XIANDAI
XINXI ANQUAN YUANLI
YU YINGYONG YANJIU

现代信息安全原理与应用研究

主 编 黄丽芬 张秀荣 孙 荣

中国商务出版社
CHINA COMMERCE AND TRADE PRESS

XIANDAI
XINXI ANQUAN YUANLI
YU YINGYONG YANJIU

现代信息安全原理与应用研究

主　编　黄丽芬　张秀荣　孙　荣
副主编　刘　夏　李　刚　李筱锋
　　陈谊楠　杨　媛

中国商务出版社
CHINA COMMERCE AND TRADE PRESS

图书在版编目(CIP)数据

现代信息安全原理与应用研究/黄丽芬，张秀荣，孙荣主编. --北京：中国商务出版社，2012.3

ISBN 978-7-5103-0665-5

Ⅰ. ①现… Ⅱ. ①黄…②张…③孙… Ⅲ. ①信息安全一研究 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字(2012)第 046248 号

现代信息安全原理与应用研究

XIANDAI XINXI ANQUAN YUANLI YU YINGYONG YANJIU

黄丽芬 张秀荣 孙荣 主编

出　版：中国商务出版社出版
发　行：北京中商图出版物发行有限责任公司
社　址：北京市东城区安定门外大街东后巷 28 号
邮　编：100710
电　话：010－64269744(编辑室)
　　010－64283818(发行部)
网　址：www.cctpress.com
邮　箱：cctp@cctpress.com
照　排：北京鑫海胜蓝数码科技有限公司
印　刷：北京鑫海胜蓝数码科技有限公司
开　本：787 毫米×1092 毫米　1/16
印　张：25.375　　**字　数**：649 千字
版　本：2012 年 3 月第 1 版　　2012 年 3 月第 1 次印刷

书　号：ISBN 978-7-5103-0665-5
定　价：36.00 元

前　言

进入21世纪以来，信息已成为社会发展的重要战略资源，社会信息化已成为当今发展的潮流与核心。随着国民经济信息化进程的不断推进，各行各业对计算机网络的依赖程度日益增强，这种高度依赖性，使得社会变得十分脆弱。一旦计算机网络受到攻击，则整个社会将陷入危机之中，因此就需要加强对网络信息安全知识的普及。总之，信息安全问题已成为关系国家安全、经济发展与社会稳定的关键性问题，也是计算机领域探讨与研究的热点问题之一。

从学科研究的角度来看，信息安全是一门综合性强、交叉性广的学科领域，涉及计算机科学、网络技术、通信技术、密码技术、信息处理技术、应用数学等多学科的知识。同时，信息安全技术也是一门实践性较强的学科，其许多技能都是从实践中得来的。因此，系统的掌握信息安全原理与应用就显得尤为重要。

全书分为11章，主要内容介绍如下：

第1章对信息安全的相关知识进行了论述。

第2章对密码技术进行了综述，介绍了对称密码技术、非对称密码技术、Hash算法、密钥分配与管理技术以及数字签名与认证技术等。

第3～7章介绍了安全保障技术。第3章介绍了信息隐藏与数字水印技术；第4章对防火墙与入侵检测技术进行了较为详细的介绍；第5章介绍了虚拟专用网(VPN)技术，并在最后对其发展趋势进行了展望；第6章分别介绍了访问控制与安全审计技术；第7章介绍了计算机病毒与恶意代码，并对其防范措施进行了逐一的介绍。

第8、9章分别探讨了系统安全机制和应用安全机制。第8章分别从操作系统和数据库系统两个方面对系统安全机制进行了研究；第9章则从三个方面讨论了应用安全机制，即Web站点安全、电子邮件安全和电子商务安全。

