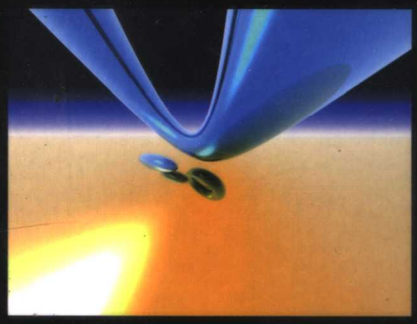
21世纪高等院校
信息安全系列规划教材

信息安全概论

徐茂智　邹维　编著



人民邮电出版社
POSTS & TELECOM PRESS

图书在版编目（CIP）数据

信息安全概论 / 徐茂智，邹维编著. —北京：人民邮电出版社，2007.8
（21 世纪高等院校信息安全系列规划教材）
ISBN 978-7-115-15979-3

Ⅰ. 信… Ⅱ. ①徐…②邹… Ⅲ. 信息系统—安全技术—高等学校—教材 Ⅳ. TP309

中国版本图书馆 CIP 数据核字（2006）第 037110 号

内 容 提 要

本书系统介绍信息安全的基本概念、基础理论和前沿技术知识。全书分为 10 章，从信息安全基本概念和技术体系出发，先介绍密码保护、身份识别、访问控制为核心的数据安全理论，再围绕网络安全、系统安全、应用安全、安全审计介绍信息安全中涉及的保护、检测和恢复技术，最后介绍信息安全评估与工程实现。本书注重知识的系统性和覆盖面的宽泛性，而且部分内容有一定深度。

本书可作为信息安全、数学、计算机、微电子专业的研究生和本科生教材，也可作为相关专业的工程技术人员的参考书。

21 世纪高等院校信息安全系列规划教材

信息安全概论

◆ 编　　著　徐茂智　邹　维
责任编辑　张　鑫

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京通州大中印刷厂印刷
新华书店总店北京发行所经销

◆ 开本：787×1092　1/16
印张：15.75
字数：376 千字　　2007 年 8 月第 1 版
印数：1－3 000 册　　2007 年 8 月北京第 1 次印刷

ISBN 978-7-115-15979-3/TP

定价：24.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223

总 序

一、出版背景

随着计算机技术与网络通信技术以及信息产业的高速发展，接入 Internet 的个人和单位主机数量快速增长，尤其是计算机在政府、国防、金融、公安和商业等部门的广泛应用，社会对计算机的依赖越来越大，而计算机系统的安全一旦受到破坏，不仅会导致严重的社会混乱，也会带来巨大的经济损失。世界主要发达国家每年因计算机犯罪所造成的经济损失令人吃惊，远远超过了普通经济犯罪的损失。因此，确保计算机系统的安全已成为世人关注的社会问题，信息安全已成为信息科学的热点课题，信息安全专业也受到了社会各界的普遍关注。

我国信息安全本科专业设置始于 2000 年，教育部首次批准开办信息安全专业。从此以后，每年都有不少高校加入了设置信息安全本科专业的行列。

我国政府对信息安全非常重视，2003 年 9 月，中央《关于加强信息安全保障工作的意见》的 27 号文件，已经把信息安全工作提升到保护公众利益和维护国家安全以及保障与促进信息化发展的高度。2004 年 1 月，国务院召开全国信息安全保障工作会议，特别强调要加强信息安全院系的建设和人才培养工作。信息安全学科专业与信息安全产业必将在中央 27 号文件精神的指引下得到健康、快速的发展。

目前信息安全方面的人才还十分稀少，尤其是政府、国防、金融、公安和商业等部门对信息安全人才的需求很大。具有关部门统计，现在国内从事信息安全的专业人才只有 3 500 人左右，并且大多分布在高校和研究院所，而按照信息化发展的状况，社会对信息安全专业的人才需求量达几十万人。要解决供需矛盾，必须加快信息安全人才的培养。人才的培养离不开教材的建设，信息安全专业急需与之教学相配套的教材。

根据教育部高教司函[2003]141 号文件的精神，教育部高等学校电子信息与电气学科教学指导委员会专家组委托北京邮电大学等五所较早设置信息安全本科专业的高等院校完成了“信息安全专业规范”（以下简称“规范”）。该规范已于 2004 年 7 月，在四川绵阳召开的“全国高校本科信息安全专业规范与发展战略研究成果发布与研讨会”上公开发布。与会老师都对信息安全专业的发展、专业规范和课程设置展开了热烈的讨论。在会议上，我们征求了大家对信息安全本科专业教材的意见。在细致研究、反复讨论的基础上，规划了与规范相配套的“21 世纪高等院校信息安全系列规划教材”。

