公安计算机应用基础
系列教材

公共信息网络安全与管理

主编　米　佳

大连理工大学出版社
DALIAN UNIVERSITY OF TECHNOLOGY PRESS

公安计算机应用基础系列教材

公共信息网络安全与管理

主　编　米　佳

副主编　侯丽波　陆宝华　赵连凤

大连理工大学出版社

图书在版编目(CIP)数据

公共信息网络安全与管理 / 米佳主编．—大连：大连理工大学出版社，2006.8
（公安计算机应用基础系列教材）
ISBN 7-5611-3336-7

Ⅰ．公… Ⅱ．米… Ⅲ．信息网络—安全技术—高等学校—教材 Ⅳ．TP393.08

中国版本图书馆 CIP 数据核字(2006)第 100768 号

大连理工大学出版社出版
地址：大连市软件园路 80 号 邮政编码：116023
发行：0411-84708842 邮购：0411-84703636 传真：0411-84701466
E-mail：dzcb@dutp.cn URL：http://www.dutp.cn
大连业发印刷有限公司印刷 大连理工大学出版社发行

幅面尺寸：185mm×260mm 印张：17 字数：391 千字
印数：1～2 000
2006 年 8 月第 1 版 2006 年 8 月第 1 次印刷

责任编辑：高智银 责任校对：于振波
封面设计：宋 蕾

定 价：23.00 元

前　言

信息网络的普及，促进了社会经济飞速发展，提高了人们的工作效率和生活质量。但是同时网上信息的泄露、篡改和假冒，黑客入侵，计算机犯罪，病毒蔓延和不良信息传播等等，也给社会公共安全带来了新的挑战。特别是随着政府、部门和行业对网络环境和网络资源依赖程度的加强，涉及国家安全和社会公共安全的所有重大问题都在网络上表现出来，信息网络的安全问题已经对社会政治经济发展构成了严重的威胁。为此中共中央特别提出：我们要在全社会广泛应用信息技术、提高计算机和网络普及应用程度的同时，加强信息化法制建设和综合管理，强化信息网络的安全管理。

我国的信息网络安全管理起步较晚，安全防护能力与发达国家有较大的差距。国内许多信息网络应用系统尚处于不设防状态，存在着很大的风险性和危险性；近年来，党和国家提高了对信息网络安全的重视程度，将信息网络安全列入国家重点基础研究发展规划项目，并作为国家“十五”、“863 计划”和国家自然科学基金会支持的重点。但是解决信息网络安全仅依靠技术是不够的，特别是面向社会的公共信息网络安全管理工作是一项系统工程，要结合技术、管理、法制、政策、教育等，将信息网络风险降低至最小程度。这其中信息网络安全技术是手段，建立安全组织、落实安全管理制度、完善法律法规是基础，普及信息网络安全教育、管好人员是核心。据 CNCERT/CC 发布的“2004 年全国网络安全状况调查报告”显示，被调查对象认为引发网络安全事件原因中最主要的是利用未打补丁或未受保护的软件漏洞占 50.3%；对员工没有进行充分的安全操作和流程的培训及教育占36.3%；紧随其后的是缺乏全面的网络安全意识教育占 28.7%。所以我们要重视信息网络安全教育，提高工作人员的安全意识，使公共信息网络安全管理措施的落实逐步转变为法律约束下的自律行为，这是信息网络安全管理的关键。

公共信息网络安全管理是国家赋予公安部门的一项新的任务，公安机关要对公共信息网络中存在的问题和违法犯罪案件严格管理、加强打击，在虚拟空间建立“打防结合”的工作机制，为我国信息网络健康发展保驾护航。为此，作为未来的人民警官，要想更好地完成历史赋予我们新的使命，就必须要树立公共信息网络安全意识，掌握信息网络安全技术基础，了解公安机关在公共信息网络安全管理方面的职能和法律法规、熟悉公共信息网络安全监察和计算机违法犯罪案件的侦察等公安业务，这也是我们本书编写的主要目的。

