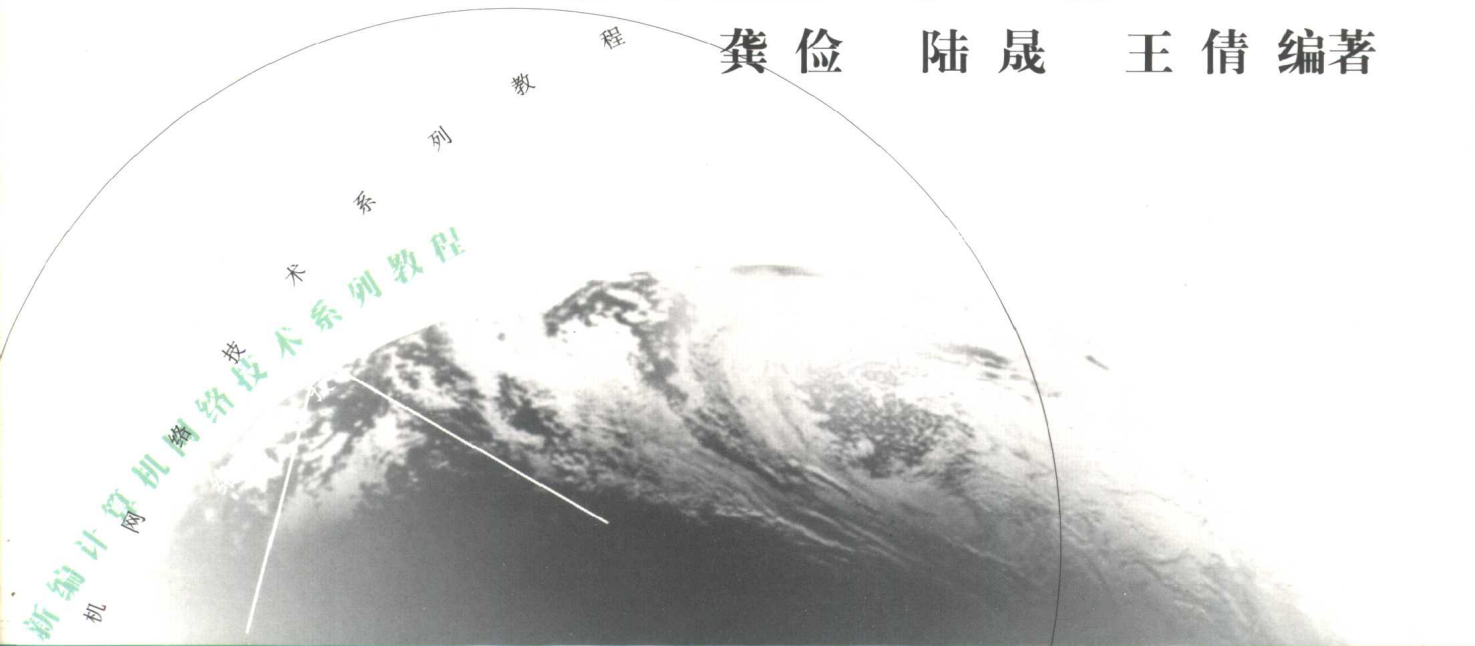
新编计算机网络技术系列教程

计算机网络安全导论

龚俭　陆晟　王倩　编著



新编计算机网络技术系列教程

新编计算机网络技术系列教程

东南大学出版社

★ 新编计算机网络技术系列教程

计算机网络安全导论

龚俭　陆晟　王倩　编著

东南大学出版社
·南京·

内容提要

本书介绍了计算机网络安全的基本知识和常用的安全技术，包括对称与非对称密钥数据加密技术、密钥管理技术、信息摘录技术、数据鉴别技术、数字签名技术及其应用、访问控制技术和防火墙技术，以及计算机网络安全监测技术的基本内容。本书还介绍了计算机网络安全管理方面的基本内容和 Internet 网络基础设施安全的一些重点发展领域的现状，覆盖了 IEFT 安全领域的主要工作。通过这些内容，可使读者掌握计算机网络（特别是计算机互联网络）安全的基本概念，了解设计和维护安全的网络及其应用系统的基本手段和常用方法。

