计算机及网络安全与防护基础

宁 章 编著

北京航空航天大学出版社

计算机及网络安全与防护基础

宁 章 编著

北京航空航天大学出版社

内 容 简 介

计算机及网络的飞速发展极大地促进了社会的繁荣和进步，但同时也带来了信息安全的问题。本书分12章介绍了计算机及网络安全的重要性、计算机及网络安全的概况和分层防护的技术措施等。本书可供高等院校涉及计算机及网络应用的各专业（理工类各专业，文科类如商业、经济、金融、法律等专业）学生作教材用，也可供机关、院校、部队、研究单位从事计算机及网络管理、开发、应用等工作的师生、工程技术人员和管理人员参考。

图书在版编目（CIP）数据

计算机及网络安全与防护基础/宁章编著．—北京：北京航空航天大学出版社，1999.10

ISBN 7-81012-894-9

Ⅰ.计… Ⅱ.宁… Ⅲ.电子计算机网络-安全技术 Ⅳ.TP309

中国版本图书馆CIP数据核字（1999）第28003号

计算机及网络安全与防护基础

宁 章 编著

责任编辑 肖之中

责任校对 陈 坤

北京航空航天大学出版社出版发行

北京市学院路37号（100083），发行部电话 82317024

http://www.buaapress.cn.net

E-mail:pressell@publica.bj.cninfo.net

北京宏文印刷厂印装 各地书店经销

开本：787×1092 1/16 印张：12 字数：300千字

1999年10月第1版 1999年10月第1次印刷 印数：4000册

ISBN 7-81012-894-9/TP·250 定价：19.00元

前　言

计算机及网络的发展为社会带来了繁荣和进步，使全社会的面貌为之一新。但在繁荣的背后潜伏着隐患。计算机的实体安全、运行安全、数据安全、软件安全等问题已成为社会各方面关注的话题，一旦计算机系统不能抵抗敌对势力的攻击，国家的安全将受到威胁。海湾战争中，伊拉克的指挥系统由于受到敌方激活的病毒攻击而瘫痪；车臣总统杜达耶夫由于受到 GPS 的跟踪定位而被击毙。信息战已不是遥远的未来。对计算机及网络安全的问题如不引起高度重视，将会造成灾难性的后果。

在发达国家，计算机普及程度高，计算机应用的历史长，应用范围广，出现的安全问题也多，因此对计算机安全的认识要比我们早。在美国的大学中，普遍开设了计算机及网络安全与伦理方面的课程，不但面向学生，而且暑期还面向社区开课，许多普通的美国人自己出钱去听课。正因如此，尽管那里对计算机系统的攻击和产生的恶性事件很多，但绝大多数的计算机是安全的，仅就病毒流行来看，远不像我国流行的范围这样广。这不能不说与他们普遍采取的安全防护措施和安全教育有关。

作者提供本书并不是要向读者系统地介绍计算机及网络安全的理论，而仅想将国内外计算机及网络防护的概况和主要技术措施介绍给读者，以期在我国普及计算机及网络的基础知识，构筑起层层安全防护的屏障，使计算机的广泛应用有一个安全稳定的环境。由于作者水平所限，也许不能满足读者的要求，书中还会有许多不当甚至错误之处，敬请读者批评指正。

本书共分 12 章，由宁章执笔。参加本书审校、录入、绘图等工作的还有张籍、王宏健、王云霞、林世琼、徐慧、普鑫、黄琼、张扬等。此外，本书的出版还得到了赵金云、李永生、张建国、王文艺以及索菲、丁申等的支持和帮助，在此一并表示感谢。

作　者

1999 年 8 月 1 日

目　录

1

概　论

信息安全是一个具有悠久历史的话题。随着阶级的出现，人们开始注意信息的保密。在古罗马时代已有简单的密码，用来隐蔽信息。国家出现以后，在政治、经济、军事、外交等领域，信息安全成为十分重要的问题。除了物理和管理上的措施外，密码技术不断发展并逐渐形成一门学科。用密码技术来隐蔽信息已成为信息传送最可靠的手段。

本世纪40年代以来，计算机的出现和迅速普及使人类社会步入信息时代，同时也促使信息安全技术更加普及，发展更快，并成为为广大人民服务的科学。

随着计算机在社会各个领域的广泛应用，以计算机为核心的信息系统安全保密的问题越来越突出。同计算机出现前的信息安全保密相比，计算机安全保密的问题要多得多，也复杂得多，涉及到物理环境，硬件、软件，数据传输等各个方面。除了传统的安全保密理论和技术外，计算机信息系统安全有更多的内容和独立的体系。

