高等院校信息管理与信息系统专业系列教材

信息系统安全教程

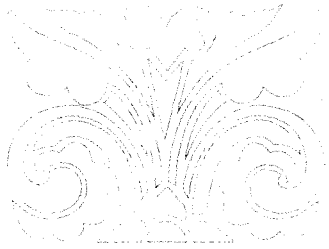
张基温 编著

清华大学出版社

高等院校信息管理与信息系统专业系列教材

信息系统安全教程

张基温 编著



清华大学出版社
北京

内 容 简 介

本书从应用的角度介绍信息系统安全原理，围绕防护、检测、响应和恢复，重点介绍了数据加密、认证技术、访问控制、入侵与攻击、网络防范和安全管理，内容覆盖了当前有关信息系统安全的基本技术。书中不但提供了较为充分的习题，还设计了17个旨在提高学习者动手能力并发挥其创造性的实验。

本书深入浅出、富有哲理、结构新颖，紧扣理论本质，实践性强，适合学习，可以激发学生的学习热情。本书适合作为计算机科学与技术专业、信息管理与信息系统专业和信息安全专业的“信息系统安全”课程的教材或教学参考书，也可供有关技术人员参考。

图书在版编目(CIP)数据

信息系统安全教程/张基温编著. —北京：清华大学出版社，2007.7
(高等院校信息管理与信息系统专业系列教材)
ISBN 978-7-302-15127-2

Ⅰ. 信…　Ⅱ. 张…　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(2007)第059884号

责任编辑：范素珍
责任校对：白　蕾
责任印制：王秀菊

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　　**邮购热线**：010-62786544
投稿咨询：010-62772015　　**客户服务**：010-62776969

印 刷 者：北京密云胶印厂
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×260　　**印　张**：17.5　　**字　数**：400千字
版　　次：2007年7月第1版　　**印　次**：2007年7月第1次印刷
印　　数：1～4000
定　　价：23.00

出版说明

20世纪三四十年代，一直摸索着前进的计算技术与刚走向成熟的电子技术结缘。这一结合，不仅孕育了新一代计算工具——电子计算机，还产生了当时谁也没有料到的巨大效应：电子计算机——这种当初为计算而开发出来的工具，很快就超出计算的范畴，成为“信息处理机”的代名词。

信息能促成管理系统的优化，促进组织创新，绩效不断上升；信息能提高计划与决策的科学性和及时性，是信息时代组织生存、发展、竞争制胜的有力武器；信息能革新企业内部的生产力要素结构，使资源转换系统的生产率大幅度提高，并同时以不断增加的柔性适应市场需求结构和消费结构的快速变化。

随着信息技术的发展与广泛应用，人类开始能够高效率地开发并利用信息，信息资源对人类社会的作用得以有效地发挥，并逐步超过材料和能源成为人类社会的重要支柱，信息化成为一个时代的口号。与此同时，信息资源开发与管理人才越来越广受社会青睐。

信息管理与信息系统专业是一个培养信息化人才的专业，是一个培养信息资源开发与管理方面的专门人才的专业。从知识结构上看，它处在管理学、信息科学与技术和有关专业领域的交叉点上。它对技术有极高的要求，又要求对组织有深刻的理解，对行为有合理的组织，反映了科学与人本融合的特点。这种交叉与融合正是信息管理与信息系统专业最重要的特征，是别的学科或专业难以取代和涵盖的。但是，从20世纪70年代末开始创办到90年代初，尽管国内设有该专业的院校已经上升到150多所，但还没有形成很好反映自己特色的一个教材体系。1991年全国10所院校的信息管理专业的负责人在太原召开第一次研讨会，异口同声地谈起创建一套符合专业需要的教材体系话题。此后，经过1993年在大连、1995年在武汉召开的会议，又有更多的院校加入到了这一研讨之中。这些研讨活动得到了国家教委有关部门的赞许和支持。通过研讨，大家在建设具有专业特点的教材体系、改变简单照搬其他专业教材上取得了共识。1996年正式启动这个项目，经协商由张基温教授担任主编，由魏晴宇教授、陈禹教授担任顾问。在清华大学出版社的大力支持下，从1997年起这套我国信息管理与信息系统专业的第一套系列教材陆续问世。迄今已经10年多，当初规划的七八本教材已经扩展到30多本，形成了一套品种多样、影响面广的系列教材，不仅为信息管理和信息系统专业建设做出了贡献，而且也被许多计算机专业所选用。这些都是编委会全体同仁和作者、广大使用本系列教材的师生以及出版社的编辑们辛勤劳动的结果。

