechanisms

在信息系统中,为检测和防止未授权访问,以及为使授权访问正确进行所设计的硬件或软件功能、操作规程、管理规程和它们的各种组合(见 GJB 2256 中 3.4)。

3.1.3 审计跟踪 adit trail

系统活动的流水记录。该记录按事件从始至终的途径,顺序重视、审查和检验每个事件的

中华人民共和国电子工业部 1997-06-17 发布 1997-10-01 实施

环境及活动。

3.1.4 鉴别 authentication

a. 验证用户、设备和其他实体的身份；

b. 验证数据的完整性(见 GJB 2256 中 3.16)。

3.1.5 授权 authorization

授予用户、程序或进程的访问权(GJB 2256 中 3.18)。

3.1.6 认证 certification

信息系统技术和非技术的安全特征及其他防护的综合评估，用以支持审批过程和确定特殊的设计和实现满足一系列预定的安全需求的程度(见 GJB 2256 中 3.28)。

3.1.7 泄漏 compromise

未授权的暴露或丢失敏感信息(见 GJB 2256 中 3.31)。

3.1.8 计算机安全 computer security

保护信息系统免遭拒绝服务、未授权(意外的或有意的)暴露、修改和数据破坏的措施和控制(见 GJB 2256 中 3.33)。

3.1.9 隐蔽系统 concealment system

把敏感信息嵌入到不相关的数据中，使其隐蔽起来，从而达到保密的一种手段(见 GJB 2256 中 3.34)。

3.1.10 保密性 confidentiality

为秘密数据提供保护状态及保护等级的一种特性(见 GJB 2256 中 3.35)。

3.1.11 隐蔽信道 covert channel

使两个共同运行的进程，以违反系统安全策略的方式传输信息的通信信道(见 GJB 2256 中 3.44)

3.1.12 隐蔽存储信道 covert storage channel

包含由一个进程直接或间接写一个存储地址，而由另一个进程直接或间接读一个存储地址的隐蔽信道(见 GJB 2256 中 3.4.5)。

3.1.13 密码算出 cryptographic algorithm

用来从明文产生密钥流或密文，或从密钥流或密文产生明文而有严密定义的规程，或一系列规则或步骤。

3.1.14 数据完整性 data integrity

信息系统中的数据与在原文档中的相同，并未遭受偶然或恶意的修改或破坏时所具的性质(见 GJB 2256 中 3.56)。

3.1.15 数据安全 data security

保护数据免受偶然的或恶意的修改、破坏或暴露(见 GJB 2256 中 3.58)。

3.1.16 解密 decipherment

使用适当的密钥，将已加密的文本转换成明文。

3.1.17 自主访问控制 discretionary access control

根据用户、进程、所属的群的标识和已知需要来限制对客体访问的一种手段。自主访问的含义是有访问许可的主体能够向其他主体转让访问权(见 GJB 2256 中 3.62)。

3.1.18 窃取 eavesdropping

通过使用非搭线窃听的办法未授权截获信息(见 GJB 2256 中 3.64)。

3.1.19 加密 encipherment

通过密码系统把明文变换为不可懂的形式。

3.1.20 加密算法 encryption algorythm

实施一系列变换,使信息变成密文的一组数学规则(见 GJB 2256 中 3.68)。

同义词:保密换算 privacy transformation。

3.1.21 形式验证 format verification

使用形式证明的过程,以论证系统形式说明与形式安全策略模型间的一致性(设计验证),或论证形式说明与它的程序实现间的一致性(执行验证)(见 GJB 2256 中 3.84)。

3.1.22 识别 identification

通过机器可读的唯一名,由系统来认定实体的过程(GJ 2256 中 3.87)。

3.1.23 信息安全 information security

为保证信息的完整性、可用性和保密性所需的全面管理、规程和控制(见 GJB 2256 中 3.90)。

3.1.24 信息系统安全 information system security

为了提供对信息系统的保护,在计算机硬件、软件和数据上所建立的技术安全设施和管理规程(见 GJB 2256 中 3.91)。

3.1.25 密钥 key

在密码术中,一系列控制加密、解密操作的符号(见 GJB 2256 中 3.95)。

3.1.26 密钥管理 key management

涉及密钥和有关信息(如初始化矢量)的生成、分配、存储和销毁的规程(见 GJB 2256 中 3.96)。

3.1.27 强制访问控制 mandatory access control

根据客体所含信息的敏感性及主体对这些敏感信息访问的正式授权来限制对客体访问的一种手段(见 GJB 2256 中 3.104)。

3.1.28 多级安全 multilevel security

一类包含不同等级敏感信息的系统,它既可供那些确有必要且具有不同安全许可和已知需要的用户同时访问,又能阻止用户去访问其无权过问的信息。

3.1.29 安全评估 security evaluation

为评定在系统内安全处理敏感信息的可信度而做的评估。

3.1.30 安全内核 security kernel

控制对系统资源的访问而实现基本安全规程的计算机系统的中心部分(见 GJB 2256 中 3.151)。

3.1.31 安全策略 security policy

规定机构如何管理、保护与分发敏感信息的法规与条例的集合(见 GJB 2256 中 3.153)。

3.1.32 敏感信息 sensitive information

由于有意或无意的泄密、修改或破坏,可能造成很大损失或危害,需要某种等级保护的信息(见 GJBB 2256 中 3.157)。

3.1.33 系统完整性 system integrity

在任何情况下,信息系统都保持操作系统逻辑上的正确性和可靠性;实现保护机制的硬件和软件的完备性时所处的状态(见 GJB 2256 中 3.162)。

3.1.34 威胁 threat

以破坏、泄漏、数据修改和拒绝服务的方式，可能对系统造成损害的环境或潜在事件(见GJB 2256 中 3.167)。

3.1.35 防泄漏发射 transient electromagnetic pulse emanation standard(TEM-PEST)