本书可用作计算机专业本科生或研究生的教材，也可作为相关领域技术人员的参考书。

图书在版编目(CIP)数据

计算机网络安全导论/龚俭编著．—南京：东南大学出版社，2000.8

新编计算机网络技术系列教程

ISBN 7-81050-648-X

Ⅰ.计… Ⅱ.龚… Ⅲ.计算机网络-安全技术-教材 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2000)第 42354 号

TS461/15

东南大学出版社出版发行

（南京四牌楼 2 号 邮编 210096）

出版人：宋增民

江苏省新华书店经销 溧阳市印刷厂印刷

开本：787mm×1029mm 1/16 印张 19 字数：512 千字

2000 年 8 月第 1 版 2000 年 8 月第 1 次印刷

印数：3000 册 定价：35.00 元

前　言

计算机网络的安全问题随着 Internet 的发展而越来越被人们所重视。在社会日益信息化的今天，信息网络的大规模全球互联趋势，以及人们的社会与经济活动对计算机网络依赖性的与日俱增，使得计算机网络的安全性成为信息化建设的一个核心问题。Internet 的最大优势之一是它的自由性，没有严格的管理体制来约束网络中的应用；但是从安全的角度看，这同时又是 Internet 的最大缺点，过分自由的网络用户和网络应用给 Internet 带来严重的安全隐患。早期的 Internet 节点(site)主要是教育科研机构或政府部门，这些节点的主要安全考虑是防止计算机黑客的入侵，因此各自设置自己的安全政策和安全措施，不存在全局的安全体系结构。随着 Internet 的商业化，越来越多的企业进入网络并在网上开展业务，从而使得与交互有关的安全问题日益突出，例如用户的身份鉴别，敏感信息的传输保护，交互的无否认等。此外，日益开放的系统和网络结构也向潜在的黑客提供了更多的信息，因此对于在 Internet 中建立全局性的网络安全体系结构的需求日益迫切。

进入 20 世纪 90 年代以来，Internet 发展的最大问题是规模和安全，且两者是相互关联的。Internet 的安全问题集中在以下四个方面：

(1) 端－端的安全问题，主要指用户(包括代理)之间的加密、鉴别和数据完整性的维护；

(2) 端系统的安全问题，主要涉及防火墙技术；

(3) 安全服务质量问题，主要指如何保证合法用户的带宽，防止用户非法占用带宽；

(4) 安全的网络基础设施，主要涉及路由器、DNS 服务器，以及网络控制信息和管理信息的安全问题。

从上可以看出，把握用户的行为，防止非法侵入网络和非法访问资源是当前网络安全的主要问题。

计算机网络的安全控制通常基于安全域的概念，它通常对应一个组织机构(如一个公司或学校)，以及一个相对独立的网络。各个安全域内的网络和信息系统使用自己的安全政策、安全机制和安全系统。因此，在互联环境中的网络安全控制本质上是各自为战，在 Internet 中也是如此。

然而，1988 年底 Internet 蠕虫事件发生后，为了应付 Internet 出现的紧急安全问题，美国国家标准及技术学会(NIST)发起建立了 Internet 的计算机紧急响应工作组 (Computer Emergency Response Team － CERT)，后改称 CERT/CC(设在美国卡内基梅隆大学的软件工程学院)，Internet 中的一些重要的网络也相应成立了类似的组织，以应付网络中出现的突发事件，维护网络的安全。

目前 IETF 在网络安全领域设立了十多个工作小组，组织研究当前 Interent 中的安全热点问题，并制定相应的标准，现有的工作组包括：

(1) 防火墙鉴别技术工作组(aft)；

(2) 通用鉴别技术工作组(cat)；

(3) DNS 安全工作组(dnssec)；

(4) IP 安全协议工作组(ipsec);
(5) 入侵检测交换格式工作组(idwg);
(6) 一次性口令鉴别工作组(otp);
(7) 公开密钥基础结构(X.509)工作组 (pkix);
(8) S/MIME 邮件安全工作组(smime);
(9) 安全 Shell 工作组(secsh);
(10) 简单公开密钥基础结构工作组(spki);
(11) 运输层安全工作组(tls);
(12) Web 的事务安全工作组(wts)。