第10章对数据备份与恢复相关知识进行了介绍，主要包括数据备份策略、灾难恢复技术以及常用工具的介绍等。

第11章从管理原则、管理技术和法律法规等方面对信息安全管理进行了讨论，最后并介绍了信息安全评估标准。

全书由黄丽芬、张秀荣、孙荣担任主编，刘夏、李刚、李筱锋、陈谊楠、杨媛担任副主编，并由黄丽芬、张秀荣、孙荣负责统稿。其具体分工如下：

第3章、第8章、第10章第3节～第4节、第11章第2节～第3节：黄丽芬(广西工业职业技术学院)；

第7章、第9章第1节～第2节：张秀荣(内蒙古民族大学)；

第1章第1节～第4节、第2章：孙荣(黑河学院)；

第1章第5节、第6章：刘夏(三亚航空旅游职业学院)；

第 4 章第 1 节～第 3 节、第 5 章：李刚（平顶山学院）；

第 9 章第 3 节、第 10 章第 1 节～第 2 节：李筱锋（大庆职业学院）；

第 1 章第 6 节、第 4 章第 4 节～第 5 节、第 11 章第 4 节～第 5 节：陈谊楠（三亚航空旅游职业学院）；

第 4 章第 6 节～第 7 节、第 11 章第 1 节：杨媛（宁夏师范学院）。

本书在编写过程中，参考了大量有价值的文献与资料，在此向这些文献的作者表示敬意。由于信息安全技术发展的日新月异，加之编者的学识和水平有限，书中难免错误和疏漏，恳请各位专家和读者给予批评指正。

编　者

2011 年 12 月

目　录

第 1 章　绪论 …… 1

1.1　信息与信息安全 …… 1
1.2　信息安全的研究内容 …… 4
1.3　信息安全威胁 …… 9
1.4　信息安全策略与机制 …… 11
1.5　信息安全体系结构 …… 16
1.6　信息安全与法律 …… 18

第 2 章　密码技术 …… 20

2.1　密码技术概述 …… 20
2.2　对称密码技术 …… 21
2.3　非对称密码技术 …… 42
2.4　Hash 算法 …… 46
2.5　密钥分配与管理技术 …… 52
2.6　数字签名与认证技术 …… 61
2.7　密码技术的应用研究 …… 65

第 3 章　信息隐藏与数字水印 …… 69

3.1　信息隐藏技术 …… 69
3.2　数字水印概述 …… 83
3.3　数字图像水印技术 …… 89
3.4　数字语音水印技术 …… 93
3.5　数字视频和文本水印技术 …… 96

第 4 章　防火墙与入侵检测 …… 105

4.1　防火墙概述 …… 105
4.2　防火墙技术 …… 113
4.3　防火墙的体系结构 …… 120
4.4　防火墙选择原则与常见产品 …… 123
4.5　入侵检测概述 …… 127

4.6 入侵检测技术 …… 134
4.7 入侵检测系统存在的问题及其发展方向 …… 143

第5章 虚拟专用网(VPN) …… 146

5.1 虚拟专用网概述 …… 146
5.2 虚拟专用网的实现技术 …… 151
5.3 隧道协议 …… 153
5.4 MLPS VPN 技术 …… 157
5.5 虚拟专用网的发展趋势 …… 159

第6章 访问控制与安全审计 …… 160

6.1 访问控制概述 …… 160
6.2 访问控制模型 …… 164
6.3 访问控制的安全策略 …… 176
6.4 安全审计技术 …… 179

第7章 计算机病毒与恶意代码 …… 191

7.1 计算机病毒概述 …… 191
7.2 计算机病毒的特征与分类 …… 196
7.3 计算机病毒的工作原理 …… 203
7.4 计算机病毒的检测与防治 …… 208
7.5 反病毒技术 …… 215
7.6 特洛伊木马 …… 219
7.7 网络蠕虫 …… 228

第8章 系统安全机制 …… 233

8.1 操作系统安全概述 …… 233
8.2 主流操作系统的安全机制 …… 237
8.3 数据库系统安全概述 …… 248
8.4 数据库加密 …… 253
8.5 主流数据库系统的安全机制 …… 259

第9章 应用安全机制 …… 272

9.1 Web 站点安全 …… 272
9.2 电子邮件安全 …… 284
9.3 电子商务安全 …… 306

第10章 数据备份与恢复 …… 330

10.1 数据备份概述 …… 330

10.2 数据备份策略…… 334
10.3 灾难恢复技术…… 338
10.4 数据备份与恢复的常用工具…… 342

第 11 章 信息安全管理与评估标准 …… 355

11.1 信息安全管理概述…… 355
11.2 信息安全策略管理…… 375
11.3 信息安全风险管理…… 376
11.4 信息安全立法管理…… 378
11.5 信息安全评估标准…… 384

参考文献…… 397

第1章 绪 论

1.1 信息与信息安全

1.1.1 信息概述

21世纪是信息的世纪，随着信息量的急剧增加和各种信息词汇的不断涌现，人类仿佛置身于信息的海洋当中。信息、信息时代、信息技术、信息化、信息系统、信息资源、信息管理、经济信息、市场信息、价格信息等各类名词术语，随时随地向我们迎面扑来。