对信息系统的泄漏发射所进行的研究和控制(见 GJB 2256 中 3.171)。

3.1.36 可信计算机系统 trusted computer system

采用充分的软件和硬件保证措施，能同时处理大量敏感或不同类别信息的系统(GJB 2256 中 3.174)。

3.1.37 可信计算基 trusted computing base

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(见 GJB 2256 中 3.175)。

3.1.38 用户鉴别 user authentication

见 3.1.1 和 3.1.4 条。

3.1.39 用户标识 user identification(user ID)

信息系统用以标识用户的一个独特符号或字符串(见 GJB 2256 中 3.179)。

3.1.40 确认 validation

为确定是否符合安全规定和要求而进行的测试和评估(见 GJB 2256 中 3.180)。

3.1.41 验证 verification

对两个适当级别的规格说明进行比较的过程。例如安全策略模型与顶层规格说明、顶层规格说明与源码、或者源码与目标码的比较(见 GJB 2256 中 3.181)。

3.1.42 病毒 virus

一种能自身传播的特洛伊木马。它一般由引导部分、破坏部分和自身传播部分组成(见 GJB 2256 中 3.182)。

3.1.43 脆弱性 vulnerability

导致破坏系统安全策略的系统安全规程、系统设计、实现、内部控制等方面的弱点(见 GJB 2256 中 3.183)。

3.1.44 窃听 wiretapping

窃听有两种情况，一是主动搭线窃听，即把未经批准的装置(如计算机终端)连到通信线路上，通过生成错误信息或控制信号，或者通过改换合法用户的通信方式以获取对数据的访问；二是被动窃听，即将通信线路上正在传送的数据被进行非法监听和记录。

3.2 符号和缩写词

TEMPEST	防泄漏发射
DBMS	数据库管理系统
DES	数据加密标准(一种分组加密/解密算法)
RSA	系 Rivest、Shamir 和 Adleman 三人名的缩写词(一种公开密钥加密/解密算法)
ISDN	综合业务数字通信网
B-ISDN	宽带综合业务数字通信网

4 一般要求

4.1 一般原则

4.1.1 应用环境

计算机系统的信息安全要求适用于下列环境：

a. 局域网和广域网，包括城域网、网际网(见 GJB 1281)；

b. 各种通信信道，如专用线路，公用电话网，X.25 分组交换网(包括快速交换)，卫星通信网，短波、超短波无线通信网，综合业务数字通信网(ISDN)以及宽带综合业务数字通信网(B－ISDN)等；

c. 计算机(集中和分布)应用处理模式；

d. 数据库系统；

e. 各种计算应用系统的互连、互通、互操作。

4.1.2 信息安全威胁

在考虑信息安全要求时，应估计到下列计算机系统本身固有的脆弱性和常见威胁的影响。

4.1.2.1 计算机系统的脆弱性

计算机系统可能存在下述脆弱性：

a. 信息存储的高密度

存储媒体可以存储大量信息，也便于随身携带，但易受意外损坏，因而可能会造成大量信息的丢失。

b. 信息泄漏

计算机系统工作时辐射出电磁可能会造成信息泄漏。

c. 信息的可访问性

信息易被访问复制而不留痕迹，一旦未授权者进入系统，可能访问系统中的信息并将其复制、删改或破坏掉。

d. 磁性媒体的剩磁效应

存储媒体中的信息有时是擦不净的，可能会留下可读信息的痕迹，一旦被利用，就会造成泄密。

e. 信息的聚生性

计算机处理时往往汇集了大量信息，这种信息的聚生性可能带来很大的潜在性安全风险。

f. 通信线路的脆弱性

对线路的物理破坏、被搭线窃听、传输串音等，可能会导致信息失密或受破坏。

g. 计算机技术的专业性

对一个拥有计算机专业技术知识，谙熟系统者，可能会突破信息的安全防护。反之，对没有多少计算机专业知识，不熟悉系统的管理、使用者，往往可能会觉察不到系统信息被窃取或遭到破坏。

4.1.2.2 常见威胁对信息安全性的影响

影响信息安全的常见威胁，见表 1。

表1

常见威胁	对信息安全性的影响		
	保密性	完整性	可用性
后门(设计者故意建立的进入系统的方法)	√	√	√
人为错误	√	√	√
拒绝使用(信息无法使用)			√
电磁泄漏	√		
信息盗用		√	
自然灾害		√	√
伪造文件或记录		√	
诈骗信息资源		√	
硬设备故障	√	√	√
访问假冒	√	√	√
不准确或过时的信息		√	
逻辑炸弹(修改程序,使之在特定条件下按某种不同的方式运行	√	√	√
错误的传输指向	√		
窃读通信(用网络分析器)	√		
附加负载	√	√	√
程序编制错误或缺陷	√	√	√
物理或逻辑破坏		√	√
废物利用(发现有用信息)	√		
偷窃	√	√	√
特洛伊木马(嵌在合法用户程序中的一段程序)	√	√	√
病毒		√	√
搭线窃听	√		
串音	√	√	