70年代以来，在计算机应用和普及的基础上，以计算机网络为主体的信息处理系统迅速发展，计算机应用也逐渐向网络发展。网络化的信息系统是集通信、计算机和信息处理于一体的，连接广大区域，直至将全球连成一体的系统，是现代社会不可缺少的基础。网络信息安全保密的问题与单纯的计算机安全问题不同，不仅有单机的问题，而且有大量环境、传输、体系结构等问题。系统安全的问题包括了计算机安全、通信安全、操作安全、访问控制、实体安全、电磁安全以及安全管理和法律制裁等。

计算机应用发展到网络阶段后，信息安全技术得到迅速发展，原有的计算机安全问题增加了许多新的内容。70年代以来是密码技术蓬勃发展的时期，这个古老而又神秘的学科开始走向民间，走向大众。

总之，计算机及其网络系统的出现和不断发展，使信息安全这个古老的学科获得了新生。计算机安全是信息系统安全的基础，随着信息系统的广泛建立和各种网络的互连，安全逐渐扩展到系统和体系，而成为全方位的安全保密。随着信息高速公路的兴起，全世界通过网络连接在一起的时代即将到来，在阶级和国家依然存在的社会，在敌对势力依然存在的环境下，安全保密必须引起高度重视并探索和解决不断出现的新问题，确保计算机信息系统真正造福于国家和人民。

1.1 计算机及网络的普及和脆弱性

1.1.1 对计算机及网络的依赖性

计算机自1946年问世以来飞速发展，已更新了四代(电子管、晶体管、集成电路、大规模集成电路)。它在政治、经济、金融、军事等领域和社会生活中得到了广泛的应用，使人类社会的工作和生活方式发生了重大变化，极大地促进了社会生产力的发展和社会的繁荣。

目前计算机网络遍及机关、学校、银行、商业等各个方面。各个领域的重要信息，如国民经济计划、人员档案、银行账目以及部队番号、武器装备、作战计划、部队调动情况等，都存在计算机内，由计算机进行统计、分析、处理、辅助设计和决策等工作。正因为如此，计算机信息处理系统已是国家政治、经济、金融、军事等部门正常工作的命脉。

由于计算机网络系统已将政治、经济、军事等各个方面连成一体，这就使敌对势力将计算机及其网络系统作为主要的攻击目标之一。今天赢得战争优势的关键已不是看谁的火力强，而更要看谁先发现对方，谁比对方反应快，谁比对方打得准，电子战已走向主战场。

通过对计算机信息系统的干扰、破坏，瓦解国民意志，使经济瘫痪，使军事指挥系统不能正常工作，丧失或削弱作战能力，从而夺取战场上的主动权，进而赢得战争胜利，这已是一种新的作战模式。计算机信息系统不仅是社会各方面正常运转的命脉，而且计算机信息系统的安全已成为军事安全和国家安全的基础。

1.1.2 计算机系统的脆弱性

计算机系统的脆弱性表现在它极易受攻击和侵害，它的抗打击力和防护力很弱。外界对计算机(硬、软件)有意或无意的攻击可使其不能正常工作。

1. 易受环境和灾害的影响

温湿度、供电、火灾、水灾、静电、灰尘、雷电、强电磁场、电磁脉冲等，均会破坏数据和影响它的正常工作。

2. 易受攻击

计算机病毒于70年代中期开始在科幻小说中描述，但不久就出现在计算机系统中，并对计算机安全构成严重威胁。目前病毒的应用正在向军用方面发展。美军就正进行病毒直接注入、间接注入的研究，并进行了以无线方式，经空间把计算机病毒注入敌方的飞机、军舰、武器系统、通信设备中去的试验。

1988年美国计算机系统发生的一次蠕虫病毒事件使18万台计算机阻塞，6 000台计算机瘫痪，大量数据因死机丢失，经济损失上亿美元。

1991年在海湾战争中第一次针对信息系统使用了计算机病毒武器。美国国家安全局研制出一种AF/91的病毒，侵入到伊拉克的军用计算机网，使伊军的指挥系统失灵，削弱了伊军战斗力。

3. 易被偷取或修改信息

计算机有共享资源的特点，这就使犯罪者可进入系统窃取信息、修改数据、盗窃他人存款、获取资金。传统的贪污方法一般要涂改银行票据，制作假支票等，而计算机犯罪只须修改计算机内的信息即可达到目的，并且作案可在很短的时间内不留痕迹地完成。

例如，某银行营业部微机操作员利用职务之便，制造假账户，晚上趁机房无人之机，利用微机向假账户非法输入 87 万元，并修改源程序，使总账虚平，进行贪污。

又如，中国工商银行某县支行城市信用社的某计算机记账员，曾在短短的 68 天中利用计算机贪污挪用了 47 万元。

据报导，在美国等西方国家，每年通过计算机窃走的金钱已高达上百亿美元。

犯罪者可采用非法手段进入系统，收集和窃取信息，打开数据库，偷窃或篡改数据库资料等。犯罪者可利用计算机网络的脆弱性，通过通信线路从终端设备上窃取重要信息。例如，在同一条通信线路上加装终端，冒充合法使用者，窃取系统中的重要信息。此外，犯罪者还可采用截获电磁波、远距离摄影、激光窃听等高技术手段，进行不直接接触计算机系统的远距离窃收，再经放大还原处理，得到重要信息。