那么，就是什么才是信息呢？在人类社会的早期，人们对信息的认识比较肤浅和模糊，对信息的含义没有明确的定义。到了20世纪，随着科学技术的发展，特别是信息科学技术的发展，对人类社会产生了深刻的影响，迫使人们开始探讨信息的准确含义。

1928年哈特莱(L. V. R. Hartley)在《贝尔系统技术杂志》(BSTJ)上发表了一篇题为“信息传输”的论文，文中他认为信息是选择通信符号的方式，且用选择自由度来计量这种信息的大小。1948年，美国数学家香农(C. E. Shannon)在《贝尔系统技术杂志》上发表了一篇题为“通信的数据理论”的论文，文中他认为信息是用来减少随机不定性的东西。就在香农创立信息论的同年，维纳(N. Wiener)出版了《控制论：动物和机器中的通信与控制问题》，他认为信息是人们在适应外部世界和这种适应反作用于外部世界的过程中，与外部世界进行互相交换的内容的名称，并创建了控制论。1975年，意大利学者朗高(G. Longo)在《信息论：新的趋势与未决问题》一书中认为信息反映了事物的形式、关系和差别，它包含在事物的差异之中，而不在事物本身。到了1988年，我国信息论专家钟义信教授在《信息科学原理》一书中，把信息定义为：事物的运动状态和状态变化的方式，并通过引入约束条件推导了信息的概念体系，对信息进行了完整和准确的描述。信息的这个定义具有最大的普遍性，不仅涵盖所有其他的信息定义，而且通过引入约束条件还能转化为所有其他的信息定义。

信息不同于消息，消息是信息的外壳，信息则是消息的内核，也可以说消息是信息的笼统概念，信息则是消息的精确概念；信息不同于信号，信号是信息的载体，信息则是信号所载荷的内容；信息不同于数据，数据是记录信息的一种形式，同样的信息也可以用文字或图像来表述，当然，在计算机里，所有的多媒体文件都是用数据表示的，计算机和网络上信息的传递都是以数据的形式进行，此时信息等同于数据。信息也不同于知识，知识是由信息抽象出来的产物，是一种具有普遍和概括性的。综上所述，一般意义上的信息可以定义为：信息是事物运动的状态和状态

变化的方式。

信息有许多重要的特征，但信息最基本的特征是信息来源于物质，又不是物质本身；它从物质的运动中产生出来，又可以脱离源物质而寄生于媒体物质，相对独立地存在。信息是“事物运动的状态与状态变化的方式”，但“事物运动的状态与状态变化的方式”并不是物质本身，信息不等于物质。

信息其他的基本特征还有下列几点。

信息也来源于精神世界。既然信息是事物运动的状态与状态变化的方式，那么精神领域的事物运动（思维的过程）当然可以成为信息的一个来源。同客观物体所产生的信息一样，精神领域的信息也具有相对独立性，可以被记录下来加以保存。

信息与能量息息相关，传输信息或处理信息总需要一定的能量来支持，而控制和利用能量总需要有信息来引导。但是信息与能量又有本质的区别，即信息是事物运动的状态和状态变化的方式，能量是事物做功的本领，提供的是动力。

信息是具体的并可以被人（生物、机器等）所感知、提取、识别，可以被传递、储存、变换、处理、显示、检索、复制和共享。

正是由于信息可以脱离源物质而载荷于媒体物质，可以被无限制地进行复制和传播，因此，信息可为众多用户所共享。

因此，信息具有下列一些性质：传递性、真伪性、可识别性、相对性、知识性、效用性、共享性、载体的可变性、普遍性、无限性。

1.1.2 信息安全概述

随着现代通信技术的迅速发展和普及，特别是随着通信与计算机相结合而诞生的计算机互联网络全面进入千家万户，信息的应用与共享日益广泛，且更为深入。世界范围的信息革命激发了人类历史上最活跃的生产力，人类开始从主要依赖物质和能源的社会步入物质、能源和信息三位一体的社会。各种信息化系统已成为国家基础设施，支撑着电子政务、电子商务、电子金融、科学研究、网络教育、能源、通信、交通和社会保障等方方面面，信息成为人类社会必需的重要资源。