注:√——为有影响。

4.1.3 信息安全防护

应开发与实施有效的信息安全策略、安全机制和相应的信息安全软、硬件,检查各种信息安全防护措施的有效性,以保护系统信息资源,尽可能减少系统面临的各种威胁所造成的损失。还应有适当的应急计划,以防备系统在遭到攻击或破坏时,采用准备好的应急措施尽快地恢复系统正常工作。

4.2 信息安全特性

4.2.1 保密性

应利用密码技术对信息进行加密处理,并采取抑制、屏蔽措施,防止电磁信息泄漏,以保证

信息只透露给有权用户。

保密性的要求如下：

a. 采用的密码体制及密码算法(见 GJB 1894)应有足够的保密强度。其密钥应有严格的保护,使之能承受各种级别的破译攻击,达到实际上的不可破译；

b. 应有有效的密钥管理,包括密钥的产生、存储、分配、更换、保管、使用、销毁的全过程。应做到密钥难以被窃取,即使被窃取也已失去应有的价值；

c. 为了可靠地检测出对传输的信息的主动攻击(如分析通信流量,篡改内容),且保证在传输的信息被截获后(如搭线侦听)也得不到信息的明文内容,对传输的信息,应能在各种传输方式下,如全双工、半双工、同步、异步、点对点、点对多点传输等,予以加密保护；

加密不同密级的信息,应有相应的保密强度和完善、合理的密钥管理。不允许用同一密钥加密两份或两份以上明文,也不允许用不同强度的密码加密同一明文。完成加密操作对信息传输、处理速度等影响不能超过原有系统要求所允许的范围；

d. 为了防止存储的信息泄露给无关人员或被非法获取、篡改以至破坏,对存储的信息应予以加密保护。应根据存储信息的密级、信息特征,以及使用信息资源的开放程度等具体情况确定加密保护方式(局部、全局加密；库内、库外加密等)。加密不应采用一次一密。保密强度应达到实际上的不可破译的程度；

密钥管理应适应加密信息存储时间短,以及不同用户访问信息时所用主密钥相同的要求。完成加密操作对占用的处理时间、存储空间等系统资源,以及查询、检索、修改、更新等操作时间与使用灵活简便性的影响,不能超过原有系统要求所允许的范围；

e. 为了防止电磁信息泄漏带来的信息失密,应对传导和辐射产生的电磁信号泄漏进行有效的屏蔽和抑制。应制定相应的标准来规定防护的分级要求。对此,可视系统的使用场合,环境条件,采用的防护方式,允许的安全区域,窃密者对泄漏信号接收、恢复的能力以及价格等因素,合理地确定防护等级。

4.2.2 可用性

应防止未授权者进入系统去访问、窃取与破坏信息资源,并保证合法用户访问到它有权访问的信息资源。

可用性的要求如下：

a. 身份识别与确认

系统应识别进入者的身份并确认是否为合法用户的身份。只有身份识别与确认都正确,才允许此用户进入系统。

采用识别、确认的手段要达到一定的精度要求,且不应受丢失、泄露或被他人伪造的影响。

b. 访问控制

对信息应划分级别并规定要被访问的系统资源的类别及其访问操作类型的授权机制。对用户应划分为几种属性的用户类别,并规定与信息的保密级别和允许访问的系统资源的类别及其访问操作类型相适应的权限签证机制,以便使系统能确定具有哪种签证,哪种权限,什么属性的合法用户能对哪些系统资源,哪种保密级别的信息,可进行什么类型的访问操作。

根据安全等级要求,系统应具有一种自主访问控制机制,或自主访问控制与强制访问控制两种机制。系统还应防止或限制隐蔽信道的信息泄露。作为对访问控制的重要补充,还应具有信息流控制机制。

c. 审计

对应用程序或用户使用系统资源，涉及信息安全事件的有关操作，包括欺诈操作的情况，应有一个完整的记录，以便分析原因，分清责任，并能采取相应安全措施，如将违反操作的用户逐出系统。

记录内容一般应包括所在数据终端上进行了哪些非法操作，使用了什么系统资源，进行了何种访问类型的操作，以及有关操作处理的时刻、顺序等。应选择主要内容记录予以审计，不应影响系统原有性能要求的允许范围。审计还应与报警结合起来，以便及时向安全员发出提醒或报警信息以便预防或采取补救措施。