从安全保密的角度讲，计算机信息系统关系着党和国家的安危。一旦敌方利用计算机的脆弱性窃取了这些重要信息，将严重危害国家的安全，在战争时期甚至会决定战争的胜负。历史上的“中途岛战役”和“山本五十六之死”均是由于密码被破译而造成重大损失的范例。特别是随着国际互连网的发展，成千上万的用户通过计算机与互连网相连，敌对势力可通过互连网搜集、处理和破坏国家的政治、经济、军事、科技等信息，引发一系列政治、经济和社会问题。

1.2 计算机犯罪

计算机科学的发展，促进了社会的繁荣和进步。然而，由于计算机科学发展得太快，使它在许多方面还不完善，还不能适应复杂的现实社会，具有易受攻击的脆弱性。随着人们对计算机的依赖与日俱增，计算机犯罪对社会的威胁也日益严重。在某些国家计算机犯罪已成为严重的社会问题。总之，一方面由于计算机系统的开放和信息共享，使计算机应用的范围不断扩大；另一方面正是由于计算机系统的开放和计算机自身的脆弱性，导致了计算机安全方面的诸多漏洞。

计算机犯罪多数是以冒充合法用户的身份进入系统并对系统实施攻击。犯罪的目的主要有：

(1) 为得到财产，采取修改程序和数据的方法，使财产转移到犯罪者的控制下。例如，可通过改变工资、存款账目等，转移钱财到另一户头并取出现金。

(2) 窃取机密信息，如外交、军事、经济计划、商业秘密等。

(3) 通过损坏硬件和软件，使合法用户的操作受到阻碍。

(4) 出于恶作剧，既显示自己编程的能力，又以破坏系统的运行而取乐，许多病毒的制造者和施放者是出于这种目的。

计算机犯罪的手段有：

1. 扩大授权

采用技术手段，扩大系统的授权，以进行非法活动。这种方法一般要熟悉操作系统，从系统程序入手扩大授权。扩大授权的内容有：

· 浏览：浏览是在系统或终端设备上利用合法手段在存储区查看登录内容，搜索有兴趣或有价值的信息，或是利用合法访问系统某一指定文件的机会，趁机访问非授权文件。这些都是在正常操作掩护下的非法活动。例如，通过使用 PC 机冒充授权用户，可浏览不公开的电话号码，拨通这些电话用户。

• 延长响应：利用操作系统延长程序停止执行指令的响应时间，察看存储器最新的使用情况，窃取重要信息。

• 后门：攻击者插入一段程序，使系统允许攻击者键入一个他自己的口令而多次进入，或采取其它措施，绕过安全控制路径进入系统。如 1994 年 2 月欧洲安全组织就曾关闭了与美国中央情报局连接的线路，同时发布了一条限制使用的说明：闯入者制造了可攻击 UNIX 操作系统自举程序的病毒并制造了使闯入者任何时候均可进入计算机系统的"后门"。

• 自举攻击：使用一条普通的操作系统命令欺骗计算机，使它承认攻击者为系统管理员的身份，具有系统管理员的特权，从而进行违法活动。

2. 线路窃收

将数据线与计算机或通信线相连，当合法用户发送口令时，捕获口令。

3. 偷 看

进入计算中心或终端区，观察显示屏上的口令和其它重要信息。如可冒充午餐或食品的送货人，多次进入。一旦察觉到口令后，就可冒充合法用户窃取重要信息，这种手段也称冒名顶替。因此，用户的口令一定要注意更新和保密。

4. 光窃收

在附近建筑物内通过高倍率望远镜观看屏幕上显示的信息。

5. 窃 收

将窃收器，即一种截获电磁波或声波的微型秘密装置，安放到计算中心数据线（或总线）上，被拦截的信号则可在几公里外的接收机上复现。典型的例子是冒充电话公司的修理工进入房间并在线路上安装窃收器，或在拟发送的计算机内事先安放好窃收器。

6. 拦 截

拦截监视器屏幕向外辐射的电磁波，并将其还原，这称为 TEMPEST 拦截。采用此法可获得许多其它方法得不到的机密信息。

7. 清理垃圾

这是从计算机系统周围的废弃物中获取信息的一种方法。例如，从废弃磁盘或磁带上窃取信息或收集抛弃到垃圾箱中的废打印输出物，以寻找有用的情报。据报导，曾发生一个用户从废弃的磁盘上获取了若干石油公司的地震测量数据，并将这些具有商业价值的数据转卖给其它石油公司的案例。