同时，我们也欣喜地看到，10年来，信息管理与信息系统专业也有了较大的发展，不仅其规模已经发展到500多个教学点，而且随着信息化的纵深推进，随着电子商务、电子政务和企业信息化的发展，专业的教学内容也与时俱进地深化和更新，从过去的围绕信息系统分析与设计，已经延伸到信息资源的开发与管理；专业的定位也逐步明晰，即为信息化建设与管理培养人才。同时，近年来围绕提高教学质量，许多学校开展了精品课程建设和教材建设。这些都标志这个专业正在走向成熟。

成熟的专业，需要优秀教材的支持。为此，我们将重新审视并陆续修订这套教材。在这套教材问世10周年之际，我们再一次表示一个心愿：希望与全国的同行共勉，在教材和专业建设上齐心协力，做出更大贡献。我们将在原来的基础上，重新审视，不断补充，不断修改，不断完善。对于它的任何建设性意见，都是我们非常期盼的。为此，这套教材将具有充分的开放性：每一本教材都是一个原型，每一位有志者对它的建设性意见都将会被采纳，并享有自己的知识产权，以使它们逐步成为精品。

《高等院校信息管理与信息系统专业系列教材》编委会

2007年1月28日

前　言

信息系统是重要的，重要的系统会导致过多的攻击，需要特别保护。信息系统是复杂的，复杂的系统是脆弱的，脆弱的系统需要特别保护。信息系统具有虚拟性，虚拟的系统给安全保护带来很大困难。现代信息系统是开放的，开放的系统会带来更多的风险。

重要、风险、虚拟和困难造就了信息系统安全攻防博弈的战场，也加速了信息安全技术和管理的快速发展，使得信息系统安全的知识体系不断扩大。

本书围绕防护、检测、响应和恢复，把有关信息系统安全的知识按照数据保密、认证、访问控制、系统攻击、网络防护和信息系统安全管理的结构进行组织。在内容的选材上，采取的原则是：重点内容详细介绍，次要内容只作一般介绍。

本书每章后都配备了较多的习题。这些习题有不同的类型：

- 有些要思考、总结；
- 有些要进一步理解；
- 有些要自己想象；
- 有些是要自己查找资料；
- 有些要动手实验。

本人期望通过这些习题使学习者的自学能力和动手能力有较大提高。

本书在编写过程中参考了大量资料。这些资料有的引自国内外论文，有的引自其他著作，有的引自网站。虽本人尽心在参考文献中予以列出，但尚有许多疏漏，也受篇幅所限，恕不能一一列出。在此谨向有关作者致谢并表歉意。

在编写过程中，蒋中云、王玉斐、魏士婧、裴浩、张秋菊、张展赫、戴璐等人参与了部分工作，并制作了课件。

计算机信息系统安全是一个涉及广泛、发展迅速的领域。尽管本人尽力想把它编写好，但客观和主观的能力所限，实在是心有余而力不足。希望读者和有关专家不吝指正，以便适当的时候进一步修订。

张基温

2006 年 8 月 18 日

读者意见反馈

亲爱的读者：

感谢您一直以来对清华版计算机教材的支持和爱护。为了今后为您提供更优秀的教材，请您抽出宝贵的时间来填写下面的意见反馈表，以便我们更好地对本教材做进一步改进。同时如果您在使用本教材的过程中遇到了什么问题，或者有什么好的建议，也请您来信告诉我们。

地址：北京市海淀区双清路学研大厦 A 座 602 室　计算机与信息分社营销室　收
邮编：100084　　电子邮件：jsjjc@tup.tsinghua.edu.cn
电话：010-62770175-4608/4409　　邮购电话：010-62786544

教材名称：信息系统安全教程

ISBN：978-7-302-15127-2

个人资料

姓名：_____ 年龄：_____ 所在院校/专业：_____

文化程度：_____ 通信地址：_____

联系电话：_____ 电子信箱：_____

您使用本书是作为：□指定教材 □选用教材 □辅导教材 □自学教材

您对本书封面设计的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书印刷质量的满意度：

□很满意 □满意 □一般 □不满意　改进建议_____

您对本书的总体满意度：

从语言质量角度看 □很满意 □满意 □一般 □不满意

从科技含量角度看 □很满意 □满意 □一般 □不满意

本书最令您满意的是：

□指导明确 □内容充实 □讲解详尽 □实例丰富

您认为本书在哪些地方应进行修改？（可附页）

_____

_____

您希望本书在哪些方面进行改进？（可附页）

_____

_____

电子教案支持

敬爱的教师：

为了配合本课程的教学需要，本教材配有配套的电子教案（素材），有需求的教师可以与我们联系，我们将向使用本教材进行教学的教师免费赠送电子教案（素材），希望有助于教学活动的开展。相关信息请拨打电话 010-62776969 或发送电子邮件至 jsjjc@tup.tsinghua.edu.cn 咨询，也可以到清华大学出版社主页（http://www.tup.com.cn 或 http://www.tup.tsinghua.edu.cn）上查询。