4.2.3 完整性

应防止信息被非法复制，非授权泄露、修改和破坏，以保证信息的正确性、有效性、一致性和授权的访问、修改，并保证信息交换的真实性、有效性。

完整性的要求如下

a. 软件完整性

为了防止软件被非法复制，软件必须有唯一的标识且能检验这种标识是否存在以及是否被修改过。还应有拒绝动态跟踪分析的能力，以免复制者绕过该标识的检验。为了防止软件被非法修改，软件应有抗分析能力和完整性校验手段。应对软件进行加密处理，即使复制者得到源代码也不能进行静态分析。

b. 数据完整性

对存储数据的媒体应定期检查物理损伤情况。要尽量减少误操作、硬件故障、软件错误、掉电、强电磁场的干扰等意外事件。要在检测错误输入、不正确程序等潜在性错误的完整性校验和审计手段。对只需调用的数据，可集中组成数据模块后，使之无法读出和修改。

对数据还应有容错、后备和恢复能力。

c. 信息交换的真实性和有效性

信息交换的收方应能证实所收到信息的来源、内容和顺序都是真实的。为了保证信息交换的有效性，收方收到了真实信息应予以确认。且对收到的信息不能删改或伪造，也不能抵赖、否认。而发方也不能谎称从未发过信息，也不应声称信息是收方伪造的。

4.3 安全系统的组成与基本安全功能要求

4.3.1 安全系统的组成

安全系统是为增强一般计算机系统的信息安全性而扩充的一个子系统，它由安全硬件和安全软件组成。

a. 安全硬件主要是低泄漏计算机、保密设备以及各种安全卡，如防/反病毒卡、身份识别卡等；

b. 安全软件主要是安全操作系统、安全网络系统、安全数据库管理系统以及专用安全软件(如反病毒软件、身份识别软件、加/解密软件、系统监视软件等)。

4.3.2 硬件设备的基本安全功能要求

4.3.2.1 防信息泄漏计算机

防泄漏发射(TEMPEST)计算机应遵循有关标准规定的安全临界值(即处理的信息在1m的距离上，不为具有高灵敏度的TEMPEST接收系统所截收的信息泄漏的边界电平)。如果泄漏电平超出临界值，由必须有抑制的防护措施。TEMPEST分三级要求，即完全保护级1m、20m、100m级。相应临界值的频率范围为1kHz～18GHz，其安全距离为1m、20m、100m。信息泄漏的具体指标由相应的标准规定。

4.3.2.2 保密设备

保密设备一般有两类:一类是用于相邻网络节点间数据传输加密的线路保密机;另一类是用于源点到目的点间数据传输加密的用户保密机。

线路保密机的基本功能要求包括:

a. 适应的通信方式:物理接口、信道、工作方式(点到点、点到多点、半双工、全双工、异步、同步)、数据传输速率和通信协议;

b. 加密保护内容和保密强度;

c. 密钥管理方式;

d. 数据传输正确性

e. 加/解密速度;

f. 资源开销;

g. 加、解密和传输、操作、显示等控制;

h. 自诊断和检测;

i. 可靠性和可维护性;

j. 使用方便。

用户保密机的基本功能除上述 a～i 的要求外,还应突出人机界面友好。

4.3.3 操作系统的基本安全功能要求

高安全级的操作系统(包括计算机系统的操作系统和网络操作系统,按 GJB 2646 的要求,应为 B 级以上)的实现应基于安全核。

操作系统的基本安全功能如下:

a. 用户标识与确认包括:

用户唯一性标识、用户身份合法性确认、为进入系统的用户设置用户选定的安全级和建立安全文档、删除用户并撤消其安全文档以及安全级的调整等;

b. 自主访问控制指:

对文件类资源进行自主访问控制,即对文件、目录等的读、写、执行,对目录的搜索和改动等授权操作等;

c. 强制访问控制包括:

设置、封闭、显示等安全级管理(但非特权用户不能管理安全级),设置用户登录安全级(但非特权用户不能管理用户安全级),对进程安全级继承关系,对普通文件的、普通目录与多级目录的访问以及对消息队列、共享存储器、信号量的访问;

在实施上述强制访问控制时,应满足强制访问控制规则,还应满足进程敏感操作的特权管理、防病毒、防特洛伊木马攻击等;

d. 信息流控制包括:

可信路径以及与其它路径的隔离隐蔽信道分析;

e. 安全审计包括:

审计事件的指定、选择、调用,记录的分析、显示报告、报警等;

f. 系统故障或其它间断后的可信恢复;

g. 加密文件系统;

h. 适用平台和兼容应用软件。

4.3.4 数据库系统的基本安全功能要求

鉴于对现已广泛使用的低安全级的数据库系统，保持原有系统接口，对其内核进行面向安全性的改造和开发，可以提高安全等级，但系统的时空开销大，且很难达到高安全级（按 GJB 2646 中的规定，应为 B2 级以上），因此，安全数据库系统应以可信计算基为安全内核；自行研制安全数据库管理系统（DBMS），以保证安全性和效率。