与此同时，信息的安全问题日渐突出，情况也越来越复杂。从大的方面来说，信息安全问题已威胁到国家的政治、经济、军事、文化、意识形态等领域，因此，很早就有人提出了“信息战”的概念并将信息武器列为继原子武器、生物武器、化学武器之后的第四大武器。从小的方面来说，信息安全问题也涉及人们能否保护个人的隐私。

信息安全已成为社会安全稳定的必要前提条件。

信息安全，即关注信息本身的安全，以防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠或无法处理等问题，使得我们在最大限度地利用信息为我们服务的同时而不招致损失或使损失最小。

信息安全关注的目标主要是保护信息的机密性、完整性、抗否认性和可用性；也有观点认为是机密性、完整性和可用性，即 CIA。

（1）机密性（confidentiality）

机密性是指保证信息不被非授权访问，即使非授权用户得到信息也无法知晓信息内容，因而不能使用。通常通过访问控制阻止非授权用户获得机密信息，通过加密变换阻止非授权用户获

知信息内容。

(2)完整性(integrity)

完整性是指维护信息的一致性,即信息在生成、传输、存储和使用过程中不应发生人为或非人为的非授权篡改。一般通过访问控制阻止篡改行为,同时通过消息摘要算法来检验信息是否被篡改。

(3)可用性(availability)

可用性是指保障信息资源随时可提供服务的特性,即授权用户根据需要可以随时访问所需信息。可用性是信息资源服务功能和性能可靠性的度量,涉及物理、网络、系统、数据、应用和用户等多方面的因素,是对信息网络总体可靠性的要求。

除上述的三个属性外,信息安全的基本属性还有不可否认性和可控性。

(1)不可否认性

不可否认性也称为不可抵赖性,即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。发送方不能否认已发送的信息,接收方也不能否认已收到的信息。

(2)可控性

可控性是指对信息的传播及内容具有控制能力的特性。授权机构可以随时控制信息的机密性,能够对信息实施安全监控。

信息安全的任务就是要实现信息的上述5种安全属性。对于攻击者来说,就是要通过一切可能的方法和手段破坏信息的安全属性。

其中机密性、完整性和可用性是信息安全的核心三要素,同理,它们也构成了数据库安全的核心三要素。目前,数据库安全除了保障三个核心要素以外,对于不可否认性、可控性也不断提出越来越多、越来越具体的要求,是研究和应用的重要突破口。总体而言,信息安全五要素采用较为抽象的方式勾勒出数据库安全的基本轮廓,为深入探讨数据库安全机制、安全月艮务等内容提供了基本框架。

近年来,人们也在不断扩展信息安全的内涵,提出了信息安全另外一些“应该”具备的特征,这些属性要素包括鉴别性、实用性、占有性、可审计性、可存活性、免疫性,等等。我们认为,这些属性深入刻画了信息安全的功能特性,可以看做体现了传统信息安全五要素的动态组合、智能演化和专门化。

例如,鉴别性(Authentication)意味着信息和信息传输的可信程度,可以解释为信息的完整性,信息发送者和接收者身份的完整性。实用性(Utility)意味着适于一些特定的目标,有能力满足特定的功能,例如,加密密钥不可丢失,可以解释为机密性、可用性和可控性。占有性(Possession)意味着防止信息载体、版权、专利被盗用和侵权使用,可以解释为可用性和可控性。可审计性(Audit)意味着在记录跟踪系统行为的基础上实现安全分析、评价、审查、调整,可以解释为不可否认性和可控性。可存活性(Survivability)意味着系统在遭受攻击或者错误的情况下继续提供核心服务并及时恢复全部服务,可以解释为可用性。免疫性(Immunity)意味着从仿生计算角度出发,通过模拟人体免疫系统自组织、自适应、记忆和鲁棒等特性解决安全问题,可以解释为可控性和可用性。目前,对于这些特性的研究和应用已经发展成为不同的专门方向。

信息安全可以说是一门既古老又年轻的学科,内涵极其丰富。信息安全不仅涉及计算机和网络本身的技术问题、管理问题,而且还涉及法律学、犯罪学、心理学、经济学、应用数学、计算机基础科学、计算机病毒学、密码学等学科。