高等院校信息管理与信息系统专业系列教材

- 信息资源管理教程　赖茂生 编著
- 数据仓库与数据挖掘教程　陈文伟 编著
- 计算机操作系统教程　张不同等 编著
- 计算机网络教程　黄叔武等 编著
- 计算机网络教程题解与实验指导　黄叔武等 编著
- 信息系统开发与管理教程(第二版)　左美云 编著
- 信息系统开发方法教程(第二版)　陈佳等 编著
- 决策支持系统教程　陈文伟 编著
- 离散数学(第三版)　耿素云等 编著
- 离散数学题解(修订版)　屈婉玲等 编著
- 计算机组成原理教程(第 3 版)　张基温 编著
- 计算机组成原理教程题解与实验指导　张基温 编著
- 信息管理英语教程　李季方 编著
- 管理信息系统教程(第二版)　闪四清 编著
- 电子商务基础教程(第二版)　兰宜生 编著
- Java 程序开发教程　张基温 编著
- Java 程序开发例题与题解　张基温 编著
- Visual Basic 程序开发教程　张基温 编著
- Visual Basic 程序开发例题与题解　张基温 编著
- 数据结构及应用算法教程　严蔚敏等 编著
- 运筹学模型与方法教程　程理民等 编著
- 运筹学模型与方法教程例题分析与题解　刘满凤等 编著
- 数据库系统原理教程　王珊等 编著
- 信息经济学教程　陈禹 编著
- C++ 程序开发教程　张基温 编著
- C++ 程序开发例题与习题　张基温 编著
- 信息系统安全教程　张基温 编著

目　录

第0章 引 论

0.1 信息系统风险

系统风险是指系统遭受意外损失的可能性，它主要来自系统可能遭受的各种威胁、系统本身的脆弱性以及系统对于威胁的失策。

0.1.1 信息系统及其重要性

人类社会的发展归根结底是人类知识体系的发展和基于这个知识体系的工具的进步。

人们对于信息已经有众多的解释。其中，认识论把信息看作不确定性的减少或传递中的知识差(degree of knowledge)，在哲学界把信息与有序度联系起来。因此可以说，信息是以传递知识差的形式来减少不确定性、增加系统有序度的资源。不确定性的减少就是风险减少。从这点上看，信息系统就是一种减少不确定性和减少风险的工具。

从生产力发展的角度看，人类社会已经经历了原始社会、农业社会和工业社会，现在已经迈入了信息社会。这4种社会形态是人类社会生产力的3次飞跃，也是人类资源开发和使用从弱意识到强意识的3次飞跃。在原始社会，人类对物质、能源及信息资源的开发和使用都处于弱意识形态，生产力极为低下。农业社会的到来是人类强意识地进行物质资源开发和使用进步的结果，生产力有了较大提高。工业社会的到来是人类在强意识地进行能源资源开发和使用方面的一次飞跃，生产力有了进一步提高。信息社会的到来是人类强意识地进行信息资源开发和使用进步的一次飞跃，人类社会生产力得到空前提高。经过3次大的经济转型和形态变化，物质、能源和信息作为人类社会三大基本资源的认识得到充分确立。而信息资源是其中一种可以无限开发的和能动的资源，它的作用日益显著，目前已经成为政治、经济竞争的主要领域和焦点。从资源的角度看，信息系统是一种开发信息资源的工具，是信息以及用于信息的采集、传输、存储、管理、检索和利用等工具的有机整体。

由于信息作为资源和减少决策风险的作用，使得信息系统成为竞争力的重要代表，也使现代社会越来越依赖于信息系统的安全运行。这种重要性也使信息系统成为竞争对手攻击的主要目标。

0.1.2 信息系统安全威胁

信息系统安全威胁(thread)是指对于信息系统的组成要素及其功能造成某种损害的潜在可能。下面从不同的角度介绍对于信息系统安全威胁的特征。

1. 按照威胁的来源分类

按照威胁的来源粗略地可以将信息系统的威胁分为内部威胁和外部威胁。进一步细分，信息系统的威胁大致有如下一些。

(1) 自然灾害威胁

自然灾害是不以人的意志为转移的一些自然事件，如地震、台风、雷击、洪涝、火灾等。这些灾害虽然不能阻止其发生，但可以通过技术或管理手段避免或降低灾害带来的损失。例如，采取防雷、防火、防水和防地震以及自然灾害预警措施等。