本书由米佳、侯丽波、陆宝华、赵连凤编写，其中，第 1、7、9、10 章由米佳编写，3～6 章由侯丽波编写，第 2、8 章由陆宝华、赵连凤编写，全书由米佳统稿。

本书紧密围绕公共信息网络安全管理与公安实践，既可以作为公安院校本、专科教材，也可以作为公安一线干警普及公共信息网络安全与管理基础知识的培训教材。

由于编写水平和时间有限，有不当之处请批评指正。

编　者

2006 年 6 月

目　录

第1章　信息网络安全概述

信息网络安全目前已成为信息时代人类共同面临的挑战。美国前总统克林顿在签发《保护信息系统国家计划》的总统咨文中陈述道："在不到一代人的时间里，信息革命以及电脑进入了社会的每一个领域，这一现象改变了国家的经济运行和安全运作乃至人们的日常生活方式，然而，这种美好的新时代也带有它自身的风险。所有电脑运行的系统都很容易受到侵犯和破坏，对重要的经济部门或政府机构的计算机进行任何有计划的攻击都可能产生灾难性的后果，这种危险是客观存在的。过去敌对力量和恐怖主义分子毫无例外地使用炸弹和子弹，现在他们可以把电脑变成有效武器，造成非常巨大的危害。如果人们想要继续享受信息时代的种种好处，继续使国家安全和经济繁荣得到保障，就必须保护计算机控制系统，使它们免受攻击。"

据有关方面统计，目前美国每年由于网络安全问题而遭受的经济损失超过170亿美元，德国、英国也均在数十亿美元以上，法国为100亿法郎，日本、新加坡问题也很严重。在国际刑法界列举的现代社会新型犯罪排行榜上，计算机犯罪已名列榜首。2003年，在CSI/FBI调查所接触的524个组织中，有56%遇到电脑安全事件，其中38%遇到1～5起、16%遇到11起以上。因与互联网连接而成为频繁攻击点的组织连续3年不断增加；遭受拒绝服务攻击(DoS)则从2000年的27%上升到2003年的42%。调查显示，521个接受调查的组织中96%有网站，其中30%提供电子商务服务，这些网站在2003年1年中有20%发现未经许可入侵或误用网站现象。更令人不安的是，有33%的组织说他们不知道自己的网站是否受到损害。据统计，全球平均每20s就发生1次网上入侵事件，黑客一旦找到系统的薄弱环节，所有用户均会遭殃。

信息网络就像一把双刃剑，它在实现了信息交流与共享、极大便利和丰富了社会生活的同时，由于网络本身的脆弱性加上人为攻击与破坏，也对国家安全、社会公共利益以及公民个人合法权益造成现实危害和潜在威胁。因此，加强对信息网络安全技术和管理的研究，无论是对个人还是组织、机构，甚至国家、政府都有非同寻常的重要意义。

1.1　信息网络安全与计算机信息系统

1.1.1　计算机信息系统与信息网络安全概念

1. 计算机信息系统

计算机信息系统是指由计算机及其相关和配套的设备、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、传输和检索等处理的人机系统。信息网络和计算机信息系统是不同发展阶段对计算机信息系统的具体称谓，在90年代中期之

前所称计算机信息系统，是以大型计算机为核心，通过网络将许多个人计算机联在一起形成的计算机信息系统；90 年代末期以来所称的信息网络，则以高速通信网络为纽带，将许多计算机信息系统联在一起形成信息网络。

2. 信息网络安全

信息网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合性科学。

目前对信息网络安全的概念有两种观点：一种观点是面向网络应用的分层思想，认为信息网络安全应包含四个层次，即信息网络实体安全、运行安全、数据安全及内容安全。图 1-1 说明了这种分层的安全结构。

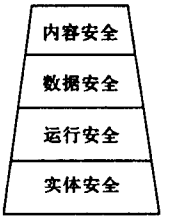


图 1-1　分层的安全结构

(1)内容安全：保证信息在传输过程中不被非法修改和阻断，保证信息内容的真实性；

(2)数据安全：保证数据在一个可信的环境中存储、传输，不会被非法修改，数据源头和目标不被否认；

(3)运行安全：保证系统正常运行，不会被非授权人恶意利用；

(4)实体安全：保护计算机设备、设施(含网络)及其他媒体免遭自然灾害及其他环境事故(包括电磁污染)破坏的措施、过程。实体安全是信息系统安全的前提。

另外一种观点基于信息安全属性，认为信息网络安全主要是指对信息和信息系统的机密性、完整性和可用性的保护。图 1-2 表示了这种安全框架。

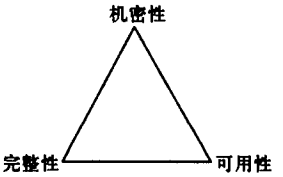


图 1-2　信息网络安全框架

①机密性(Confidentiality)：指保证关键信息和敏感信息不被非授权者获取、解析或恶意利用。

②完整性(Integrity)：指保证信息从真实的信源发往真实的信宿，在传输、存储过程中未被非法修改、替换、删除；信息完整性是网络信息安全的基本要求。破坏信息的完整性是影响网络信息安全的常用手段。