8. 模 拟

对计算机编程，使其模拟一个目标计算机，用它收集、破译用户的口令，再冒充合法用户回答呼叫。

9. 欺 骗

假冒一个合法用户，通过电话向系统管理员询问口令，或通过贿赂获取口令，然后闯入系统。使用口令词典，借此猜中用户的口令。还可利用各种特征，如生日、房间号、街道、城市、影星、球星等，提高口令的猜中率。

10. 顺手牵羊

顺手牵羊是利用计算机系统分时处理的特点获取情报。分时使用的用户使用口令进入后，可能因事离开，此时会被他人利用，冒充已被授权的合法用户，窃取信息或数据。在数据处理中心，用户的程序和打印结果常会被人冒领，这也是钻了管理上的漏洞而出现的顺手牵羊。

11. 尾 随

紧跟在授权用户之后，通过转动门或其它障碍，绕过物理访问控制措施。

12. 线间进入

当已授权用户吃午饭或进洗手间时，接管一个已注册的终端或 PC 机窃取信息。

13. 高级对抗

使用一个实用的人工干预程序侵犯安全控制系统。更改程序和数据的运行时间，或采取措施，利用系统调用或干预程序，使计算机处于特权方式下操作，以实现非法目的。例如，美国一州立银行就曾发生一起计算机犯罪案件，银行的计算机操作人员利用人工干预程序修改了账目，而没有通过控制日志记录，从一个客户的账目中盗走了 12.8 万美元。

14. 计算机病毒

这是隐藏在可执行文件或数据中的一段程序，它具有传染性、潜伏性和可激发性。它可对本系统，也可对网上连接的其它系统发起攻击，使被攻击的系统瘫痪。其主要的形式有：

· 特洛伊木马：这是一种恶毒的程序，平时以合法的身份隐藏在其它程序中，一旦发作，则对系统产生威胁，使计算机在完成正常任务的同时，执行非授权功能。如复制一段越过系统授权的程序(后门)等。特洛伊木马本身可通过电子邮件渗透。

· 蠕虫：这是一种可自我复制的病毒，发作时可自我复制，使存储器充满代码，致使计算机瘫痪。同时，它还可通过网络来传播错误，从而造成网络服务中止和死锁。通常需要清除病毒和重新启动才能恢复。

· 逻辑炸弹：这是一种恶毒的程序，平时处于休眠状态，至日历上的某个日期或时刻被激活，对计算机进行恶意破坏，甚至将计算机硬件损坏。逻辑炸弹又称为定时炸弹，是对系统的潜在威胁和隐患，可以造成严重危害。例如，曾报导一起案件，某公司一财务人员在被公司解雇时，向计算机中输入一段程序，在他本人离开 3 个月后被激活，破坏系统文件，使计算机瘫痪。又如已发现的 10 月 26 日病毒，就在每月的 26 日发作，1998 年 10 月 26 日曾在我国大面积发作，使成千上万台计算机的硬、软件受到攻击而损坏。

· 偷袭程序：这是出现频度很高的一类病毒，它藏在计算机大容量存储器的隐蔽处，通过被特洛伊木马欺骗的用户激活，或是通过逻辑炸弹爆炸，对系统实施有目的的攻击。

· 意大利香肠：意大利香肠是采取不易察觉的手段，迫使对方做出一连串细小的让步，而达到偷窃的目的。在金融系统的计算机犯罪中，多次发生此类案件。在处理客户存取账目时，每次截留一个零头，然后将这部分钱转到另一个虚设的账号上。日积月累，可盗窃一大笔款项。例如，据报导，纽约一家银行的程序员，利用计算利息时对结果四舍五入的特点，在计算利息的程序中插入一个累计舍去值并将其转移出去的子程序。利用该程序，将用户存款利息的舍去值累计起来，并转移到自己的账号上，从而获得一大笔非法收入。会计在审查时，看到支付利息的总数是正确的，因此不易被发现。

1.3 计算机及网络安全的研究内容和发展过程

1.3.1 研究内容

计算机安全是指计算机资产安全，即计算机信息系统资源和信息资源不受自然和人为有害因素的威胁和危害。一切影响计算机安全的因素和保障计算机安全的措施都是计算机安全

学研究的内容。主要有：

实体安全——系统设备及相关设施运行正常，系统服务适时。包括环境、建筑、设备、电磁辐射、数据介质安全及灾害报警等。

运行安全——系统资源和信息资源使用合法。包括电源、空调、人事管理、机房管理、出入控制、数据与介质管理、运行管理等。

数据安全——系统拥有的和产生的数据或信息完整、有效，使用合法，不被破坏或泄漏。包括输入/输出数据安全、进入识别、访问控制、加密、审计与追踪、备份与恢复等。

软件安全——软件(网络软件、操作系统、资料)完整。包括软件开发规程、软件安全测试、软件的修改与复制等。

通信安全——计算机通信和网络的安全。包括线路、传输、接口、终端与工作站、路由器的安全等。

1.3.2 发展过程

事物的发展一般是从无到有，从小到大，从简单到完善的过程。计算机安全问题也同样。50年代，计算机应用范围很小，安全问题并不突出，计算机系统并未考虑安全防护的问题。后来发生了袭击计算中心的事件，才开始对机房采取一些实体防护措施。但这时计算机的应用主要是单机，计算机安全主要是实体安全防护和硬、软件防护。多用户使用计算机时，将各进程所占存储空间划分成物理或逻辑上相互隔离的区域，使用户的进程并发执行而互不干扰，即可达到安全防护的目的。