(2) 滥用性威胁

意外人为威胁主要由系统内部人员(设计人员、操作人员、管理人员等)的操作不当或失误引起。这种威胁的发生是偶然的，但却是时有发生的，并且存在于信息系统开发的整个生命周期中。安全专家经过长期调查得出一个结论：无论是私人机构还是公共机构，大约65%的损失是由于无意的错误或疏忽所造成。

(3) 有意人为威胁

有意人为威胁主要来自两种情况：一是好奇心人为威胁，一是敌意性人为威胁。前者一般由一些好奇心强者实施，后者往往是由竞争对手、泄愤者、间谍等实施。

2. 按照作用对象分类

按照所作用的对象，信息系统威胁有如下几种。

(1) 针对信息的威胁

基于信息(资源)的威胁是指偶然地或故意地造成信息系统中信息在如下几个方面的损失：

- 机密性(confidentiality)：数据在传输或存储时有被非法截取的可能，就会形成机密性威胁。例如被监听、被分析等。提高信息机密性的方法有数据加密、进行访问控制以及对访问者进行身份验证等，以保证数据不被非授权者知晓。
- 完整性(integrity)：完整性威胁是指数据在传输或存储过程中被篡改、被丢失、被破坏的可能。为了保护数据完整性，可以进行数据的完整性校验以及认证等，可以发现数据是否被篡改，进而可以进行数据的恢复。
- 可用性(availability)：指保障合法用户正常使用信息的能力。例如，拒绝访问的攻击，就导致了合法用户正常访问信息资源的能力丧失。
- 真实性(authenticity)：真实性主要是指接收方所具有的辨认假冒和抗拒否认的能力。

因此，针对信息(资源)的威胁可以归结为以下3类：

- 信息破坏：非法取得信息的使用权，删除、修改、插入、恶意添加或重发某些数据，以影响正常用户对信息的正常使用。
- 信息泄密：故意或偶然地非法侦收、截获、分析某些信息系统中的信息，造成系统数据泄密。
- 假冒或否认：假冒某一可信任方进行通信或者对发送的数据事后予以否认。

(2) 针对系统的威胁

针对系统的威胁包括对系统硬件的威胁、对系统软件的威胁和对于系统使用者的威胁。

- 对于通信线路、计算机网络以及主机、光盘、磁盘等的盗窃和破坏都是对于系统硬件(实体)的威胁。

- 病毒等恶意程序是对系统软件的威胁，流氓软件等是对于系统访问者的威胁等。
- 通过旁路控制，躲过系统的认证或访问控制进行未授权的访问等。

通过对系统的威胁可以使系统运行不正常或瘫痪，丧失可用性。

3. 按照方法的分类

对于信息系统的威胁有许多方法或手段。下面是几种主要的威胁方法。

(1) 信息泄露

信息泄露是指系统的敏感数据有意或无意地被未授权者知晓。信息泄露的主要途径有：

- 在传输中利用电磁辐射或搭接线路的方式窃取。
- 授权者向未授权者泄露，例如一个公司职员用文件名传输公司的秘密文件的同时，对文件名编码，使公司的正常秘密文件传输信道被乱用为隐蔽的泄密信道。
- 存储设备被盗窃或盗用。
- 未授权者利用特定的工具捕获网络中的数据流量、流向、通行频带、数据长度等数据并进行分析，从中获取敏感信息。

(2) 扫描(scan)

扫描是利用特定的软件工具向目标发送特制的数据包，对响应进行分析，以了解目标网络或主机的特征。

(3) 入侵(intrusion)

入侵即非授权访问，是指没有经过授权(同意)就获得系统的访问权限或特权，对系统进行非正常访问，或擅自扩大访问权限越权访问系统信息。主要的非授权访问形式有如下几种。

- 旁路控制：攻击者利用系统漏洞绕过系统的访问控制而渗入系统内部。
- 假冒：某个未经授权的实体通过出示伪造的凭证骗取某个系统的信任，非法取得系统访问权或得到额外的特权。
- 口令破解：利用专门的工具穷举或猜测用户口令。
- 合法用户的非授权访问：合法用户进入系统后擅自扩大访问权限或越权访问。

(4) 拒绝服务(denial of service,DoS)

DoS 指系统可用性因服务中断而遭到破坏。DoS 攻击常常通过用户进程消耗过多的系统资源造成系统阻塞或瘫痪。

(5) 抵赖(否认)

通信一方由于某种原因而实施的下列行为都称为抵赖：

- 发方事后否认自己曾经发送过某些消息；
- 收方事后否认自己曾经收到过某些消息；
- 发方事后否认自己曾经发送过某些消息的内容；
- 收方事后否认自己曾经收到过某些消息的内容。

(6) 滥用(misuse)

滥用泛指一切对信息系统产生不良影响的活动。主要内容如下。

- 传播恶意代码：恶意代码是一些对于系统有副作用的代码。它们或者独立存在(如