二、教材特色

本系列教材具有以下特色。

1. 参照“信息安全专业规范”确定教材题目、组织教材书稿内容。

本系列教材的所有题目是根据“信息安全专业规范”确定的。所有教材严格按照“规范”要求，结合信息安全专业的学制、培养规格、素质结构要求、能力结构要求、知识结构要求

撰写，使其所含知识点完全覆盖“规范”中的要求，确保能够达到“规范”中的学习目标。

2．注重套书的整体策划。

由于本系列教材涉及的内容比较多，在教材内容选择时，一方面要考虑教材内容相互的衔接，另一方面要考虑许多课程相互之间有内容交叉的现象；同时，充分考虑了先进性和成熟性之间的和谐关系，确保教材既能够反映信息安全领域的前沿科研状态，又能使学生掌握基础的核心知识和较成熟稳定的技能；我们在一开始策划时就对这两个方面相当重视，多次召开编委会，审定教材的大纲，落实教材的主要知识点，避免了内容的重复。

3．特别注意学生工程实际动手能力的培养。

根据“信息安全专业规范”的要求，本系列教材适当减少理论知识和技术知识层次的学时和要求，增加结合工程实际动手实践和专业应用技能层次的学时和要求。

4．本系列教材的作者都是在我国信息安全领域具有丰富教学和实践经验的一流专家，部分教材已经被评为“普通高等教育‘十一五’国家级规划教材”（以下简称“国家十一五规划教材”）。

本系列教材的书名及作者如下。

21世纪高等院校信息安全系列规划教材

编　号	书　名	作　者	作者单位
1	信息安全概论	徐茂智	北京大学
2	信息安全数学基础（国家十一五规划教材）	裴定一	广州大学
3	现代密码学（国家十一五规划教材）	何大可	西南交通大学
4	公钥密码学基础与应用	覃中平	武汉大学
5	安全操作系统原理与技术（国家十一五规划教材）	陈钟	北京大学
6	信息安全工程	方勇	四川大学
7	信息安全管理（国家十一五规划教材）	张红旗	解放军信息工程大学
8	信息安全标准与法律法规	秦玉海	中国刑事警察学院
9	网络攻击与防御技术（国家十一五规划教材）	张宏莉	哈尔滨工业大学
10	安全协议及其分析（国家十一五规划教材）	陈钟	北京大学
11	数字水印基础教程（国家十一五规划教材）	杨义先	北京邮电大学
12	计算机病毒原理与防范（国家十一五规划教材）	秦志光	电子科技大学
13	入侵检测技术（国家十一五规划教材）	曹元大	北京理工大学

5．提供完善的教学服务。

为了方便教学，我们免费为选用本套教材的老师提供以下教学服务。

（1）所有教材的电子教案。

（2）部分教材的习题答案。

（3）信息安全专业本科教学实验室建设方案与实验教学指导咨询（联系单位：“北京邮电大学信息安全中心”，联系方式：100876，北京西土城路十号北京邮电大学 126 信箱，yxyang@bupt.edu.cn）。

（4）信息安全专业本科生实习、实训与技能认证咨询（联系单位：“北京邮电大学信息安

全中心”；“四川绵阳灵创科技园”，联系方式：621000，绵阳市科创园区九州大道中段灵创科技园内灵创科技有限公司，0816-6336559（传真），6336520，yxyang@bupt.edu.cn）。

本系列教材尽管经过反复讨论修改，但限于作者水平和其他条件限制，难免存在不足和值得商榷之处，敬请批评指正。

21世纪高等院校信息安全系列规划教材编委会

2007年1月

编者的话

本书是为高等学校信息安全专业本科生提供的一本导引性教材。本书符合教育部拟定的教学大纲，而且注重知识的系统性和覆盖面的宽泛性。

在实际编写过程中我们发现，要处理好上述关系非常不易，因为近年来信息安全已经发展成一个庞然大物，是数学、计算机、微电子等学科融合的产物。目前市场上有关信息安全的书籍多半是围绕其中一种技术展开的，这样可以解决系统性问题，但是无法兼顾覆盖面。同时也存在着只注重了覆盖面的书籍，在读书过程中，实在让人无法理清头绪。

