军用信息系统信息安全要求研究*

赵志法
(总参第 61研究所，北京 100039)

摘 要：为了保障军用信息的机密性、完整性和可用性，文中从信息分类和安全管理、密码系统配置、信息处理公共安全基础设施、本地用户环境安全设施以及信息传输公共安全设施等五个方面研究并提出了对军用信息系统的信息安全要求。

关键词：军用信息系统；信息安全；安全要求
中图分类号：TP311 文献标识码：A 文章编号：0032-1289（2001）01-0031-05

The Study of the Information Security Reqttirement of the Military Information System

ZHAO Zhi-fa
(The 61rd Research Institute of PLA General Staff Headquarters, Beijing 100039, China)

Abstract: In order to guarantee the confidentiality, integrity and usability of military information, the paper, with regard to the information sorting, security management, cryptograph system allocation, information process public security infrastructure, local user environment facilities and information transmission public security facilities, discusses the information security requirements for the military information system.

Key words: military information system; information security; security requirement

为了保护我军信息、基于信息的过程和信息系统，对抗各种信息作战的攻击，保证军用信息的机密性、完整性和可用性，防止涉密军用信息的泄露、扩散、破坏和非授权访问，现根据我军作战对信息安全保密的总要求，提出军用信息系统信息安全要求，实现系统安全的互连、互通、互操作。

信息安全包括系统结构和密码系统的配置，也涉及在信息建模、人机界面、信息传送、信息处理、安全管理等方面的一系列安全服务，还包括防电磁泄露、物理安全、人事的和环境等方面的安全。本文重点涉及信息传送和信息处理公共安全基础设施。为了便于对信息安全要求的理解，下面先从信息系统的技术参考模型开始，然后讨论有关信息安全要求。

1 技术参考模型

为了叙述问题的需要，首先简述一下军用信息系统技术参考模型。技术参考模型是为理解信息系统中各种不同技术的分类以及彼此之间相互联系的一种模型，它是用来确定技术基础设施的目标框架和标准轮廓的文件，包括公共语汇，及一组信息系统共同采用的服务实体和接口。图 1是军用信息系统的技术参考模型，它由任务应用软件、应用支撑软件、应用平台实体和外部环境四个部分组成。其中任务应用软件和应用支撑软件又被称为应用软件实体。它通过一组应用编程接口（API）实现对应用平台实体的联接。特定

* 收稿日期：2000-09-07
作者简介：赵志法（1940-），男，高级工程师。

任务应用软件保障具体的末端用户需要,而应用支撑软件包含了可标准化的、跨越特定任务的公用应用,该公用集合是构成特定任务应用开发的基础。

应用编程接口(API)是指任务应用软件和应用支撑软件之间及应用支撑软件和应用平台实体之间的接口,规定这些接口主要是支持应用软件的可移植性,也支持系统和应用软件的可操作性。

应用平台实体是一些资源的集合,包括应用平台服务和跨领域服务。这些资源对那些将在其上执行应用软件的服务给予支持。应用平台概念并不意味对硬件平台强求某种具体的实施。

外部环境接口(EEI)是应用平台实体与外部环境之间的接口,信息经这个接口交换。外部环境接口是用来支持和应用软件的互操作,及用户和数据的可移值性,并配合应用编程接口实现应用软件的可移植性。