安全数据库系统应以安全操作系统为支撑。对于分布式数据库系统，还应以安全网络系统为支撑。

多级安全关系型数据库系统的基本安全功能如下：

a. 用户标识与确认；

b. 访问控制和授权；

c. 客体再使用；

d. 信息流控制和隐蔽信道分析；

e. 安全审计，包括资源审计、操作审计、应用程序审计、欺诈审计、产生隐蔽信道事件审计等；

f. 推断控制，应能释放群体统计信息，不泄露敏感信息；

g. 数据库加密，应考虑密码强度、加密粒度、加密速度、安全简便的密钥管理、库系统运行效率；

h. 数据完整性和可靠性，应具数据语义完整性、并发控制、数据容错、备份与恢复；

i. 适用的平台。

4.3.5 网络系统的基本安全功能要求

4.3.5.1 安全体系结构

高安全级（按 GJB 2646 中的规定，应为 B 级以上）的开放型网络，应具有如下六类安全服务：

a. 对等实体鉴别；

b. 访问控制；

c. 数据保密；

d. 数据完整性；

e. 数据源点鉴别；

f. 抗抵赖。

为了提供这些安全服务，还应采用下述八种安全机制：

a. 加密；

b. 数字签名；

c. 访问控制；

d. 数据完整性；

e. 鉴别交换；

f. 业务流量填充；

g. 路由控制；

h. 公证。

这种体系结构还应具有如下的五种安全管理功能：

a. 鉴别管理；

b. 访问控制管理；

c. 密钥管理；

d. 安全恢复管理；

e. 安全审计跟踪管理。

根据军用计算机网络的安全要求，应在网络体系结构的层次中设置相应的安全，机制，提供所需的安全服务，并实施安全管理功能。

4.3.5.2 客户机服务器结构

应具有保护客户机/服务器结构中分离实体(如客户机、服务器)上的静止数据的安全机制。这种机制的目标如下：

a. 不应阻碍信息流，即不应阻碍移动用户传输敏感信息；

b. 待保护的资源(如文件)，必须在它建立时就能立刻对其实施保护，而不应由文件创建者采取保护措施；

c. 保护应作为该数据的整体组成部份，即不管文件位于何处或如何被传输，都应对该文件实施保护；

d. 应实施集中化安全管理，使安全管理人员能将所有站点置于其管理之下，包括对远地站点和工作站/服务器地异地环境实施管理；

e. 应不破坏原有网络结构和现有程序，而能与现有基础设施集成一起有效地运行；

f. 模块化，降低成本。

这种安全保护机制应具有下述基本功能：

a. 站点安全控制，如用户身份标识与确认，限制使用资源等；

b. 服务器安全控制，如用户线路拨入控制、互连服务器的网际访问控制、共享打印安全控制、限制使用资源等；

c. 传输和访问数据安全控制，即应具保密性、可用性、完整性保护；

d. 防网络病毒；

e. 数据可靠性保护，应具容错、备份和恢复；

f. 安全管理；

g. 安全审计。

5 详细要求

5.1 加密

5.1.1 概述

为达到保密性要求，在加密技术设计上应立足于对付攻击者，即使用拥有最高级别攻击能力，也不能破译密码；而在使用时，应尽量使攻击者只能得到最低级别的攻击能力，更难以破译密码。

5.1.2 密码体制

密码设计的核心是采用什么样的密码体制。在选择 DES 或 RSA 以及其他一些密码体制时，应根据具体的安全需求，遵循保密强度高、成本低、运行效率高、密钥管理方便和适用性好等原则。这些原则也可组合使用(见 GJB 1894)。

基于数据的互通和共享时的兼容性、便于联网、降低成本和推广使用的考虑，可以采用标准密码算法。如果采用公开的密码算法，则应加强密钥管理，对密钥严格保护。

5.1.3 密钥管理

为了加强密钥管理，在对称加密体制中应建立密钥的层次结构，用密钥来保护密钥。尤其要保证最高层(即一级)密钥(也叫主密钥)的安全并经常更换各层密钥，以增大破译难度。为了提高工作效率和数据的安全性，除一级密钥外，其他各层的密钥由密钥管理系统实行动态的自动维护，包括密钥的分配、更换、动态刷新、销毁等全过程。

5.1.4 密钥的随机性测定

为了不易破译，产生随机性密钥序列时，应对其不可预测性进行严格的测量以判定随机性。

当用统计方法检验密钥的随机性时，应使不随机的密钥序列出现的概率最小。

5.1.5 密钥分配

加密时，应按密钥分配协议和授权协议把密钥分配给用户。为了防止长时间使用密钥有可能被窃取或被泄露，应经常更换密钥且应尽量减少人的参与。

在网络加密通信时，密钥只应在一次通信内有效。

应根据网络的规模、拓扑结构、通信方式和不同的密码体制来确定密钥分配方式。

5.1.6 密钥存储

密钥应以密文方式存储在密码装置中，至少应存储主密钥。

对存储的密钥应具保护措施，如加、解密的操作口令应由密码操作人员掌握；密码装置应有掉电保护；拆开装置时会自动消失密钥；非法使用装置时会自动审计等。

5.1.7 密钥注入

采用键盘、软盘、磁卡、磁条、专用密钥枪等密钥注入方式时，注入应正确、可靠且应防止泄露。

密钥注入时应有保护措施，如注入过程应有一个封闭的工作环境；工作人员应可靠；注入前的操作口令应验证；注入的内容不应显示；对重要的密钥应多批次注入；一旦窃取者试图读出、分析注入的密钥时，密钥应自行销毁等。