从信息安全的发展过程来看，在计算机出现以前，通信安全以保密为主，密码学是信息安全的核心和基础。随着计算机的出现，计算机系统安全保密成为现代信息安全的重要内容。网络的出现使得大范围的信息系统的安全保密成为信息安全的主要内容。信息安全的宗旨是向合法的服务对象提供准确、正确、及时、可靠的信息服务；而对其他任何人员和组织，包括内部、外部乃至于敌对方，保持最大限度的信息的不透明性、不可获取性、不可接触性、不可干扰性、不可破坏性，而且不论信息所处的状态是静态的、动态的还是传输过程中的。

1.2 信息安全的研究内容

1.2.1 信息安全研究概述

信息安全是一门新兴学科，它除了涉及数学、通信、计算机等自然科学多方面的理论和应用知识外，还涉及法律、心理学等社会科学。但是，狭义上的信息安全只是从自然科学的角度研究信息安全。

虽然，现阶段关于信息安全的具体特征的标志尚无统一的界定标准。但在现阶段，信息安全研究大致可以分为基础理论研究、应用技术研究、安全管理研究等几方面的内容。基础理论研究包括密码研究、安全理论研究；应用技术研究包括安全实现技术、安全平台技术研究；安全管理研究包括安全标准、安全策略、安全测评等。各部分研究内容及相互关系如图 1-1 所示。

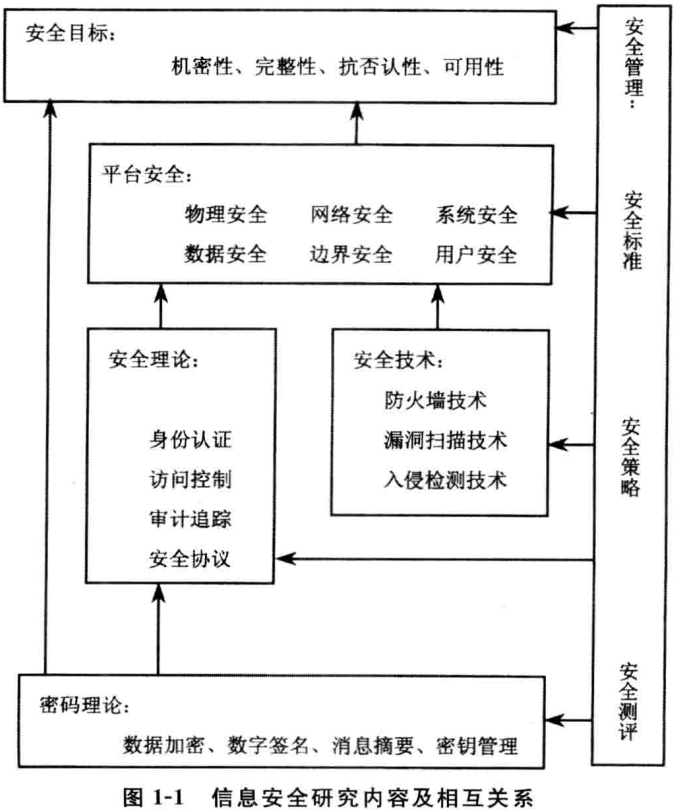

图 1-1 信息安全研究内容及相互关系

而通常对信息安全的研究从总体上又可以分为5个层次的研究，即安全的密码算法、安全协议、网络安全、系统安全以及应用安全等，其层次结构如图1-2所示。

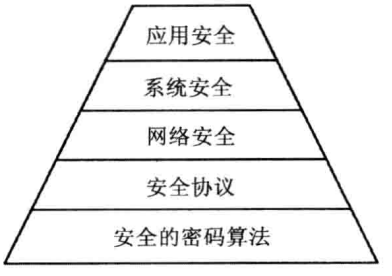

图1-2 信息安全的层次

1.2.2 信息安全基础研究

信息安全基础研究的主要内容包括密码学研究和网络信息安全基础理论研究。如图1-1所示，密码理论主要包括数据加密、数字签名、消息摘要、密钥管理等内容；安全理论主要包括身份认证、访问控制、审计追踪、安全协议等内容。

1. *密码理论*

密码理论是信息安全的基础，信息安全的机密性、完整性和抗否认性都依赖于密码算法。通过加密可以保护信息的机密性；通过信息摘要可以检测信息的完整性；通过数字签名可以保护信息的抗否认性。加密变换需要密钥参与，因而密钥管理也是十分重要的研究内容。因此，密码学的主要研究内容是加密算法、消息摘要算法、数字签名算法以及密钥管理。