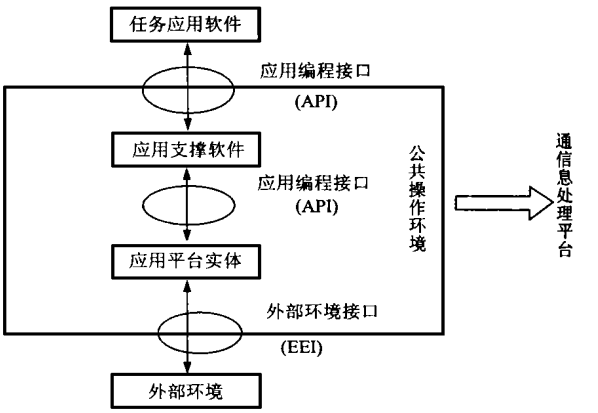

图 1 军用信息系统技术参考模型

应用支撑软件、应用平台实体、应用编程接口及外部环境接口一起构成了所谓的“公共操作环境”,也就是“通用信息处理平台”。

外部环境包括那些与应用平台交换信息的外部实体,如用户(人),信息交换实体(硬盘、软盘),以及网络实体(电话线路,分组交换设备,局域网,通信网)。

2 信息安全分类和安全管理类

军用信息系统对属于不同密级、不同军种或不同使用范围的信息访问应有必要的区别控制措施。

(1) 军用信息系统中涉及的信息按密级可分为四级:非密信息、秘密信息、机密信息和绝密信息。军用秘密级、机密级、绝密级信息在存储和传送过程中必须采用相应级的密码保护。

(2) 属于不同军兵种或使用范围(类别)的信息在安全管理上相互区分。

3 密码配置要求

(1) 密码技术在信息安全方面起着主导性和关键性的作用。因此,在提供信息安全服务时,应尽量选用密码为主的强安全机制,确保机制有效性。

(2) 密码系统的配置既要支持不同安全域的分割,也要支持各系统的安全互连互通互操作。

(3) 军用信息系统采用的所有密码方案及其使用部署必须经过主管部门的审查批准。

(4) 所有保密设备应具有良好的物理安全性保护措施,具备密钥紧急销毁、自检查等保护功能。

(5) 保密设备的设计要实现模块化、通用化、系列化。

(6) 所有安全保密设计必须兼顾安全保密性和系统整体效能,在时空和信道开销上不应造成系统整体效能的显著下降;终端密码处理的时间开销要满足系统总体要求,信道加密处理要求满足实时性要求。

(7) 所有保密设备应符合军用信息系统关于电磁兼容和电磁发射的标准要求。

(8) 所有保密设备应符合有关系统所在军用环境下可靠性、可维修性要求。

4 信息处理安全要求

(1) 通用信息处理平台和多级安全信息处理平台均应在适当层次上不同程度地支持军用信息的安全分

类和安全管理要求, 并应提供配置自主研制的不同密码系统的接口。

(2) 通用信息处理平台和多级安全信息处理平台上配置的自主研制的公共安全服务模块 (如数据加密、密钥管理、数据完整性、用户识别、鉴别、访问控制、抗抵赖等) 必须由可独立评价的硬/固/软件组成, 它们与系统的其他部件应有严格的分界, 有防篡改和防信息泄露的措施; 其安全性要经过论证, 并有必要的测试或评价。

5 通用信息处理平台安全要求

(1) 应符合 GJB2646- 96"军用计算机安全评估准则"中有关 C2级的有关要求。

(2) 应提供数据加密、数据完整性检验、数字签名、鉴别、访问控制等公共安全保密编程接口。

(3) 应提供自主研制的密钥分发、密钥管理的工具, 如鉴别/授权密钥分配服务器、公开密钥基础设施或安全证书管理系统。

(4) 自主研制的在网络中传送涉密信息的应用支撑软件 (如文电处理系统、文件传送系统等) 应满足以下要求: ① 根据需要对所传送的信息附加信息密级和使用范围的安全标记, 并对安全标记加密传送; ② 支持基于安全标记和用户身份 (或地址) 的访问控制; ③ 对不同密级/范围的信息采用不同的密码, 实施端到端加密保护; ④ 对重要应用应有数字签名; ⑤ 建立/拆除连接或传送信息之前/之后应有源鉴别和目的地鉴别; ⑥ 对传送的数据应提供完整性保护。

(5) 涉密数据库数据的保护应符合 GJBz20107- 93"军队涉密信息系统安全保密要求"中的有关要求。主体进入时有合法性验证, 特别信息应加密存储, 应有审计功能。