5.1.8 密钥的更换

注入的密钥超过有效期应立即更换。更换时，必须清除原密钥的存储区或重写。更换密钥应按新密钥生效后，旧密钥才能废除的原则进行。对更换后的密钥应检查是否有错，存储位置是否正确，以便及时发现人为的错误和防止敌对势力的破坏。

检查的方法、过程应简便、有效，以保证工作效率和可靠性。

5.1.9 密钥的连通和分割

在网络环境下实现保密通信和资源共享，应具有密钥连通和分割的能力。互通能力可达到网络拓扑结构的地址极限，但为了安全性，应通过分割来限制连通范围，使保密通信和资源共享限制在若干封闭的小环境中。

5.1.10 数据库密钥管理

数据库加密时，密钥管理应适应密钥的时间不变性(随着存库数据的不变，其密钥也不应改变)和用户的不变性(不同用户访问同一数据时，所用密钥的加密密钥，即主密钥应相同且在用户密钥或口令等改变后，主密钥也应保持不变)。数据库容量大，需要加密的数据多，在难以做到对一个数据用一个密钥或用一个密钥来加密多个数据会增加不安全性而需采用密钥转换方法时，应保证安全性、转换速率以及操作管理方便、迅速等要求。

密钥管理中心应按加密强度产生相应的密钥，并由主密钥对所产生的密钥进行加密后保存起来，以便在建库时用同一主密钥解密，得到密钥以加密明文数据。当用户访问数据库时，

应核对用户识别符和用户密钥后才允许访问。采用集中或分由管理方式应视安全性、运行效率、方便管理、技术成熟程度等因素确定。

5.2 防电磁信息泄漏

5.2.1 概述

计算机系统工作时，对通过地线、电源线、信号线传播出去的(传导发射)和通过空间传播出去的(电磁辐射发射)泄漏信息，应采取防护措施，以防泄漏信息中的有用信息被接收、重现而造成失密。

防护对象应是一个系统，包括计算机、服务器、各种外围设备、通信网络设备、传输线和连接器等。

5.2.2 信息泄漏的分析和预测

应对计算机系统的泄漏情况进行分析、预测，包括发射源和发射部位的确定，发射源数学模型的建立及其发射特性的分析，以便了解发射场强度以及频谱范围、空间近远、场区衰减等影响。分析、预测应由实验系统的测试来进行比较验证。

5.2.3 泄漏信息的复现

为了了解信息泄漏后能否被接收并复现出原有的有用信息而造成失密，应对接收的泄漏信号进行识别、复原和提取等处理。

5.2.4 信息泄漏的综合防护

在了解信息泄漏的基础上应从材料、器件、电路、结构、工艺等各方面采取综合防护措施。应根据安全性要求和防护对象是改造、利用，还是新研制、生产等情况，确定采用包容或抑源或两者结合的设计方法。

5.2.5 信息泄漏的指标和测试

信息泄漏指标及其分级、指标测试的频率范围、测试室的消音和屏蔽性能、所用专门的测试设备以及测试规范等要求应由相应标准加以规定。

5.2.6 研制、生产信息泄漏防护产品的管理程序

研制、生产信息泄漏防护产品应贯彻科学的管理程序。一个较完整的管理程序应包括分析和预测、提出和实施设计、设计审查、阶段试验和鉴定试验等工作阶段。根据安全等级、研制生产周期、成本等要求，可以减少分析和预测、设计审查、阶段试验等工作阶段。用适应性(满足安全等级要求的程度)、人员(参与各工作阶段的人员数量、结构)、成本(各工作阶段的费用)、风险(返工、进度推迟的概率)、进度(研制、生产周期)和控制(组织管理)诸参数来评价管理程序。

为了定量测定，可按重要程度对诸参数给以不同的加权系数。首先是适应性的加权系数最大(因涉及影响安全等级要求实施的所有工作)；其次是成本和风险(因两者是紧密相关的，初始成本最低，其风险可能会最高；反之，初始成本高些，往往因风险小反而使总成本低)；其三是人员(人员主要指数量，而人员的才能已包含在适应性参数中)；加权系数最小的是进度和控制(因它们对工作成功的影响比其他参数要小)。研制、生产的低泄漏产品应由专门的机构测试、认证，合格者予以登记。

5.3 访问控制

5.3.1 概述

为了识别合法用户进入系统，应对每个用户规定唯一的标识符。还需对用户身份进行确认。采用的识别、确认的技术手段应不受泄露、丢失或被伪造的影响。

当使用口令实现确认时，口令必须可读、易记、难猜且应以密文存放。口令应正确分配给合法用户。通信双方应交换口令，相互鉴别身份。为了防止对口令的试探性探测或在口令传送过程中的被搭线窃听而后冒充合法者，应采用可变口令和经常更换口令等防护措施。

当使用用户拥有的磁条卡等信物实现确认时，应采用符合标准的推荐品，并应具有安全性能对付诸如冒充、猜测、伪造和穷举等攻击。对智能化、小型化的信物应优先采用。

当采用人体具有的生物特征或下意识动作留下的特征的技术手段实现确认时，应满足安全精度要求，做到既不能错误拒绝一个合法用户，也不能错误接受一个非法用户，且应力求减少确认系统的复杂性，降低成本和提高用户心理上的接受程度。