(1)数据加密

数据加密算法是一种数学变换，在选定参数(密钥)的参与下，将信息从易于理解的明文加密为不易理解的密文，同时也可以将密文解密为明文。加、解密时用的密钥可以相同，也可以不同。加、解密密钥相同的算法称为对称算法，典型的算法有DES、AES等；加、解密密钥不同的算法称为非对称算法，通常一个密钥公开，另一个密钥私藏，因而也称为公钥算法。典型的算法有RSA、ECC等。

(2)数字签名

数字签名机制主要决定于签名和验证两个过程。签名过程是利用签名者的私有信息作为密钥，或对数据单元进行加密，或产生该数据单元的密码校验值；验证过程是利用公开的规程和信息来确定签名是否是利用该签名者的私有信息产生的。

数字签名主要是消息摘要和非对称加密算法的组合应用。从原理上讲，通过私有密钥用非对称算法对信息本身进行加密，即可实现数字签名功能。用私钥加密只能用公钥解密，使得接受者可以解密信息，但无法生成用公钥解密的密文，从而证明此密文肯定是拥有加密私钥的用户所为，因而是不可否认的。实际实现时，由于非对称算法加/解密速度很慢，通常先计算消息摘要，再用非对称加密算法对消息摘要进行加密而获得数字签名。

(3)消息摘要

消息摘要算法也是一种数学变换，通常是单向(不可逆)的变换，它将不定长度的信息变换为

固定长度(如 16 字节)的摘要,信息的任何改变(即使是 1bit)也能引起摘要面目全非,因而可以通过消息摘要检测消息是否被篡改。典型的算法有 MD5、SHA 等。

(4)密钥管理

密码算法是可以公开的,但密钥必须严格保护。如果非授权用户获得加密算法和密钥,则很容易破解或伪造密文,加密也就失去了意义。密钥管理研究就是研究密钥的产生、发放、存储、更换和销毁的算法与协议等。

2. 安全理论

(1)身份认证

身份认证是指验证用户身份与其所声称的身份是否一致的过程。最常见的身份认证是口令认证。口令认证是在用户注册时记录下其用户名和口令,在用户请求服务时出示用户名和口令,通过比较其出示的用户名和口令与注册时记录下的是否一致来鉴别身份的真伪。复杂的身份认证则需要基于可信的第三方权威认证机构的保证和复杂的密码协议来支持,如基于证书认证中心和公钥算法的认证等。身份认证研究的主要内容包括认证的特征,如知识、推理、生物特征等和认证的可信协议及模型。

(2)授权和访问控制

授权和访问控制是两个关系密切的概念,经常替换使用。授权侧重于强调用户拥有什么样的访问权限,这种权限是系统预先设定的,并不关心用户是否发起访问请求;而访问控制是对用户访问行为进行控制,它将用户的访问行为控制在授权允许的范围之内,因此,也可以说,访问控制是在用户发起访问请求时才起作用的。打个形象的比喻,授权是签发通行证,而访问控制则是卫兵,前者规定用户是否有权出入某个区域,而后者检查用户在出入时是否超越了禁区。授权和访问控制研究的主要内容是授权策略、访问控制模型、大规模系统的快速访问控制算法等。

(3)审计追踪

审计和追踪也是两个关系密切的概念。审计是指对用户的行为进行记录、分析和审查,以确认操作的历史行为。追踪有追查的意思,通过审计结果追查用户的全程行踪。审计通常只在某个系统内进行,而追踪则需要对多个系统的审计结果综合分析。审计追踪研究的主要内容是审计素材的记录方式、审计模型及追踪算法等。

(4)安全协议

安全协议指构建安全平台时所使用的与安全防护有关的协议,是各种安全技术和策略具体实现时共同遵循的规定,如安全传输协议、安全认证协议、安全保密协议等。典型的安全协议有网络层安全协议 IPSec、传输层安全协议 SSL、应用层安全电子商务协议 SET 等。安全协议研究的主要内容是协议的内容和实现层次、协议自身的安全性、协议的互操作性等。

1.2.3 信息安全应用研究

信息安全的应用研究是针对信息在应用环境下的安全保护而提出的,是信息安全基础理论的具体应用,它包括安全技术研究和平台安全研究。如图 1-1 所示,安全技术中包括防火墙技术、漏洞扫描技术、入侵检测技术和防病毒技术等;平台安全研究包括物理安全、网络安全、系统安全、数据安全、边界安全以及用户安全等。