本书试图从建立信息安全体系结构出发，将其分解为技术体系、组织体系和管理体系。其中，从安全策略或安全目标角度将技术体系分解为系统安全、数据安全和事务安全，而从工程实现角度又将技术体系分解为物理环境安全、计算机系统平台安全、网络通信平台安全和应用平台安全，从而逐步理清了本门学科的脉络。其后章节的内容则可以对号入座，从而给学生一个整体展示，解决了系统性和覆盖面的关系。本书注重基础性，并妥善处理成熟性和先进性之间的关系，力图使所讲的内容不会很快过时。本书作为信息安全专业的先行专业基础课教材，不假定学生对信息安全有任何准备知识，并配备大量习题供读者思考，方便师生使用。本书的这种处理方式是否合适还有待实践和时间的检验。

本书编写过程中，得到国家自然科学基金网络与信息安全重大项目（批准号 90104004）、国家密码发展基金的资助，北京大学的叶志远、陈昱和韩心慧等老师以及赵彦慧、梁知音、诸葛建伟、司端锋、张磊等同学做出了重要贡献。在此一并表示衷心的感谢。

由于作者水平有限，加之时间仓促，书中难免存在疏漏之处，恳请各位专家和读者批评指正。

编　者

2007 年元月于燕园

目　录

▶▶▶ 第 1 章

信息安全简介

本章首先回顾信息安全的发展历程，然后介绍信息安全的一些基本概念，再说明信息安全是什么、它所关注的问题以及面临的挑战是什么，从而为读者对后续章节的理解提供背景和线索。在后续章节中再对这些概念进行细化，逐步揭示贯穿这些概念的内在逻辑。

1.1 信息安全的发展历史

密码技术在军事情报传递中悄然出现，并扮演着重要角色，这可以追溯到若干个世纪以前。在第二次世界大战中，密码技术取得巨大飞跃，特别是 Shannon 提出的信息论使密码学不再是一种简单的符号变换艺术，而成为一门真正的科学。与此同时，计算机科学也得到了快速发展。直到 20 世纪 60 年代，对于计算机系统，人们主要关注的是它的物理安全。到 20 世纪 70 年代，随着计算机网络的出现，人们才把重心转移到计算机数据的安全上来。从此，信息安全技术得到持续高速的发展。本节通过对一些重要历史阶段的回顾，来介绍信息安全的由来和研究领域的拓展。

1.1.1 通信保密科学的诞生

人类很早就在考虑怎样秘密地传递信息了。文献记载的最早有实用价值的通信保密技术是古罗马帝国时期的 Caesar 密码。它能够把明文信息变换为人们看不懂的称为密文的字符串，当把密文传递到自己伙伴手中的时候，又可方便地还原为原来的明文形式。Caesar 密码实际上非常简单，需要变为密文（称为加密）时，把字母 A 变成 D、B 变为 E、……、W 变为 Z、X 变为 A、Y 变为 B、Z 变为 C，即密文由明文字母循环移 3 位得到。反过来，由密文变为明文（称为脱密）也是相当简单的。

1568 年 L.Battista 发明了多表代替密码，并在美国南北战争期间由联军使用，Vigenere 密码和 Beaufort 密码是多表代替密码的典型例子。1854 年 Playfair 发明了多字母代替密码，英国在第一次世界大战中采用了这种密码，Hill 密码是多字母代替密码的典型例子。多表、多字母代替密码成为古典密码学的主流。

研究密码破译（也称为密码分析）的技术也在发展，并以 1918 年 W.Friedman 关于使用重合指数破译多表代替密码技术为重要里程碑。其后，各国军方对密码学进行了深入研究，但相关成果并未发表。1949 年 C.Shannon 的《保密系统的通信理论》文章发表在贝尔系统技术杂志上。这两个成果为密码学的科学研究奠定了基础。学术界评价这两项工作时，认为它们把密码技术从艺术变为科学。实际上这是通信保密科学的诞生，其中密码是核心技术。

1.1.2 公钥密码学革命

在 C.Shannon 的文章发表之后的 25 年内，密码学的公开研究几乎是空白。直到 20 世纪 70 年代初，IBM 公司的 DES（美国数据加密标准）和 1976 年 Diffie-Hellman 公开密钥密码思想的提出，以及 1977 年第一个公钥密码算法 RSA 的提出，才为密码学的发展注入了新的活力。