端 - 端的安全问题包含了数据加密、鉴别、完整性维护等方面,这里的端系统指的是直接参与通信活动的主机或是它的代理(如防火墙)。数据加密可防止网络中存储和传输的数据内容被泄露,采用的方法包括通信双方使用相同密钥的对称密钥体制(如 DES、IDEA 等方法),也可以是通信双方使用不同密钥的公开密钥体制(如 RSA、离散对数方法等)。然而,数据安全是一个敏感问题,在绝大多数国家都存在控制和应用上的矛盾。例如,大部分数据加密技术涉及知识产权问题,因此推广使用有一定的难度;另外,大多数 Internet 成员国对数据加密的使用有限制,这也为构造整个 Internet 的安全体系结构带来人为的障碍。Internet 的最大成员美国的政策矛盾就很典型,一方面要求大力推行国际化的电子商贸,要求免除这方面的关税;另一方面又禁止数据加密技术出口,从而又束缚了美国企业在开展国际化电子商贸方面的手脚。

鉴别技术用以验证用户的身份,传统的方法是使用用户标识和口令,还可使用基于各种信息摘录(message digest)算法,如 MD5 的数字签名技术,以提高可靠性。数据完整性技术用以保护网络中的数据不被非法修改,通常使用数字签名技术来实现。

与 Internet 上密钥管理有关的全局标识体系尚未完成。X.500 具有良好的技术特性,这对于在 Internet 内建立全局标识体系较为理想。但是由于它进入 Internet 的速度太慢,至今尚未形成全局的管理体系,如对 DN 的定义和分配,因此无法进入实用阶段。PKIX 工作组正在为之奋斗,他们研究使用 X.509 支持 Internet 全局的公开密钥管理的方法,并已提出了一系列的标准草案。SPKI 工作组 1997 年初开始正在进行一项类似的工作,开发一个称为简单公开密钥基础结构的新标准,但其基本思想与 X.509 大不相同。

防火墙是对在 Internet 中传输的数据的过滤功能,分为安全通道(通常为加密的 TCP 连接)、IP 级防火墙和应用级防火墙三类,用于对 Internet 的某一部分进行安全隔离。目前 Internet 中对防火墙有两种看法:一类意见认为防火墙是一个强有力的概念,它将安全的管理、配置和实施集中到了一点;另一类意见认为防火墙提供了一种虚假的安全感,使内部人员放松了警惕,而大部分计算机犯罪是由内部人员所为。IETF 的 AFT 工作组为防火墙环境下的网络应用服务开发了一个安全鉴别协议,使报文在穿越各个 IP 防火墙时能不断地得到鉴别,所采用的技术方案基于著名的 SOCKS 系统(RFC 1928)。

良好的网络安全是需要付出高代价的,这不仅在增加物理设备或软件系统方面,更重要的是它增加了网络管理的复杂程度,并增加了对网络管理人员的知识和技能的要求。专家认为,Internet 的最大安全挑战是如何保持比黑客领先一步,因为目前发现系统安全漏洞的速度几乎与网络安全设施的开发一样快。据一些美国商业咨询公司估计,未来几年中,Internet 上的电子贸易营业额将会迅速上升,但是若不能较好地解决网络安全问题(包括在技术和立法两方

面),这个巨大的商业机会很可能会夭折。然而,就像飞机与火车的安全性比较一样有趣,据"Telecommunication"1996年的统计研究,移动电话系统因欺诈而产生的损失与营业收入的比例是29.74美元对1500美元;而Internet上这个比例为1.5美元对1500美元。这似乎也从一个侧面说明目前的Internet网比电话网更安全。

本书侧重计算机网络安全而不是计算机系统安全的讨论。研读本书,可使读者掌握计算机网络安全的基本概念,并了解设计和维护网络及其应用系统安全的基本手段和常用方法。本书原是为满足东南大学计算机系硕士研究生专业课的需要而编写的讲义,经过几轮使用后,在内容上进行了一些调整。本书的重点是面向计算机互联网络的网络安全技术,并且作为前提,介绍了一些应用密码学的相关内容。在形式上比较多地介绍了方法,突出了应用的需要,避开了许多原理性的介绍和一些基本数学理论内容,力争反映网络安全技术(尤其是Internet安全技术)的最新发展,主要是想满足构造安全的网络应用系统的需要。