70年代以来，随着计算机在政府机关、金融、商业等部门的广泛应用，随着重要机密的信息采用计算机处理，间谍和罪犯将计算机系统作为侵犯的目标，计算机犯罪的案件不断发生。人们认识到，计算机安全关系到国家的安全和社会的稳定并开始重视这个问题。许多人开始进行研究，并出现了计算机安全的法律、法规和各种防护手段，如防止非法访问的措施，口令、身份卡、指纹识别等。这时计算机已由单机应用发展到计算机网络，除存储和数据处理外，信息尚须通过线路传输，使网络受到攻击的部位增多，特别是传输线路和网络终端最为薄弱。这时，针对网络安全防护，出现了强制性访问控制机制、完善的鉴别机制和可靠的数据加密传输措施。数字签名则是鉴定用户合法性的手段。

70年代中期，在安全保密研究中出现了两个引人注目的事件。一是 Diffie 和 Hellman 冲破人们长期以来一直沿用的单钥体制，提出一种崭新的公开密钥密码体制；二是美国国家标准局(NBS)公开征集，并于1977年1月正式公布实施美国数据加密标准(DES)。公开 DES 加密算法，并广泛应用于商用数据加密，这在安全保密研究史上是第一次，它揭开了密码学的神秘面纱，极大地推动了密码学的应用和发展。

80年代以来，国外又发展出以抑制计算机信息泄漏为主的 TEMPEST 技术，重要的部门均配备 TEMPEST 认证的计算机及外围设备。

为对用户计算机安全性进行评价，为研制、生产提供依据，80年代中期美国国防部计算机安全局公布了可信计算机安全评估准则，主要是规定了操作系统的安全要求。准则提高了计算机的整体安全防护水平，至今仍具权威性。

进入90年代以来，信息系统安全保密研究出现了新的侧重点。一方面，对分布式和面向对

象数据库系统的安全保密进行了研究；另一方面，对安全信息系统的设计方法、多域安全和保护模型等进行了探讨。随着信息系统的广泛建立和各种不同网络的互连、互通，人们意识到，不能再从单个安全功能、单个网络来个别地考虑安全问题，而必须从系统上、从体系结构上全面地考虑安全保密。

国际互连网是世界范围内信息交流的基础设施。它的出现促进了人类社会向信息社会的过渡，并将彻底改变人们的生活、学习和工作方式，使人们在更大的范围内交流信息、共享信息。作为开放的信息系统，互连网成为信息战的攻击重点，成为窃密与反窃密斗争的战场。为保护互连网的安全，主要是保护与互连网相连的内部网站的安全，除了传统的各种防护措施外，还出现了防火墙和适应网络通信的加密技术。它们有效地提高了网站的整体安全防护水平。

近年来，国内外在安全方面的研究主要集中在两个方面：一是以密码学理论为基础的各种数据加密措施；另一是以计算机网络为背景的通信安全模型的研究。前者已更多地付诸于实施，并在实际应用中取得了较好的效果；而后者尚在理论探索阶段，ISO 在 1989 年提出了一个安全体系结构，虽然包括了开放式系统中应该考虑的安全机制、安全管理以及应提供的安全服务，但只是一个安全模型。随着信息高速公路的兴起，全球信息化建设步伐不断加快，网络的安全保密研究将会得到更进一步的发展。

从 60 年代以来，计算机安全已逐渐发展成为一门新兴学科。成立了计算机安全的国际组织，每两年召开一次学术会议。在美、日等国每年有上千篇计算机安全方面的论文发表。国外的计算机系统已将安全性作为计算机系统性能的一项重要考核指标。在美国的大学中专门设有计算机安全的课程和信息保护方面的课程设计。