1. 安全技术

(1)防火墙技术

防火墙技术是一种安全隔离技术,它通过在两个安全策略不同的域之间设置防火墙来控制两个域之间的互访行为。防火墙技术的主要研究内容包括防火墙的安全策略、实现模式、强度分析等。

(2)漏洞扫描技术

漏洞扫描是针对特定信息网络中存在的漏洞而进行的。信息网络中无论是主机还是网络设备都可能存在安全隐患,有些是系统设计时考虑不周而留下的,有些是系统建设时出现的。这些漏洞很容易被攻击,从而危及信息网络的安全。由于安全漏洞大多是非人为的、隐蔽的,因此,必须定期扫描检查、修补加固。操作系统经常出现的补丁模块就是为加固发现的漏洞而开发的。由于漏洞扫描技术很难自动分析系统的设计和实现,因此很难发现未知漏洞。对于未知的漏洞,目前主要是通过专门的漏洞分析技术来完成的,如逆向工程等。漏洞扫描技术研究的主要内容包括漏洞的发现、特征分析以及定位、扫描方式和协议等。

(3)入侵检测技术

入侵检测是通过计算机网络系统中的若干关键结点收集信息,并分析这些信息,监控网络中是否有违反安全策略的行为或者是否存在入侵行为,是对向计算机和网络资源的恶意行为的识别和响应过程。目前主要有基于用户行为模式、系统行为模式和入侵特征的检测等。在实现时,可以只检测针对某主机的访问行为,也可以检测针对整个网络的访问行为,前者称为基于主机的入侵检测,后者称为基于网络的入侵检测。入侵检测技术研究的主要内容包括信息流提取技术、入侵特征分析技术、入侵行为模式分析技术、入侵行为关联分析技术和高速信息流快速分析技术等。

(4)防病毒技术

病毒是一种具有传染性和破坏性的计算机程序。随着 Internet 的普及,计算机病毒的传播速度大大加快,破坏力也在增强,出现了智能病毒、远程控制病毒等。因此,研究和防范计算机病毒也是信息安全的一个重要方面。病毒防范研究的重点包括病毒的作用机理、病毒的特征、病毒的传播模式、病毒的破坏力、病毒的扫描和清除等。

2. 平台安全

(1)物理安全

物理安全是指保障信息网络物理设备不受物理损坏,或损坏时能及时修复或替换。通常是针对设备的自然损坏、人为破坏或灾害损坏而提出的。目前常见的物理安全技术有备份技术、安全加固技术、安全设计技术等。例如,保护 CA 认证中心,采用多层安全门和隔离墙,核心密码部件还要用防火墙、防盗柜保护。

(2)网络安全

网络安全的目标是防止针对网络平台的实现和访问模式的安全威胁。主要包括安全隧道技术、网络协议脆弱性分析技术、安全路由技术、安全 IP 协议等。

(3)系统安全

系统安全是各种应用程序的基础。系统安全关心的主要问题是操作系统自身的安全性问

题。信息的安全措施是建立在操作系统之上的，如果操作系统自身存在漏洞或隐蔽通道，就有可能使用户的访问绕过安全机制，使安全措施形同虚设。因此，系统自身的安全性非常重要。现在商用操作系统自身的安全级别都不高，并且存在大量漏洞，研究系统安全就更为重要。系统安全研究的主要内容包括安全操作系统的模型和实现、操作系统的安全加固、操作系统的脆弱性分析、操作系统与其他开发平台的安全关系等。

(4)数据安全

数据安全主要关心数据在存储和应用过程中是否会被非授权用户有意破坏，或被授权用户无意破坏。数据通常以数据库或文件形式来存储，因此，数据安全主要是数据库或数据文件的安全问题。数据库系统或数据文件系统在管理数据时采取什么样的认证、授权、访问控制及审计等安全机制，达到什么安全等级，机密数据能否被加密存储等，都是数据的安全问题。数据安全研究的主要内容有安全数据库系统、数据存取安全策略和实现方式等。

(5)边界安全

边界安全关心的是不同安全策略的区域边界连接的安全问题。不同的安全域具有不同的安全策略。边界安全研究的主要内容是安全边界防护协议和模型、不同安全策略的连接关系问题、信息从高安全域流向低安全域的保密问题、安全边界的审计问题等。