全书共分九章。第一章从体系结构的角度介绍了计算机网络安全的基本概念,并对计算机单机系统的安全问题作了简单介绍,因为计算机网络安全的许多问题是从单机的安全问题发展出来的。第二章介绍数据加密技术,在介绍了一些基本概念之后给出了几种在Internet中常见的数据加密技术方法。第三章讨论密钥管理方法,重点介绍了与当前网络应用的发展密切相关的公开密钥管理体制。第四章介绍数据完整性保护技术,主要是与鉴别有关的各种技术以及它们的应用。第五章介绍了一些在Internet中常用的鉴别应用技术。第六章介绍一些基于数据加密技术的网络安全应用,包括PGP等在Internet中比较流行的典型应用系统。第七章讨论单机和网络的访问控制问题,重点介绍各种防火墙技术。第八章以Internet的安全为背景,重点介绍了网络安全监测技术的主要内容和最新发展。第九章以IETF安全领域一些工作组的工作内容为背景介绍了网络基础设施安全方面的一些新进展,这些内容已经逐渐在Internet中得到应用。计算机病毒的防范从技术的角度看应属于计算机单机系统的安全问题,它们在网络上的传播并没有利于特别的网络安全漏洞,而是使用者的疏忽和无知,因此有关计算机病毒的问题并没有在本书中讨论。

本书的前五章由龚俭、王倩编写,第六章由陆晟编写,第七章由龚俭、王倩编写,第八章由陆晟、王倩、龚俭编写,第九章由陆晟、龚俭编写。另外,第三章中有关PKI的介绍引用了刘建航和王礼强的硕士论文内容。

本书可用作计算机专业本科生或研究生的教材,也可作为相关领域技术人员的参考书。

希望本书的出版对读者,尤其是高年级本科生和硕士研究生学习、掌握网络安全技术有所帮助。书中如有错误和疏漏,敬请各位同仁批评指正,并提出宝贵意见,以便再版时改进。

联系邮址:jgong@njnet.edu.cn

编 者

2000年5月

目　录

第一章　网络安全的体系结构

1.1　计算机安全

计算机系统是计算机网络的基本元素，没有计算机系统的安全，自然也就没有计算机网络的安全。当然反之不然，因为连接计算机的信道是新增加的不安全因素。由于本书的重点是讨论计算机网络的安全，所以对于计算机系统的安全问题只作概念性的介绍，有兴趣的读者可以参阅有关的参考文献。

1.1.1　计算机系统的安全问题

自从计算机诞生以来，它一直与国家的重要领域，如国防、金融等部门有着密切的联系，因此计算机系统的安全问题由来已久，已经得到了大量的研究和较充分的认识。在国防安全、经济建设和社会生活的各个方面，计算机正在发挥日益重要的作用，并越来越多地取代原来需要手工进行的工作，人类对计算机的依赖越来越强烈。由于计算机处理并存储仅供授权者访问的敏感数据（即那些数据不像公开数据那样可供任何人进行访问），人们需要保护这些数据不被泄露或破坏，从而需要研究计算机系统中可能导致安全问题的薄弱环节，即系统的脆弱性。在长期的应用过程中，人们发现到目前为止的通用计算机系统仍然是不完善的，还存在着多种安全隐患，使计算机系统有意或无意地受到损害。这些安全隐患包括：

（1）存储数据的密度极高，因此磁介质的损坏和丢失都会造成大量数据的损失。

（2）数据的传送和使用过程中系统的电磁辐射会造成信息泄漏。另外储存媒体的许多操作是逻辑的，使得被丢弃的信息往往还实际存在在系统中。若不进行物理清除，就存在被非法访问的可能，如许多系统可以作 Undelete 操作和内存镜像（dump）分析。

（3）电子信息可以很容易地被拷贝而不留下任何痕迹；另外由于系统的本地或网络访问控制可能存在漏洞，使数据被非法访问。

（4）信息具有聚生性，当信息以分离的小块形式出现时，其价值可能不大，但当大量相关信息聚集在一起时，则可能会产生有意义的结果（如破译）。因此通过对系统的长期观察或零星数据的收集，有可能获取系统的信息。例如翻有关部门的垃圾桶就是计算机黑客收集系统信息的常用手法。