随着科学技术的发展，每当一种计算机安全防护技术出现不久，犯罪者就会以更高的技术手段从事窃密和破坏活动，使得原来的防护措施失效，计算机仍然处于不安全的状态。由于社会日益依赖计算机，计算机犯罪逐渐成为信息社会中的重要犯罪方式。犯罪者也逐渐由个人作案转变为犯罪团伙，有些甚至发展为国际性的犯罪组织。随着计算机科学的发展和计算机应用范围的进一步扩大，还会出现一些新的安全问题。例如，目前计算机网络的规模不断扩大，计算机的容量、速度不断增加，而防护措施较差，甚至没有防护措施的微机连网数目又不断增多，使得成千上万的用户可直接接触计算机的资源。此外，随着存储载体容量的增加，建立了不同用途的、集中的大型数据库，这也扩大了直接接触计算机的人员数量，这些都使计算机信息更易受到损害。面对以上这些问题，如何从整体上采取积极的防护措施加以解决，这也是各国正在考虑和研究的问题。

1.4 计算机及网络安全的分层防护措施

计算机安全是一门新兴学科。目前尚有许多理论与工程实践问题没有解决。对计算机的安全防护问题也还有不同的看法。但比较一致的意见是计算机系统的安全没有一种一劳永逸的解决措施，需要将计算机系统的各种安全防护技术，如实体安全防护技术、防电磁辐射泄漏技术、硬软件防护技术、防火墙技术、数据保密变换，以及安全管理与法律制裁等结合使用，对计算机系统进行综合的分层防护，从而提高计算机信息的整体安全防护水平。这也是各国从事计算机安全研究的科学家的共同认识。分层防护的原理见图 1-1。其中最外层是社会层，主要通过法律、管理、伦理道德教育等，减少犯罪的可能、保持社会的稳定。由外及内，分别是实体安

全防护、电磁防护、硬软件防护、通信和网络防护、数据保密变换等。

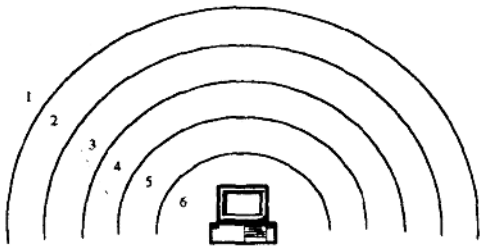

图 1-1 计算机及网络的分层防护

1.4.1 法律、管理、伦理道德教育等

1978 年出现了世界上第一部计算机犯罪法——佛罗里达计算机犯罪法。它首次将计算机犯罪定为侵犯知识产权罪。计算机软件也逐渐被列入知识产权的范畴，从而受到法律的保护。而在此之前，对偷取信息、篡改信息是否有罪尚无法律依据。

对计算机犯罪定罪、量刑产生的威慑力可使有犯罪企图的人产生畏惧心理，从而减少犯罪的可能，保持社会的安定。

加强计算机安全管理的法规建设，建立、健全各项管理制度是确保计算机系统安全不可缺少的措施。如制定人员管理制度，加强人员审查；组织管理上，避免单独作业，操作与设计分离等。这些强制执行的制度和法规限制了作案的可能性。

加强伦理道德教育对社会的稳定和计算机安全十分重要。

总之，采取这些措施可保持社会的稳定，将侵犯计算机的企图减到最低，在最广大的范围内保证计算机系统的安全。

1.4.2 实体安全防护

为保证计算机系统的正常工作，首先要保证正常供电。要采取一系列保护措施，稳压器、不间断电源、应急发电设备等，避免供电中断、异常状态、瞬变、冲击、噪声等事件的影响。此外，还应保证机房有合适的温湿度、洁净度、防静电措施等。为防止火灾的破坏，应有符合要求的消防、报警和管理措施。要对接地系统进行合理设计，以保证设备的安全，减少干扰，防止静电，避免雷击等。

采用物理防护手段，建立物理屏障，阻止非法入侵者接近计算机系统，是行之有效的防护措施，这些措施有进入识别、区域隔离和边界防护等。

进入识别已从早期的专人值守、验证口令等发展为密码锁、磁卡等身份识别措施。为了防伪造，新型的磁卡带有智能化的单片机(即微处理器)，称为“灵巧卡”。它识别安全性好，可避免冒充、伪造和穷举等形式的攻击。80 年代以来又出现了指纹识别、视网膜识别和语音识别等手段，有效地阻止了许多非法入侵事件。

区域隔离和边界防护是将重要的计算机系统周围构造一个安全警戒区，边界设置障碍，区内采取重点防范，甚至昼夜警戒，将入侵者阻拦在警戒区以外。

1.4.3 电磁防护

1. 电磁干扰和电磁兼容

计算机是一种电子设备，它在工作时向外辐射电磁波，同时又受到其它电子设备的电磁干扰，到一定的程度就会影响它的正常工作。

电磁干扰可通过电磁辐射和传导两条途径影响设备的工作。一条是电子设备辐射的电磁波通过电路耦合引入到另一台电子设备中引起干扰；另一条是通过连接的导线、电源线、信号线等耦合而引起相互之间的干扰。