(6)用户安全

用户安全一方面指合法用户的权限是否被正确授权，是否有越权访问，是否只有授权用户才能使用系统资源，如一个普通的合法用户可能被授予了管理员的身份和权限。另一方面指被授权的用户是否获得了必要的访问权限，是否存在多业务系统的授权矛盾等。用户安全研究的主要内容包括用户账户管理、用户登录模式、用户权限管理、用户的角色管理等。

1.2.4 信息安全管理研究

1. 安全标准研究

安全标准研究是推进安全技术和产品标准化、规范化的基础。主要的标准化组织都推出了安全标准，著名的安全标准有可信计算机系统的评估准则(TCSEC)、通用准则(CC)、安全管理标准 ISO17799 等。安全标准给出了技术发展、产品研制、安全测评、方案设计等多方面的技术依据。如 TCSEC 将安全划分为 7 个等级，并从技术、文档、保障等方面规定了各个安全等级的要求。安全标准研究的主要内容包括安全等级划分标准、安全技术操作标准、安全体系结构标准、安全产品测评标准和安全工程实施标准等。

2. 安全策略研究

安全策略是安全系统设计、实施、管理和评估的依据。它针对具体的信息和网络的安全，决定应保护哪些资源，花费多大代价，采取什么措施，达到什么样的安全强度等。不同的国家和单位针对不同的应用都应制定相应的安全策略。例如，什么级别的信息应该采取什么保护强度，针对不同级别的风险能承受什么样的代价，这些问题都应该制定策略。安全策略研究的内容包括安全风险的评估、安全代价的评估、安全机制的制定以及安全措施的实施和管理等。

3. 安全测评研究

安全测评是依据安全标准对安全产品或信息系统进行安全性评定。目前开展的测评有技术评测机构开展的技术测评，也有安全主管部门开展的市场准入测评。测评包括功能测评、性能测评、安全性测评、安全等级测评等。安全测评研究的内容有测评模型、测评方法、测评工具、测评规程等。

1.3 信息安全威胁

所谓信息安全威胁，是指某人、物、事件、方法或概念等因素对某信息资源或系统的安全使用可能造成的危害。通常把可能威胁信息安全的行为称为攻击。虽然人为因素和非人为因素都可以对通信安全构成威胁，但是精心设计的人为攻击威胁最大。

目前还没有统一的方法来对各种威胁进行分类，也没有统一的方法来对各种威胁加以区别。信息安全所面临的威胁与环境密切相关，不同威胁的存在及程度是随环境的变化而变化的。常见的信息安全威胁有以下几类。

(1)信息泄露。指信息被泄露给未授权的实体(如人、进程或系统)，泄露的形式主要包括窃听、截收、侧信道攻击和人员疏忽等。

(2)篡改。指攻击者可能改动原来的信息内容，但信息的使用者并不能识别出被篡改的事实。

(3)重放。指攻击者可能截获并存储合法的通信数据，然后出于非法的目的重新发送它们，而接收者可能仍然进行正常的受理，从而被攻击者所利用。

(4)拒绝服务。对信息或其他资源的合法访问被无条件地阻止。

(5)假冒。指一个人或系统谎称是另一个人或系统，但信息系统或其管理者可能并不能识别，这可能使得谎称者获得了不该获得的权限。黑客大多采用假冒攻击。

(6)否认。指参与某次通信或信息处理的一方事后可能否认这次通信或相关的信息处理曾经发生过，这可能使得这类通信或信息处理的参与者不承担应有的责任。

(7)非授权使用。也称非法使用，指信息资源被某个未授权的人或系统使用，同时也包括被越权使用的情况。

(8)网络与系统攻击。攻击者可能利用网络与主机系统存在的设计或实现上的漏洞进行恶意的侵入和破坏，或者攻击者仅通过对某一信息服务资源进行超负荷的使用或干扰，使系统不能正常工作，后面一类攻击一般被称为拒绝服务攻击(DoS)。

(9)窃听。用各种可能的合法或非法的手段窃取系统中的信息资源和敏感信息。例如，对通信线路中传输的信号进行搭线监听，或利用通信设备在工作过程中产生的电磁泄漏截取有用信息等。

(10)授权侵犯。被授权以某一目的使用某一系统或资源的某个人，却将此权限用于其他非授权的目的，也称为“内部攻击”。

(11)业务流分析。通过对系统进行长期监听，利用统计分析方法对诸如通信频度、通行的信息流向、通信总量的变化等参数进行研究，从而发现有价值的信息和规律。