对传统密码算法的加密密钥和脱密密钥来说，从其中的任一个容易推出另一个，从而两个必须同时保密。而公钥密码的关键思想是利用计算难题构造密码算法，其加密密钥和脱密密钥两者之间的相互导出在计算上是不可行的。

公钥密码掀起了一场革命，因为它对信息安全来说至少有 3 方面的贡献。其一，它首次从计算复杂性上刻画了密码算法的强度，突破了 Shannon 仅关心理论强度的局限性。其二，它把传统密码算法中两个密钥管理中的保密性要求，转换为保护其中一个的保密性及另一个的完整性的要求。其三，它把传统密码算法中密钥归属从通信两方变为一个单独的用户，从而使密钥的管理复杂度有了较大下降。

公钥密码提出后的几年中，有两件事值得注意。一是密码学的研究已经逐步超越了数据的通信保密范围，开展了对数据的完整性、数字签名技术的研究。另一件事是随着计算机及其网络的发展，密码学已逐步成为计算机安全、网络安全的重要支柱，使得数据安全成为信息安全的核心内容，超越了以往物理安全占据计算机安全主导地位的状态。

1.1.3 访问控制技术与可信计算机评估准则

20 世纪 70 年代，在密码技术应用到计算机通信保护的同时，访问控制技术的研究取得了突破性的成果。

1969 年，B.Lampson 提出了访问控制的矩阵模型。模型中提出了主体与客体的概念，客体是指信息的载体，主要指文件、数据库等，主体是指引起信息在客体之间流动的人、进程或设备。访问是指主体对客体的操作，如读、写、删除等，所有可允许操作的集合称为访问属性。这样，计算机系统中全体主体作为行指标，全体客体作为列指标，取值为访问属性的矩阵就可以描述一种访问策略。可以设想随着计算机所处理问题的复杂性的增加，不可能显式地表示一个计算机的访问控制矩阵，所以用访问控制矩阵来实施访问控制是不现实的。

1973 年，D.Bell 和 L.Lapadula 取得突破，创立了一种模拟军事安全策略的计算机操作模型，这是最早、也是最常用的一种计算机多级安全模型。该模型把计算机系统看成是一个有限状态机，为主体和客体定义了密级和范畴，定义了满足一些特性（如简单安全特性 SS）的安全状态概念。然后，证明了系统从安全状态出发，经过限制性的状态转移总能保持状态的安全性。模型使得人们不需要直接管理访问控制矩阵，而且可以获得可证明的安全特征。

1985 年，美国国防部在 Bell-Lapadula 模型的基础上提出了可信计算机评估准则（TCSEC），通常称为橘皮书。按照计算机系统的安全防护能力，分成 8 个等级。它对军用计算机系统的安全等级认证起了关键作用，而且对后来的信息安全评估标准的建立起了重要参考作用。

由于 Bell-Lapadula 模型主要是面向多密级数据的机密性保护的，它对数据的完整性或系统的其他安全需求刻画不够。所以，1977 年提出的针对完整性保护的 Biba 模型、1987 年提

出的侧重完整性和商业应用的 Clark-Wilson 模型，可以看成在不同程度上对 Bell-Lapadula 模型进行的扩展。基于角色的访问控制模型（RBAC）、权限管理基础设施（PMI）则使得访问控制技术在网络环境下能方便地实施。

1.1.4 网络环境下的信息安全

在冷战期间，美国想要建一种有多个路径的通信设施，一旦发生战争，因为网络有路径备份，不易被炸断。从而在 1968 年就开始设计一种叫做 APANET 的网络。APANET 诞生后，经历了军事网、科研网、商用网等阶段。经过 30 多年的发展，APANET 逐步发展成了现在的互联网（Internet）。目前互联网正从 IPv4 向 IPv6 跨越，在技术上仍然保持着强劲的发展态势。

在 20 世纪 80 年代后期，由于计算机病毒、网络蠕虫的广泛传播，计算机网络黑客的善意或恶意的攻击，DDoS 攻击的强大破坏力，网上窃密和犯罪的增多，人们发现自己使用的计算机及网络如此脆弱。与此同时，网络技术、密码学、访问控制技术的发展使得信息及其承载系统安全的含义逐步完善。随之，人们研究杀毒、入侵检测等检测技术，防火墙、内容过滤等过滤技术，虚拟专用网（VPN）、身份识别器件等新型密码技术，这不仅引起了军界、政府的重视，而且引起了商业界、学校、科研机构的普遍研究热情。近年来，社会上已经开发出一系列相关的信息安全产品，它们被广泛应用到军方、政府、金融及企业中，标志着网络环境下的信息安全时代的到来，信息安全产业的迅速崛起。