电子设备及其元器件都不是孤立存在的，而是在一定的电磁干扰的环境下工作。电磁兼容性就是电子设备或系统在一定的电磁环境下互相兼顾、相容的能力。

电磁兼容的历史很长。1831 年法拉第发现电磁感应现象，总结出电磁感应定律。1881 年英国科学家希维思德发表了"论干扰"的文章。1888 年赫兹证明了电磁干扰现象。20 世纪以来，特别是在二次世界大战中，电磁兼容理论进一步发展，逐步形成了一门独立的学科。一直到 80 年代，电磁兼容设计已成为军用武器装备和电子设备研制中必须严格遵守的原则，电磁兼容性成为产品可靠性保证的重要组成部分。如果设备的电磁兼容性很差，在电磁干扰的环境中就不能正常工作。如果是机载、弹载设备，就会造成飞机、导弹失事。各国的民标和军标都是从电磁干扰和敏感度两方面来规定电子设备的电磁兼容性要求，我国亦已将电磁兼容性作为强制性的标准来执行。

2. 现代战争对电磁防护的要求

现代战争的重要特征之一是改变了传统的靠硬武器决胜的观念，而广泛采用电子战等作战手段。即以电子侦察、电子伪装、电子攻击等手段，与地面战斗行动相配合，硬杀伤与软杀伤相结合，形成协同作战的整体威力。

在近代战争中有许多电子战的战例。在 70 年代到 80 年代的中东战争中，以军将电磁干扰站配置在第一战斗梯队中，对埃、叙的雷达和通信设备实施干扰。干扰总是在最重要、最紧急通报的时刻进行，使埃、叙的雷达和通信设备不能正常工作，从而遭到重大损失。

海湾战争是典型的现代战争的战例。这场战争作战时间仅为 42 天：

第一阶段：1991 年 1 月 17 日开始，共 38 天，主要是空袭。空袭的主要目标是通信、指挥系统，使伊军整体作战能力下降 50%以上。

第二阶段：1991 年 2 月 24 日开战，共 4 天，地面部队行动。伊拉克共伤亡 10 多万人，损失 2 000 亿美金。

采用的手段有：

(1) 电子侦察：卫星、飞机、侦察站等窃收信息，截获电磁波；

(2) 电子干扰：强电磁干扰，压制防空雷达、武器制导、指挥系统等；

(3) 电子伪装：F—117、B—2 等飞机采用各种吸波透波材料及独特的外形设计，能吸收雷达和红外辐射。突破 200 公里纵深，如无电子干扰措施，损失为 6.5%，反之为 0。

(4) 精确制导和反辐射武器：精确制导系统、反辐射雷达、反辐射电子设备等。

在海湾战争开战前几个月就开始截获伊拉克的电磁波，分析出通信和雷达系统的各种参数。1991 年 1 月 17 日空袭前，电子干扰机和地面设备实施电子干扰，使伊军通信中断、指挥失灵。同时，受多国部队电磁波激活的攻击程序使伊拉克的指挥系统遭破坏而瘫痪。接着进行空

中打击和地面部队的行动。

有人认为目前大规模杀伤性武器的发展道路已走到尽头，战争已主要不是打钢铁，而是打芯片。以电子信号欺骗和电子干扰为主的软杀伤武器已走向战场。电磁空间和计算机安全方面的对抗在现代战争中极为激烈。电子设备不具备电磁防护的功能，很难取得战争的胜利。有人认为未来战争的胜利属于能够驾驭电磁频谱的一方。

3. 电磁防护的措施

为提高电子设备的抗干扰能力，除在芯片、部件上提高抗干扰能力外，主要的措施有屏蔽、隔离、滤波、吸波、接地等。其中屏蔽是应用最多的方法。

电磁波经封闭的金属板之后，大部分能量被吸收、反射和再反射，再传到板内的能量已很小，从而保护内部的设备或电路免受强电磁干扰。

滤波是另一种重要的方法。滤波电路是一种无源网络，它可让一定频率范围内的电信号通过而阻止其它频率的电信号，从而起到滤波作用。在有导线连接或阻抗耦合的情况下，进出线采用滤波器可使强干扰被阻止。吸波是采用铁氧体等吸波材料，在空间很小的情况下起到类似滤波器的作用。

隔离是将系统内的电路采用隔离的方法分别处理，将强辐射源、信号处理单元等隔离开，单独处理，从而减弱系统内部和系统向外的电磁发射。

接地对电磁兼容来说十分重要，它不仅可起到保护作用，而且可使屏蔽体、滤波器等集聚的电荷迅速排放到大地，从而减小干扰。作为电磁兼容要求的地线需单独埋放，对其地阻、接地点等均有很高的要求。

4. 计算机通过电磁发射引起的信息泄漏

1985年在法国举办的"计算机与通信安全"国际会议上，荷兰的一位工程师现场演示了用一套稍加改装的设备和黑白电视机还原一公里以外的机房内计算机显示屏上的信息。这说明计算机的电磁辐射造成信息泄漏的危险是经常存在的。尤其是在微电子技术和卫星通信技术飞速发展的今天，各种窃取手段日趋先进，计算机电磁辐射泄密的危险越来越大。