5.3.2 访问控制的策略、模型和机制

为了防止非法用户进入计算机系统和合法用户对系统资源的非法使用，应根据安全需求确立访问控制策略、模型与相应的机制。访问控制策略除识别与验证的一次控制外，还应包括授权访问方式的二次控制。为了精确描述策略，应使用数学模型并由相应机制的功能集合来实施。

5.3.3 自主访问控制和强制访问控制

视安全等级要求，系统应具有自主访问控制方式或强制访问控制方式或两者的结合。在自主访问控制时，用户应在被授权的情况下才能访问系统，且允许具有授权地位的用户根据自己的意愿将访问权授与其它用户，但必须经系统的访问控制机构检查、认可。在强制访问控制时，应对用户和被访问的系统资源都分配一种不能更改的唯一的安全属性，经系统的访问控制机构比较、认可，用户才能访问系统。

实施多级安全控制应根据最小特权原则，划分用户类别和对应的权限，以便信息的使用被限制在用户为了工作确需的范围内。还应对用户和系统资源都分配一个访问类，包括安全级(信息的密级、用户的许可级)和资源类别集。只有用户的安全级大于或等于信息的安全级，且用户必须具有包括该信息所有的访问类别时，才允许访问该信息。

访问控制必须遵循下述规则：

仅当用户的安全级不低于访问资源的安全级时，才允许该用户读取该资源；当用户安全级不高于访问资源的安全级时，才允许该用户对该资源进行写操作的访问控制。

5.3.4 多级访问控制

当更有效地实施两种以上的信息安全保护要求时(如保密性和完整性)，应采用多级访问控制结构。采用的机制应是：访问控制规则为多种规则组成的集合，且相应地存在多个访问控制判定。对多个判定产生的结果进行处理变成一种判定后执行访问控制。

5.3.5 访问控制机构的功能

系统的访问控制机构应具有的基本功能是：安全的精确性，即既能满足访问控制的安全要求，又不能因过分保护而拒绝合法的访问控制。此外，还应考虑共享的层次性(如共享原型，共享副本等)、经济性(机构尽可能简单)、校验的完备性(有效地检查每次访问操作的合法性)、分离性(访问所需条件不止一个)、可靠性(公用机构少，减少潜在的信息泄漏通路)以及心理可接受性(机构使用方便)等功能。

5.4 信息流控制

5.4.1 信息流控制机制

为了安全控制程序使用信息，防止授权的程序对未经授权的信息进行访问而造成信息泄露，作为访问控制的重要补充，系统还应具有信息流控制机制。

5.4.2 信息流控制规则

信息流控制规则应是：只允许安全级低的信息类流向安全级高的信息类或在同类间流动。对信息的状态(由实体值及其安全类来描述)，只允许信息从低安全类的实体流向高安全类的实体。

实施信息流控制机制既要保证安全性又要兼顾完备性，还需对三种类型的信息流通道(正规通道、存储通道、隐蔽通道)提供安全保护。

5.5 防火墙安全防护

对专用网络及其与公共网络的互连，在网络的边界上，应通过监测、过滤信息流，屏蔽网络内部结构，隔离应用服务类型以及安全审核、报警等技术手段，建立防火墙防卫系统。

5.6 审计控制

5.6.1 概述

安全审计过程应包括收集审计事件、产生审计记录。根据记录进行安全违反分析以及采取处理措施。审计范围应包括操作系统、数据库系统和应用程序。

5.6.2 操作系统的审计功能

操作系统审计的基本功能是：审计对象的选择；审计文件的定义与自动转换；文件系统完整性的定时检测；审计信息的格式和输出媒体；安全级阈值、报警阈值和逐出系统阈值的设置与选择；审计报告的提供以及审计日志管理等。报警类型应包括访问控制和权限的违章、隐蔽通道的使用情况、用户进入系统的登录失败以及病毒活动情况等。

5.6.3 数据库系统的审计功能

数据库系统审计的基本功能是：对应用程序或用户使用资源(包括数据)的情况进行记录和审查，以保证数据的安全。同时一旦出现问题，审计人员对审计的事件进行分析，查出原因，分清责任。为了支持数据库系统的审计，数据库管理系统必须有很高的可靠性和完整性。

5.6.4 应用程序的审计功能

应用程序审计的基本功能是：周期性地检测应用程序是否被修改和安全控制是否在发挥正确作用；判断程序、数据是否完整；依靠身份确认、终端保护等办法能否控制应用程序的运行，以及限制软件工具的授权使用范围等。

5.7 软件保护

软件保护的基本功能是：防止软件的非法复制和对软件的分析、修改。防非法复制应采用市场策略(价格低、销售服务优良)、法律策略(版权保护法)和技术策略进行综合保护。

软件加密应在某个载体(如软、硬盘、加密卡)上设置并保存密钥，且应在被保护的软件中嵌入一段判读程序识别密钥，以便启动执行被保护的软件，而拒绝执行软件复制品。所设置的密钥不应具有过高的反复制能力，以致不能使用要保护的软件。防非法分析、修改软件应使软件加密部份具有反动态跟踪和抗静态分析能力。