(6) 平台应提供安全 PC卡或用户身份卡。① 安全 PC卡应满足下列要求: 可控制系统启用; 内含强加密算法; 可支持 PC机实施用户识别和强鉴别; 可作为用户个人安全设备, 支持 PC机实施基于用户个人安全信息的数据加密、数字签名、访问控制、数据完整性等安全服务。② 用户身份卡 (IC智能卡) 应能满足下列要求: 芯片操作系统可扩展; 可装载加密算法, 支持分组加密、密码校验和介质访问控制 (MAC)、内外部鉴别、随机数生成、个人身份号 (PIN) 鉴别和管理等运算。

(7) 应具有一定的病毒或其他恶意程序的检测、防御、消除的软件。

6 多级安全信息处理平台要求

此类平台可处理多密级、多类别的信息, 在军用信息系统中可根据需要充当多级安全数据服务器、通信服务器或本地用户环境与外部连接的堡垒主机。

(1) 应符合 GJB2646- 96"军用计算机安全评估准则"中有关 B1级的有关要求。

(2) 应在 B1级操作系统提供的多级安全特性的基础上, 尽量配置与通用信息处理平台同样的自主研制的安全保密模块 (同上述 5节中的 (2) ~ (4) 的要求)。

7 本地用户环境共性安全要求

(1) 一个涉及多密级多类别信息、与外部有广泛信息交互的本地用户环境 (LSE), 应设置安全管理中心, 负责安全设备管理、授权管理、密钥管理、安全证书管理、审计、监控等。

(2) 每个本地用户环境 (LSE) 应通过安全设备 (如数据链路加密设备、安全路由器、加密机、防火墙或堡垒主机) 与外部网络相连, 防止非授权访问或信息泄露; 如果对外交互的是多密级信息, 应使用能隔离多级安全信息的设备与外部相连。

(3) 各类综合数据库、专业数据库、文件服务器中存储的信息,应对每个用户、席位或角色按照“知其所必需”(“需知”)和“最低特权”原则分配访问权限。用户及进程代理访问秘密级以上信息应经过授权。

8 信息传送系统安全要求

信息传送系统包括端系统(ES)和中继系统(RS)中的通信协议部分、本地通信系统(LCS)和通信网(CN)。

8.1 端系统和中继系统安全要求

信息传输端系统包括有线或无线的话音/数据/传真/图形/图象等用户终端设备,也包括信息处理平台中的通信部分。中继系统包括路由器、网关、中继设备、交换设备等。

(1) 信息处理平台中用以传输涉密信息的网络协议部分,必须根据需要在适当的层次中配置自主研制的密码机制,完成开放系统安全体系结构中必要的安全服务。

(2) 直接接入军用通信网的话音/数据/传真/图形/图像的保密终端应与军用通信网实现一体化安全设计,应满足下列安全要求:① 保密终端可实现多种密级的加密;② 所有传输信息的加密一般要实现多重密钥、一次一密加密要求;③ 可支持通信网密钥管理中心的管理和自动密钥分发;④ 应有可靠的密码同步和密码失步自动恢复能力;⑤ 保密端系统的启用要根据工作需要配置访问控制措施。

(3) 实现军用不同保密通信网之间安全互连的保密网关应具有下列要求:① 能对互连的两个网的通信协议和信令进行转换;② 能对经过密网关的信息进行密级核以,根据安全策略实行访问控制;③ 能对互连的两个网的加密协议进行转换(密码转换和密码同步等);④ 支持密钥管理和密钥自动分发;⑤ 实现相应的信息编码转换;⑥ 接口符合标准。

8.2 本地通信系统安全要求

(1) 无线传输的本地通信系统(LCS)应配置相应的无线保密设备,对所有无线传输的信息实施加密保护。同时应配置本地密钥管理中心和密钥分配中心,负责本地通信系统的密钥的分发和管理,并负责与本地通信系统外部网络(通过安全的连网设备)的密钥沟通。

(2) 采用跳频技术的无线传输应尽量采取密码技术进行控制。

8.3 通信网安全要求

军用通信网主要是指军用电话交换网、军用数据网、军用数字电话保密网、高速光缆网、区域综合通信系统、集团军野战网等,其他军用通信网是指各军兵种专用网等战时可能接入的军用通信网。