③可用性(Availability)：指保证信息和信息系统随时可为授权者提供服务而不被非授权者滥用和阻断。

具体地说：信息的机密性是针对信息被允许访问(Access)对象的多少而不同，所有人员都可以访问的信息为公开信息，需要限制访问的信息一般为敏感信息或秘密，秘密可以根据信息的重要性及保密要求分为不同的密级，例如国家根据秘密泄露对国家经济、安全利益产生的影响(后果)不同，将国家秘密分为秘密、机密和绝密三个等级，组织可根据其信息安全的实际，在符合《国家保密法》的前提下将其信息划分为不同的密级；对于具体的信息的保密性有时效性，如秘密到期解密等。

信息的完整性主要包括两方面，一方面是指信息在使用、传输、存储等过程中不被篡改、丢失或缺损等，另一方面是指信息处理的方法的正确性，不正当的操作，如误删除文件，有可能造成重要文件丢失。

信息的可用性是指信息及相关的信息资产在授权人需要的时候，可以立即获得。例如通信线路中断故障会造成信息在一段时间内不可用，影响正常的商业运作，这是信息可

用性的破坏。

不同类型的信息及相应资产的信息安全在保密性、完整性及可用性方面关注点不同，如组织的专有技术、市场营销计划等商业秘密对组织来讲保守机密尤其重要；对于工业自动控制系统，控制信息的完整性相对其保密性重要得多；而对于瞬息万变的金融证券市场来说，保证信息的可用性是用户的第一需求。

目前，人们又赋予了信息网络安全的第四和第五个特性：

可控性(Access Control)：即对信息、信息处理过程及信息系统本身都可以实施合法的安全监控和检测。如及时切断和可疑用户的对话连接。

不可否认性(Non－repudiation)：保证出现信息安全问题后可以有据可查，可以追踪责任到人或责任到事，又称信息的抗抵赖性。如电子邮件的数字签名。

概括地讲，信息网络安全的实质就是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，确保系统能连续可靠正常地运行，网络服务不中断。

因而信息网络安全的主要内容包括：

(1)了解网络系统受到的威胁及脆弱性，以便人们能注意到网络这些弱点和它存在的特殊性问题。

(2)如何从人、技术和政策(包括法律、法规等)三方面保护网络系统的各种资源，避免或减少自然或人为的破坏。

(3)开发和实施卓有成效的安全策略，尽可能减小网络系统所面临的各种风险。

(4)准备适当的应急计划，使网络系统中的设备、设施、软件和数据受到破坏和攻击后，能够尽快恢复工作。

(5)制定完备的安全管理措施，并定期检查这些安全措施的实施情况和有效性，从而保证数据信息的机密性、完整性、可用性、可控性和不可否认性。

1.1.2　保障信息网络安全的三大要素

进入 20 世纪 90 年代，信息网络系统的攻击事件日趋频繁，对信息及信息网络系统单纯的保护已不能满足安全的需要，人们需要对整个信息和信息系统进行全面防御，以确保整个信息网络的安全性。为此，美国国家安全局(NSA)在其发布的《信息保障技术框架》(ITF)中提出了深层防御(Defense in-depth)的安全设计思想。深层防御概念从宏观上提出了人、政策(包括法律、法规、制度、管理)和技术三大要素来构成宏观的信息网络安全保障体系结构的框架。由此看到，信息网络安全保障不仅仅是技术问题，而是人、政策和技术三大要素的结合。

人在最底层，是信息网络安全管理的根本。保障信息网络系统的安全性，既要靠先进的技术，又要有完善的管理，但其核心都是人，实际上，大部分安全和保密问题是由人为差错造成的，因此，在信息安全管理中人的因素应该是最重要的。它主要包括人员的岗位责任安全性明确、人事监督监测、安全保密协议、安全事件及隐患报告、安全教育与培训、安全奖惩制度等，另外，还要有和组织外部的合作者进行信息交流时的安全性规定。

技术是顶端的东西，但是技术是要通过人，通过相应的政策和策略去操作这个技术

的。

从技术层面上讲，任何一个用户的信息网络都可以从三个环节去考虑其安全，即主机（包括 PC 和服务器）、连接主机的网络设备以及应用和网络的边界，三个环节都安全了，整个信息系统才是安全的，如图 1-3 所示。同时采用信息安全保障框架（PDRR，保护、检测、反应和恢复）等综合安全手段。