（5）由于计算机的使用要求一定的知识和技能，因此非专业人员不容易发现或觉察到围绕计算机的渎职和犯罪行为。

系统安全的主要威胁可能是通过设备故障或人为操作过程无意中引入的，也可能来自于自然灾害或人为的攻击。

系统无意产生的威胁具有很大的偶然性，通常需要采用备份或双重操作等方式进行预防。常见的威胁包括：

（1）由硬件故障引起的设备机能失常，例如由于使用寿命或环境因素而引起的硬盘故障往往导致整个系统或数据文件的丢失；

(2) 由操作失误而引起的人为错误,如按错开关、敲错命令、用错外设或存储介质等;

(3) 由于系统或应用软件中存在的 bug 而引起的软件故障,导致系统的异常操作甚至破坏;

(4) 由于电源或空调等环境故障而引起的设备故障。

自然灾害的威胁主要表现在如火灾、水灾、地震、化学污染、外力破坏(例如滑坡或地陷)等引起的设备损坏。这就要求机房的建设要满足一定的条件,尤其对于大型机系统。

人为攻击对计算机系统产生的威胁分为主动和被动两种类型。被动类型的攻击主要表现为信息的窃取,例如攻击方出于政治、军事、经济等方面的原因,希望获取敌方的信息,窃取方式以电磁窃听为多;或者商业领域的竞争对象为竞争的需要而设法窃取对方的商业秘密,窃取的方式也有多种。主动攻击主要表现为对数据的篡改,或对资源的非法使用。例如用户冒充他人的名义使用计算机资源;系统内部人员出于报复的目的而对系统进行恶意修改或设置逻辑炸弹;系统内部人员或外部人员利用计算机进行犯罪,以经济原因为主,多出现在金融系统。

1.1.2 计算机系统的安全目标

计算机系统的基本安全目标是保持系统能够正常工作,即系统能够按预期方式工作,完成预定的任务,并给出正确的结果。具体的安全目标分为以下几方面。

1) 安全性

(1) 内部与外部安全

计算机系统的安全性分内部安全和外部安全两方面。系统的内部安全是系统的固有特性,在系统的软、硬件和外设中体现。包括系统中的安全设备,如加密部件、防止电磁辐射的屏蔽罩等;软件中设置的安全功能,如访问控制功能、口令鉴别功能等。

外部安全涉及系统的维护和使用,包括:

① 物理安全:指对环境的保护,按照系统所担负的处理任务,可包括电源、空调、防尘、防止鼠害、防震、防污染以及安全警卫等方面的内容。

② 人事安全:指有关人员的可靠性,包括操作人员、维护人员、管理人员、勤杂人员、警卫人员等。

③ 过程安全:指操作过程的可靠性,包括有关人员的职责划分,操作规程制定和执行控制等方面。

(2) 可信系统

可信系统是指那些确认没有安全缺陷的计算机系统,这些系统的安全依赖于对它们的正确操作。系统的可信程度是相对的,如果对系统的某些方面特别设置安全措施,负责系统安全,则对于这些方面来说系统是可信的。非可信的一般计算机系统称为良性系统,它们存在安全缺陷,可能会对系统造成无意的破坏。例如,如果系统没有自动的硬盘镜像备份功能,则突然发生的硬盘故障就会导致数据丢失,即使有定期的备份也不行。对于像处理信用卡交易的银行计算机系统来说,这样的良性系统就不能满足要求。主动出现不良行为的计算机系统称为恶性系统,例如扩散计算机病毒,或通过网络向其他系统发起攻击。

为了方便讨论,可以将系统抽象为有关的计算机及其通信环境的总和,因此系统边界定义了需要安全保护的范围。由内部安全措施构成的安全边界称为安全防线。

(3) 系统安全性的维护方法

系统安全性的维护可从用户的进入、使用和事后检查这三个方面来进行。

对用户进入系统的控制是通过标识与鉴别来实施的。标识是识别用户的手段，而把用户与他的标识符相结合的过程则称为鉴别(或称为身份认证，本书对这两个术语不加区分地使用)。为了实现可靠的鉴别，鉴别信息必须通过一种系统与用户都不能伪造(或冒充)的途径来交换。

对用户使用系统的控制是通过访问控制来实施的，分为三方面的内容：

① 授权：决定哪个主体有资格访问哪个客体；

② 确定访问权限：限定这个主体对指定客体的访问方式；

③ 实施访问控制：具体实现访问控制。

审计跟踪实现对用户使用系统情况的追踪了解。它要求在一个计算机系统中对使用了何种系统资源、使用时间、如何使用、以及由哪个用户使用等信息提供一个完备的记录，以备非法事件发生后能够有效地进行追查。