(1) 军用网络传输一般安全要求为:① 所有传输涉密信息的通信网均需采用端端加密,并根据需要采用逐链加密的措施,确保涉密信息在传输过程中在保密装置以外一律不以明文形式出现,保证传输信息的保密性。② 所有传输涉密信息的通信网应具有人工与自动相结合的密钥管理和分配措施。③ 所有传输涉密信息的通信网应具有自动的安全设备管理、控制和检测功能,确保军用通信的准确、迅速、保密和不间断,保证网络的可用性。④ 经网络传输的涉密数据应具有完整性保护措施,对抗传输过程中对信息的篡改、删除、插入、重放等攻击。⑤ 不同军用通信网互连互通要配置相应的保密网关,实现密码协议和密钥的转换。⑥ 涉密网与公众网相连要有必要的安全措施,防止任意从公众网进入军用网。

(2) 各类用户接入接口安全要求

① 需直接接入通信网的保密的话音/数据/传真/图形/图像/会议电视等用户业务,不论是无线接入还是有线接入,保密终端、接入交换机、节点交换机、网管设备等必须在以下几个方面支持相匹配的安全接口:通信安全协议;密钥分配协议;密钥管理/安全管理协议。

(3) 军用通信网的安全管理要求

① 各军用通信网应在现有的密钥管理中心的基础上,根据需要在重要的本地用户环境 (LSE)所挂接的骨干交换节点、接入节点设置区域级、地区 (或军)级、设备 (或师)级网络安全管理中心,配置相应的安全管理设备,以完成下列功能要求: 网络访问控制; 网络安全设备管理; 安全审计、监控和信息战应急处理。本地用户环境 (LSE)的本地安全管理分中心接受网络管理中心的管理。② 多密级安全通信要求应遵循统一的安全策略,不同密级通信要受限制,低密级用户不能接受高密级的信息,高密级用户不能向低密级用户发送高安全级信息。③ 跨网络通信的网络安全管理要求: 由网络安全管理中心配置两网络互通的安全策略 (同密级、不同密级、多安全级互通策略),以及保密网关的安全参数。由两网络的密钥管理中心 (KMC) 共同完成对密网关的密钥管理 (密钥审计管理、更换和销毁管理等),两网的密钥管理中心 (KMC) 在上一级别的密钥管理中心 (KMC) 的支持下相互协商,要有严格的鉴别和安全保密措施。

9 结束语

本文旨在从军用信息系统信息安全顶层设计考虑出发,从系统整体的观点研究提出了军用信息系统的信息安全保密要求。在未来高技术战争中信息战往往成为首战的情况下,军用信息系统的信息安全就显得格外重要。但对此往往缺乏顶层设计。本文的目的是抛砖引玉。

参考文献:

[1] GJBz20107— 93, 军队涉密信息系统安全保密要求 [S].
[2] GJB 1894— 94, 自动化指挥系统数据加密要求 [S].
[3] GJB 2646— 96, 军用计算机安全评估准则 [S].
[4] GJB 2824— 97, 军用数据安全要求 [S].

(上接第 17页)

生产的空白,代表了我国短波同频多信道接收机最新的发展方向。经过不断地改进和完善,目前在短波通信的各种测向系统中已取代了国外进口产品,为短波通信事业的发展起到了积极的作用。

参考文献:

[1] 刘松强. 数字信号处理系统及其应用 [M]. 北京: 清华大学出版社, 1996.
[2] 陈世伟. 锁相原理及应用 [M]. 北京: 兵器工业出版社, 1990.
[3] Nicholas H TⅢ, Samueli H. An analysis of the output spectoum of direct digital frequency synthesizers in the presence of phase-accumulator truncation [A]. IEEE 41st Annual Frequency Control Symposium Digest of Papers [C]. IEEE Publication, 1987. 495— 502.
[4] 沈兰荪. 智能仪器与信号处理技术 [M]. 北京: 科学出版社, 1990.
[5] Yuen C K, Beauchamp K G, Robinson G P S. Microprocessor systems and their application to signal processing [M]. USA: Academic Press, 1982.