5.8 数据保护

数据保护的基本功能是完整性和可靠性。在出现偶然事故威胁和非法用户破坏数据时。完整性应包括语义完整性、结构完整性和并发控制。完整性还应包括数据本身的完全性和正确性，以防非法者在不破坏语义完整性和结构完整性的条件下，非法修改、删除数据。

数据完整性保护要求是：合法用户和用户权限正确才能查询、检索所需的数据及其相应的密级。且应能发现、阻止用户或有恶意的软件代码破坏数据。

对多用户访问数据应保证多事务同时运行时的数据一致性和正确性。一旦数据完整性受

损,应能尽快恢复。

系统应采取容错(如容错用户、容错计算机硬件、容错外存储、容错电源、容错网络等)、备份(软、硬件)和修理(自修理、热修理、冷修理)等措施,以防止系统故障和提高数据可靠性。

5.9 信息交换真实性和有效性的保护

为了证实信息交换过程的真实性和有效性,系统应具有身份鉴别、消息鉴别和第三方仲裁的功能。

身份鉴别要求相同于访问控制时的用户识别与确认。消息鉴别应包括消息内容、消息源点和消息时间性的鉴别。当信息收发双方对信息的内容及发送源点发生争执时应采用第三方仲裁机制。其功能是:

a. 防止收方否认已收到的真实信息或删改、伪造信息内容,谎称该信息内容是由发方发过来的;

b. 防止发方删改、伪造信息内容或抵赖发过的信息,并声称是收方伪造的信息;

c. 防止冒充发方或收方。

5.10 防病毒

对计算机病毒应采取预防、诊断、清除相结合的原则,采取增强用户自我保护意识、防病毒技术保护以及与其他信息安全技术相结合的综合治理措施。对病毒的防范不仅应指向单机而且应面向网络和应用平台;不仅应指向已知病毒,还应指向未知病毒;而且应面向表现形式和破坏性更隐蔽、更具有恶性和各种类别的病毒机制。

为保证反病毒的质量,应防止病毒的误报、错报、漏报,不能检测、检测出错,不能消除、消除出错,死机和系统崩溃;还应提供系统恢复手段和质量测试规范。

5.11 系统安全评估与形式化描述验证

5.11.1 安全评估

系统安全评估应包括:

a. 风险评估,侧重分析系统的脆弱性及其对系统构成的威胁,以确定什么风险是不可接受的;

b. 审计评估,侧重对安全审计记录进行评估;

c. 安全级别评估,侧重对能达到什么安全等级进行评估。

5.11.2 安全级别评估

安全级别评估首先应遵循主要面向操作系统安全和侧重保密特性的 GJB 2646。它提供的 27 条评估准则和四类、八个安全等级应作为研制,生产计算机安全系统的依据和用户采购、验收、使用安全系统的尺度。不同的安全等级,评估准则要求不同,等级越高,评估准则要求越多、越严(见表 2)。在面向网络、数据库应用环境,全面考虑保密性、可用性和完整性要求时,对网络、数据库的安全评估,在无国家军用标准和国家标准的情况下,可参考国外相关标准。

表 2

类别	评估准则	序号	安全等级							
			D	C1	C2	B1	B2	B3	A1	超 A1
安全策略	自主访问控制	1	√	√	—	—	√	—	—	—
	客体再用	2			√	—	—	—	—	—
	客体敏感标记	3				√	√	—	—	—
	标记的完整性	4				√	—	—	—	—
	标记信息的输出	5				√	—	—	—	—
	多级设备输出	6				√	—	—	—	—
	单级设备输出	7				√	—	—	—	—
	标记的硬拷贝输出	8				√	—	—	—	—
	强制访问控制	9				√	√	—	—	—
	主体安全标记	10					√	—	—	—
	设备标记	11					√	—	—	—
责任	标志与验证	12		√	√	√	—	—	—	—
	审计	13			√	√	√	√	—	—
	安全结构	14					√	√	—	—
保证	体系结构	15		√	√	√	—	—	—	—
	系统的完整性	16		√	—	—	—	—	—	—
	安全测试	17		√	√	√	√	√	√	√
	安全规范与验证	18				√	√	√	√	√
	隐蔽信道分析	19					√	√	√	—
	可信设施管理	20					√	√	—	—
	配置管理	21					√	—	√	—
	恢复	22						√	—	—
	可信分配	23							√	—
文件	安全性能用户指南	24	√	—	—	—	—	—	—	—
	安全设施、手册	25		√	√	√	√	√	—	—
	测试文件	26		√	—	—	√	—	—	—
	设计文件	27	√	—	√	√	√	√	√	—

注：表中空白为无要求；“√”相对低一等的增加或修改的要求；“—”为与低一等级的要求相同。

5.11.3 形式化描述与验证

要求 A 级安全级，应采用形式化描述与验证。即要用一种精确的、无二义性的以及对计算机处理可验证的方式来描述系统的安全需求，为此应建立一个能满足安全性要求的形式化描述。对系统进行可靠、精确的描述与验证；还应采用形式描述语言和相应的验证工具。

附加说明：

本标准由中国电子技术标准化研究所归口。

本标准由电子工业部第十五研究所负责起草。

本标准主要起草人：严育民、张佳昆、吕怀玉、卜宗义、陈炳从、向维良。

计划项目代号：B56002