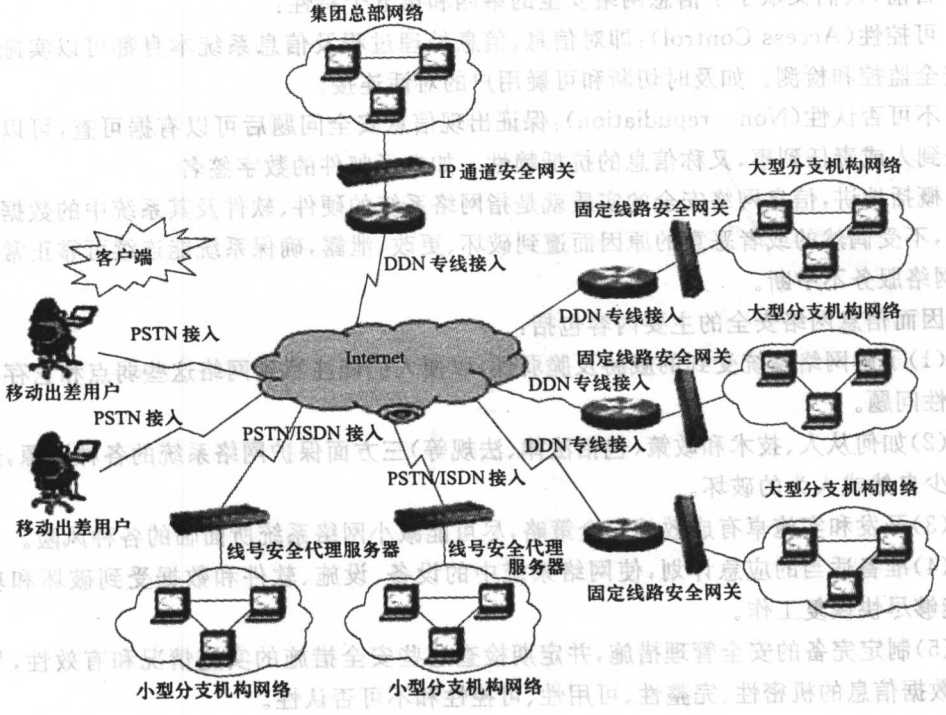


图 1-3　技术层面上信息网络安全的三个环节

图 1-4 给出了信息安全保障（PDRR）框架的模型。

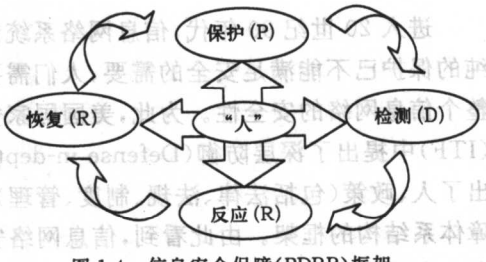


图 1-4　信息安全保障（PDRR）框架

保护（Protection），就是采用一切手段实现我们信息系统的机密性、完整性、可用性、可控性和不可否认性。我们国家已经提出来实行计算机信息系统的等级保护的问题，我们应该依据不同等级的系统安全要求来完善自己系统的安全功能、安全机制。

检测（Detection），就是利用高技术提供的工具来检查系统存在的，可能提供黑客攻击、白领犯罪、病毒泛滥等等这样一些脆弱性。

反应（Respond），就是对于危及安全的事件、行为、过程，及时做出响应的处理，杜绝危害进一步扩大，使得我们的系统力求提供正常的服务。

恢复（Restore），包括对自然灾害和人为破坏的数据恢复。例如：美国 9.11 后，有些

公司倒闭了，但是有的公司却能正常运转，这主要因为公司的运转机制有异地备份能够迅速地对灾难进行恢复。

现阶段，在该框架的指导下大多数信息网络系统采用的防御和检测技术有安装病毒防火墙、网络防火墙，进行入侵检测、行为审计，配置安全路由等。但是信息网络安全保障的关键是从系统工程的角度在总体上考虑安全问题，不仅在技术手段上统筹规划，建立一个被动防御与主动防御有机结合的技术保障体系，更重要的是在整个体系结构中，始终要坚持以“人”为本的思想，制定防范策略，加强教育、管理、立法等手段。

1.2　信息网络面临的威胁与自身的脆弱性

1.2.1　信息网络面临的威胁

信息网络面临的威胁主要来自：电磁泄露、雷击等环境安全构成的威胁，软硬件故障和工作人员误操作等人为或偶然事故构成的威胁，利用计算机实施盗窃、诈骗等违法犯罪活动的威胁，网络攻击和计算机病毒构成的威胁，以及信息战的威胁等，概括起来主要有以下几类：

(1)内部泄密和破坏：内部人员可能对信息网络形成的威胁包括：内部人员有意或无意泄密、更改记录信息；内部非授权人员有意偷窃机密信息、更改记录信息；内部人员破坏信息系统等。