1.1.5 信息保障

1998 年 10 月，美国国家安全局（NSA）颁布了信息保障技术框架（IATF）1.1 版，2002 年 9 月，又颁布了该框架的 3.1 版本。另一方面，美国国防部（DoD）于 2003 年 2 月 6 日颁布了信息保障的实施命令 8500.2，从而信息保障成为美国军方组织实施信息化作战的既定指导思想。

美国国防部对信息保障（Information Assurance，IA）的定义是“通过确保信息的可用性、完整性、可识别性、保密性和抗抵赖性来保护信息和信息系统，同时引入保护、检测及响应能力，为信息系统提供恢复功能。”这就是信息保障的 PDRR 模型，PDRR 是指保护（Protect）、检测（Detect）、响应（React）和恢复（Restore）。

美国信息保障技术框架的推进，使人们意识到，对信息安全的认识不要停留在保护的框架之下，同时还需要注意信息系统的检测、响应能力。该框架还对保障的实施提出了相当细致的要求，从而对信息安全的概念和相关技术的形成将会产生深远影响。

2003 年，中国发布了《国家信息领导小组关于信息安全保障工作意见》，这是国家把信息安全提到战略高度的指导性文件，但不是技术规范。

1.2 信息安全的概念和目标

1.2.1 信息安全的定义

信息安全的概念随着网络与信息技术的发展而不断地发展，其含义也在动态地变化。

20 世纪 70 年代以前，信息安全的主要研究内容是计算机系统中的数据泄漏控制和通信系统中的数据保密问题。然而，今天计算机网络的发展使得这个当时非常自然的定义显得非常不恰当。

首先，因为随着黑客、特洛伊木马及病毒的攻击不断升温，人们发现除了数据的机密性保护外，数据的完整性保护以及信息系统对数据的可用性支持都非常重要。这种学术观点，是从保密性、完整性和可用性的角度来衡量信息安全的。它不仅要求对数据的机密性和完整性的保护，而且还要求计算机系统在保证数据不受破坏的条件下，在给定的时间和资源内提供数据的可用性服务。安全问题涉及了更多的方面，安全问题也更为复杂。但这种安全概念仍然局限在“数据”的层面上。

其次，不断增长的网络应用中所包含的内容远远不能用“数据”一词来概括。例如，在用户之间进行身份识别的过程中，虽然形式上是通过数据的交换实现的，但等身份识别的目的达到以后，交换的中间数据就变得毫无用处了。仅仅逐包保护这些交换数据的安全是不充分的，原因是这里传递的是身份“信息”而不是身份“数据”。还可以举出很多其他例子来说明仅仅考虑数据安全是不够的，信息安全与数据安全相比有了实质性的扩展。

人们普遍认为，信息安全是研究保护信息及承载信息的系统的科学。但是，我们需要更深入地认识它的含义。

理想的信息安全是要保护信息及承载信息的系统免受网络攻击的伤害。这种类型的保护经常是无法实现的或者实现的代价太大。进一步的研究表明，信息或信息系统在受到攻击的情况下，只要有合适的检测方法能发现攻击，就可以做出恰当的响应（如发现网络攻击行为后，切断网络连接），对攻击造成的灾难进行恢复（如对数据进行备份恢复）。检测、恢复是重要的补救措施。检测可以看成是一种应急恢复的先行步骤，其后才进行数据和信息恢复。因此信息安全的保护技术可分为三类：保护、检测和恢复。这一点与 IA 框架结构中的分类本质差异不大，但那里把信息安全技术分成两类：保护与恢复（恢复包含检测和响应）。

事实上，信息及其系统的安全与人、应用及相关计算环境紧密相关，不同的场合对信息的安全有不同的需求。例如，电子合同的签署需要不可抵赖性，而电子货币的安全中又需要不可追踪性，这两者是截然相反的要求。又如，有人可能认为把文件放到公共目录服务器上是安全的，而另一些人则可能认为将其保存到自己的计算机上还需要口令保护才是安全的。这种人们在特定应用环境下对信息安全的要求叫做安全策略。