2) 完整性

完整性体现了系统的可信度，分为软件完整性和数据完整性两方面。

(1) 软件完整性

软件的完整性是指软件的标称功能与实际功能的一致性。系统硬件由于采用了标准的单元，因而通常是可信的；而软件的灵活易变性给系统安全带来隐患。软件完整性的威胁来自设计的缺陷、实现中的 bug、设计人员或使用人员故意设置的特洛伊木马或逻辑炸弹、计算机病毒等。软件完整性的程度依赖于事前的正确性验证或可靠性测试，以及事后的安全维护。

(2) 数据完整性

数据的完整性是指数据的标称内容与实际内容的一致性，即要求存储在计算机系统中或在计算机系统之间传输的数据能够不受非法删改或意外事件的破坏，从而保持数据整体的完整。数据损坏的原因包括：系统的误动作，如系统软件故障、存储或传输过程中的外界干扰等；应用程序的错误；存储介质的损坏；人为的破坏等多个方面。

3) 保密性

系统中不能公开的数据称为敏感数据，这些数据可能涉及国家机密、商业秘密或个人隐私，因此要利用密码术对信息进行加密处理，防止信息内容非法泄漏。另外，系统的一些配置数据也可能是敏感数据，如用户的口令，也需要保密存放。数据的加密对于数据存储和数据传输都可能是必要的。

1.1.3 计算机系统安全的主要内容

计算机信息系统的安全可分为实体安全、运行安全和信息安全等三个方面，其中实体安全包括环境安全、设备安全和媒体安全等三个方面；运行安全包括风险分析、审计跟踪、备份与恢复、应急技术等四个方面；信息安全包括操作系统安全、数据库安全、网络安全、计算机病毒防护、访问控制、数据加密与鉴别等七个方面。在这里，计算机信息系统是指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。

1) 实体安全

实体安全研究和提供保护计算机设备、设施(含网络)以及其他媒体免遭地震、水灾、火灾、

有害气体和其他环境事故(如电磁污染等)破坏的措施和过程。

(1) 环境安全

环境安全提供对计算机信息系统所在环境的安全保护,主要包括受灾防护和区域防护。受灾防护提供受灾报警、受灾保护和受灾恢复等功能,其目的是保护计算机信息系统免受水、火、有害气体、地震、雷击和静电的危害。具体的内容包括:灾难发生前,对灾难的检测和报警的方法;灾难发生时,对正遭受破坏的计算机信息系统,采取紧急措施,进行现场实时保护的方法;以及灾难发生后,对已经遭受某种破坏的计算机信息系统进行灾后恢复的方法。

区域防护对特定区域提供某种形式的保护和隔离。具体包括:静止区域保护,如研究通过电子手段(如红外扫描等)或其他手段对特定区域(如机房等)进行某种形式保护(如监测和控制等)的方法;活动区域保护,如研究对活动区域(如活动机房等)进行某种形式保护的方法。出入控制主要用于阻止非授权用户进入机构或组织,一般是以电子技术、生物技术或者电子技术与生物技术结合阻止非授权用户进入。例如物理通道的控制技术,利用重量检查控制通过通道的人数;门的控制技术,双重门、陷阱门等。

(2) 设备安全

设备安全应提供对计算机信息系统设备进行安全保护的机制,主要涉及以下几方面的内容:

① 设备的防盗:提供对计算机信息系统设备的防盗保护,例如将一定的防盗手段(如移动报警器、数字探测报警和部件上锁)用于计算机信息系统设备和部件,以提高计算机信息系统设备和部件的安全性。

② 设备的防毁:提供对计算机信息系统设备的防毁保护,包括对抗自然力的破坏,使用一定的防毁措施(如接地保护等)保护计算机信息系统设备和部件;对抗人为的破坏,使用一定的防毁措施(如防砸外壳)保护计算机信息系统设备和部件。

③ 防止电磁信息泄漏:研究开发防止计算机信息系统中的电磁信息泄漏的技术和设备,从而提高系统内敏感信息的安全性;研究干扰泄漏的电磁信息的方法(如利用电磁干扰对泄漏的电磁信息进行置乱);研究吸收泄漏的电磁信息的方法(如通过特殊材料/涂料等吸收泄漏的电磁信息)等。