(2)截收：网络攻击者可能通过搭线或在电磁波辐射范围内安装截收装置等方式，截获机密信息，或通过对信息流量和流向、通信频度和长度等参数的分析，推出有用信息。这种方式是过去军事对抗、政治对抗和当今经济对抗中最常采用的窃密方式，也是一种针对计算机通信网的被动攻击方式，它不破坏传输信息的内容，不易被察觉。

(3)非法访问：非法访问是指未经授权使用信息资源或以未授权的方式使用信息资源，它包括：非法用户(通常称为黑客)进入网络或系统，进行违法操作；合法用户以未授权的方式进行操作。

(4)破坏信息的完整性：网络攻击者可能从三个方面破坏信息的完整性：

①篡改——改变信息流的次序、时序、流向，更改信息的内容和形式；

②删除——删除某个消息或消息的某些部分；

③插入——在消息中插入一些信息，让接收方读不懂或接收错误的信息。

(5)冒充：网络攻击者可能进行的冒充行为包括：冒充领导发布命令、调阅密件；冒充主机欺骗合法主机及合法用户；冒充网络控制程序套取或修改使用权限、口令、密钥等信息，越权使用网络设备和资源；接管合法用户，欺骗系统，占用合法用户的资源。

(6)破坏系统的可用性：网络攻击者破坏计算机通信网的可用性：使合法用户不能正常访问网络资源；使有严格时间要求的服务不能及时得到响应；摧毁系统等。

(7)重演：重演指的是攻击者截收并录制信息，然后在必要的时候重发或反复发送这些信息。例如，一个实体可以重发含有另一个实体鉴别信息的消息，以证明自己是该实体，达到冒充的目的。

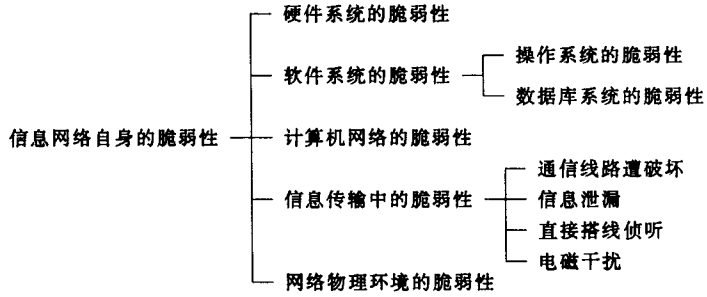
(8)抵赖:可能出现的抵赖行为包括:发送信息者事后否认曾经发送过某条消息;发送信息者事后否认曾经发送过某条消息的内容;接收信息者事后否认曾经收到过某条消息;接收信息者事后否认曾经收到过某条消息的内容。

(9)其他威胁:对计算机通信网的威胁还包括计算机病毒、电磁泄漏、各种灾害、操作失误等。

1.2.2 信息网络自身的脆弱性

脆弱性主要指网络系统和设备、计算机软硬件在设计时由于考虑不周等留下的缺陷,容易被威胁主体所利用从而危害系统的正常运行。

由于信息网络分布的广域性、网络体系结构的开放性、信息资源的共享性和通信信道的共用性,因而信息网络自身存在很多严重的脆弱点,成为网络安全的隐患,为攻击型的威胁提供了可乘之机。



归纳起来,信息网络自身的脆弱性主要包括:

(1)计算机硬件系统的脆弱性:电源掉电、电磁干扰以及硬件设计缺陷等,在其他方面如磁盘高密度存储受到损坏造成大量信息的丢失,存储介质中的残留信息泄密等。

(2)计算机软件系统的脆弱性:包括信息网络自身在操作系统、数据库管理系统以及通信协议等存在安全漏洞和隐蔽信道等不安全因素。

(3)计算机网络的脆弱性:TCP/IP 协议本身开放性带来的脆弱性。

(4)信息传输中的脆弱性:在信息输入、处理、传输、存储、输出过程中存在的信息容易被篡改、伪造、破坏、窃取、泄漏等不安全因素。

(5)网络物理环境:包括自然灾害和一般物理环境。比如火灾和洪水;机房的安全门、人员出入机房规定等。物理环境安全保护的范围,不仅包括计算机设备和传输线路,也包括一切可以移动的物品,比如打印数据的打印纸和装有数据、程序的磁盘、未经处理的电子废弃物等。

另外,网络安全的脆弱性和网络的规模有密切关系。网络规模越大,其安全的脆弱性越大。资源共享与网络安全是相对矛盾的,随着网络的发展,资源共享加强,安全问题会越加严重。