综上分析，信息安全定义如下所述。

信息安全是研究在特定的应用环境下，依据特定的安全策略，对信息及其系统实施防护、检测和恢复的科学。

该定义明确了信息安全的保护对象、保护目标和方法，下面将围绕这一定义加以说明。

1.2.2 信息安全的目标和方法

信息安全的保护对象是信息及其系统。安全目标（Security Target，ST）又由安全策略所定义，信息系统的安全策略是由一些具体的安全目标组成的。不同的安全策略表现为不同的安全目标的集合。安全目标通常被描述为“允许谁怎样使用系统中的哪种资源”、“不允许谁怎样使用系统中的哪种资源”或事务实现中“各参与者的行为规则是什么”等。

安全目标可以分成数据安全、事务安全、系统安全（包括网络系统与计算机系统安全）三类。数据安全主要涉及数据的机密性与完整性；事务安全主要涉及身份识别、抗抵赖等多方计算安全；系统安全主要涉及身份识别、访问控制及可用性。

安全策略中的安全目标则是通过一些必要的方法、工具和过程来实现的，这些方法称为安全机制。安全机制有很多，但可以从防护、检测和恢复三个角度进行分类。防护机制包括密码技术（指加密、身份识别、消息鉴别、数字签名）、访问控制技术、通信量填充、路由控制、信息隐藏技术等；检测机制则包括审计、验证技术、入侵检测、漏洞扫描等；恢复机制包括状态恢复、数据恢复等。

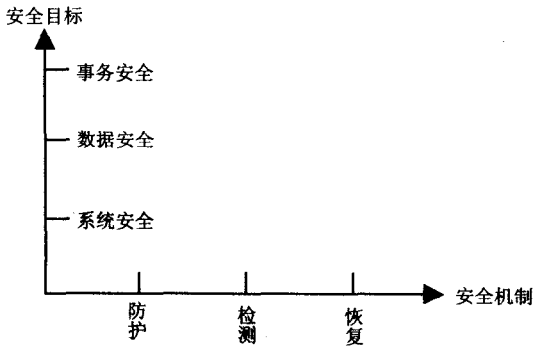


图 1.1 安全机制、安全目标关系图

安全机制与安全目标关系如图 1.1 所示。

安全目标在不同的文档中经常有不同的表述。例如，在第 2 章的 OSI 安全体系结构中，它被称为安全服务。因为在 OSI 网络分层体系结构中，低层是通过向高层提供服务实现安全通信功能的。从而很自然地把各层上达到的安全目标称为安全服务。有时安全目标又称为安全功能，强调了安全目标的实现过程。

1.3 安全威胁与技术防护知识体系

安全目标分为三类，即系统安全（包括网络安全与计算机安全）、数据安全和事务安全，它们之间有一定的层次关系。

如图 1.2 所示，网络和计算机所组成的系统作为信息的承载者，其安全性是基本的要求，而后，才能实现其上运行的数据的安全目标，但最终目标则是为各种应用事务提供安全保护。下层的安全为上层的安全提供一定的保障（assurance），但不提供安全服务。这就是说，在实现上层的安全性中经常需要下层的安全做基础，但上层的安全不能仅通过对下层的功能调用来实现，需要用专门的安全机制来实现。

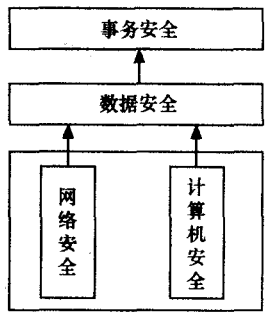


图 1.2 系统安全、数据安全、事务安全层次图

从管理角度看，上述层次关系是相当重要的。虽然各层次所采用的安全机制或技术可以有重复，但它们之间的区别是显著的。例如，一组计算机或一个局域网，无论其上是否承载着重要的数据和事务，其安全性都应当得到保障；而对于一些穿梭于计算机和网络间的数据，就要有明确、可靠的机制来保障它们的机密性和完整性，而这些安全隐式地要求我们对计算机安全和网络安全至少要有初步的保障。同样道理，事务安全隐式地要求我们对数据安全、计算机安全和网络安全至少要有初步的保障。下面我们从分析可能出现的威胁来理解这些层面上的安全问题。

1.3.1 计算机系统中的安全威胁

计算机系统是用于信息存储、信息加工的设施。计算机系统一般是指具体的计算机系统，但