计算机工作时，明信号的泄漏主要是通过传导发射和向空间的辐射发射传播出去的。由窃取信号泄漏得到的情报比其它方式更为隐蔽、准确和及时，同时也更为危险。

美、俄、北约诸国对这个问题进行了多年研究并逐渐发展成一种专门的技术——抑制信息处理设备的噪声泄漏技术，简称信息泄漏防护技术(TEMPEST 技术，美国：NACSIM5100A)。

从80年代初期开始，美国市场上陆续出现了一种符合 TEMPEST 标准的军用通信设备，并逐渐形成商品化、标准化生产。美国政府规定，凡属高度机密部门所使用的计算机等信息处理设备，其电磁泄漏发射必须达到 TEMPEST 标准规定的要求。

TEMPEST 技术是综合性很强的技术，包括泄漏信息的分析、预测、接收、识别、复原、防护、测试、安全评估等项技术，涉及到多个学科领域。它基本上是在传统的电磁兼容理论的基础上发展起来的，但比传统的抑制电磁干扰的要求要高得多，技术实现上也更复杂。它关心的是不要泄漏出有用的信息，即红信号。一般认为显示器的视频信号、打印机打印头的驱动信号、磁头读/写信号、键盘输入信号以及信号线上的输入/输出信号等为红信号，须重点防护。

电磁防护层主要是通过种种措施，提高计算机的电磁兼容性，提高设备的抗干扰能力，使计算机能抵抗强电磁干扰；同时将计算机的电磁泄漏发射降到最低，使之不致将有用的信息泄漏出去，从而在未来的电子战、信息战中立于不败之地。

1.4.4 硬、软件防护

1. 硬件防护

硬件是计算机系统的基础。硬件防护一般是指在计算机硬件(CPU、存储器、外设等)上采取措施或通过增加硬件来防护。如计算机加锁,加专门的信息保护卡(如防病毒卡、防拷贝卡),加插座式的数据变换硬件(如安装在并行口上的加密狗等),输入/输出通道控制,以及用界限寄存器对内存单元进行保护等措施。

2. 软件防护

软件防护主要指通过计算机软件提供安全防护功能。

系统软件是软件的重要组成部分,计算机系统的安全在很大程度上依赖于操作系统本身的安全和它为系统提供的安全防护功能。近年来按照可信计算机安全评估准则(TCSEC)的要求进行安全操作系统的设计和改进,在安全防护方面增加了许多功能,有效地提高了系统的安全性。目前已有达到A1级安全标准的操作系统,传统的UNIX经重新设计安全内核,也已达到B级安全标准。

操作系统提供的安全防护功能主要有个人身份鉴别、存取控制授权矩阵、隔离控制、监视程序控制(需要调数据时必须经监视程序判别合法性,再决定是否调)等。这几种方法主要用于访问控制和系统隔离。即系统要确定是否合法用户,享有何种授权,对资源(内存、I/O、CPU等)可进行什么类型的访问操作(读/写、运行等),同时对用户规定与信息密级和资源类型相适应的授权。此外,通过软件使系统隔离,避免安全隐患的扩散,从而保证信息系统的安全。

近年来专门的防护软件出现了不少,这些专门的软件针对性强、研制快、见效快、使用灵活。例如防病毒的软件在国外已十分普遍,绝大多数网络系统均装有这类防护软件。一开机先扫描,通过后再继续执行。一旦有外来盘插入使用,要先详细检查,无问题后才可进入。

1.4.5 计算机通信及互连网的安全防护

1. 通信安全

计算机通信安全主要包括:线路安全、传输安全、数据保密变换、辐射安全、技术安全和终端安全。内部和外部通信线路是敌对势力窃取信息的重要目标。为保护线路安全,除采取物理防护措施外,还可采用报警等技术措施。

数据传输首先要考虑安全可靠,为此对传输初始化、测试、校验和纠错等有一系列要求。此外,对注册、语言保密、通信报量分析等要采取相应的措施。

上述信息安全防护方法主要是针对单台计算机。随着网络的发展,特别是国际互连网的出现,我们面临的是更加开放、更大范围,甚至是全球性的互连网系统。有些防护措施对网上站点,网上主机、工作站,是适合的,但对与互连网相连的内部网的安全,对于传输、通信安全则应有更完善的技术手段来保证。

2. 互连网的安全

防火墙是适应互连网的发展而出现的一种安全防护技术。它是内部网和外部网之间实施安全防范的系统,也是一种访问控制机制。防火墙通常安装在被保护的内部网与互连网的连接点上。从互连网或内部网上产生的任何活动都必须经过防火墙,由防火墙来确定这些活动是否可以接受。