④ 防止线路截获:研究防止对计算机信息系统通信线路的截获和外界对计算机信息系统通信线路干扰的方法,具体的技术可包括预防线路截获,使线路截获设备无法正常工作;探测线路截获,发现线路截获并报警;线路截获动作的定位,发现线路截获设备工作的位置;对抗线路截获,阻止线路截获设备的有效使用。

⑤ 抗电磁干扰:用于防止对计算机信息系统的电磁干扰,从而保护系统内部的信息,包括对抗外界对系统的电磁干扰和消除来自系统内部的电磁干扰。

⑥ 电源保护:为计算机信息系统设备的可靠运行提供能源保障,包括:对工作电源的工作连续性的保护,如不间断电源;对工作电源的工作稳定性的保护,如稳压电源。

(3) 媒体安全

媒体安全分为媒体数据保护和媒体本身的安全保护两方面。媒体本身的安全主要是对媒体的安全保管,目的是保护存储在媒体上的信息,包括媒体的防盗,媒体的防毁(如防霉和防砸等)。媒体数据的安全包括媒体数据的防盗,如防止媒体数据被非法拷贝;媒体数据的销毁,包括媒体的物理销毁(如媒体粉碎等)和媒体数据的彻底销毁(如消磁等),防止媒体数据删除或

销毁后被他人恢复而泄露信息，以及媒体数据的防毁，防止意外或故意的破坏所导致的媒体数据丢失。

2) 运行安全

运行安全研究为保障系统功能的安全实现所应提供的安全措施（如风险分析、审计跟踪、备份与恢复、应急技术等），以保护信息处理过程的安全。

(1) 风险分析

计算机信息系统（人工或自动）的风险分析分成三个层次。首先是对系统进行静态的分析（尤指系统设计前和系统运行前的风险分析），旨在发现系统的潜在安全隐患；其次是对系统进行动态的分析，即在系统运行过程中测试，跟踪并记录其活动，旨在发现系统运行期的安全漏洞；最后是系统运行后的分析，并提供相应的系统脆弱性分析报告。

风险分析是计算机信息系统的安全需求分析，通过它可明确风险的类型及其影响范围，例如确认数据存放在计算机系统中是否会有泄露的可能（有哪些用户可能接触数据），这些数据的泄露所造成的危害是否是可以承受的。这样系统可针对可能的风险选择适当的防护措施。例如，如果数据泄露所产生的危害是可承受的，则可采用一般的访问控制和加密存放方法；如果产生的危害是不可承受的，则应该采取进一步的防范措施，如对于计算机系统的电磁屏蔽措施，以及对用户接触计算机的范围进行限制等等。

风险评估通常基于一些系统模型和数学方法，如排列方法、特征记分法、Delphi 顾问团（Delphi Panels）法等。

(2) 审计跟踪

通过保存审计记录和维护详尽的审计日志可实现对计算机信息系统进行人工或自动的审计跟踪。审计跟踪技术可实现记录和跟踪各种系统状态的变化，如提供对系统故意入侵行为的记录和对系统安全功能违反的记录；实现对各种安全事故的定位，如监控和捕捉各种安全事件。

(3) 备份与恢复

系统设备和系统数据的备份与恢复包括联机的高速度、大容量自动的数据存储，备份和恢复功能；脱机的数据存储，备份和恢复功能，如通过专用安全记录存储设施对系统内的主要数据进行备份；以及对系统设备的备份。

(4) 应急技术

应急技术提供紧急事件或安全事故发生时，保障计算机信息系统继续运行或紧急恢复所需要的功能，例如应急计划辅助软件和应急设施等。

应急计划辅助软件为制订应急计划提供计算机辅助支持，例如进行紧急事件或安全事故发生时的影响分析，提供应急计划的测试与完善等。

应急设施提供紧急事件或安全事故发生时，计算机信息系统实施应急计划所需要的支持，包括实时应急设施、非实时应急设施等。这些设施的区别主要表现在对紧急事件发生时的响应时间长短上。

3) 信息安全

信息安全研究防止信息内容被故意地或偶然地非授权泄露、更改、破坏，或使信息被非法地系统辨识、控制的各种机制，它可确保信息的完整性、保密性、可用性和可控性。

(1) 操作系统安全