21世纪 高等学校信息安全专业规划教材

信息系统安全

陈萍 张涛 赵敏 编著

清华大学出版社

21世纪 高等学校信息安全专业规划教材

信息系统安全

陈萍 张涛 赵敏 编著

清华大学出版社
北京

内 容 简 介

本教材以教育部《信息安全类专业指导性专业规范》所列知识点为基础，从信息系统体系结构层面系统描述信息系统的安全问题及对策。

全书共12章，第1章介绍信息系统安全的基本概念、发展历史、主要目标和技术体系；第2章介绍密码学基本理论与应用，具体包括对称密码体制和公钥密码体制，以及基于密码学的消息认证、数字签名、公钥基础设施PKI；第3章介绍物理安全技术；第4、第5章分别介绍身份认证和访问控制技术；第6章介绍操作系统安全机制；第7章介绍数据库安全技术；第8章介绍信息安全评估标准和我国的信息安全等级保护制度；第9章介绍信息系统安全风险评估的概念、工具、方法、流程；第10章介绍恶意代码的检测与防范技术；第11章介绍软件安全漏洞及防范措施，重点介绍Web应用安全机制；第12章介绍信息安全新技术。

本书可以作为信息安全专业、信息对抗专业、计算机专业、信息工程专业和其他相关专业的本科生和研究生教材，也可作为网络信息安全领域的科技人员与信息系统安全管理员的参考书。

图书在版编目(CIP)数据

信息系统安全/陈萍，张涛，赵敏编著. —北京：清华大学出版社，2016
21世纪高等学校信息安全专业规划教材
ISBN 978-7-302-42227-3

Ⅰ. ①信…　Ⅱ. ①陈…　②张…　③赵…　Ⅲ. ①信息系统—安全技术　Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2015)第279084号

责任编辑：黄　芝　薛　阳
封面设计：杨　兮
责任校对：梁　毅
责任印制：杨　艳

出版发行：清华大学出版社
网　　址：http://www.tup.com.cn，http://www.wqbook.com
地　　址：北京清华大学学研大厦A座　　邮　　编：100084
社 总 机：010-62770175　　邮　　购：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
课 件 下 载：http://www.tup.com.cn，010-62795954

印 刷 者：北京富博印刷有限公司
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：185mm×260mm　　**印　张**：21　　**字　　数**：523千字
版　　次：2016年4月第1版　　**印　　次**：2016年4月第1次印刷
印　　数：1～2000
定　　价：39.50元

产品编号：065214-01

前　言

随着计算机和网络技术的日益普及和广泛应用，信息的应用和共享日益广泛且更为深入，各种信息系统已经成为国家基础设施。与此同时，计算机信息系统的安全问题日益突出，情况也越来越复杂，针对计算机信息系统的攻击与破坏事件层出不穷，如果不对其加以及时和正确的保护，这些攻击与破坏事件轻则干扰人们的日常生活，重则造成巨大的经济损失，甚至威胁到国家安全，所以信息系统的安全问题已经引起许多国家的高度重视，社会对信息安全人才的需求越来越迫切。

确保信息系统安全是一个整体概念，解决某一信息安全问题通常要综合考虑硬件、系统软件、应用软件、管理等多层次的安全问题，目前市面上信息安全方面的书籍大多侧重于网络安全，而专门从信息系统体系结构层面讲解信息安全的教材较少，不利于相关课程教学的实施。

本书以教育部《信息安全类专业指导性专业规范》所列知识点为基础，从信息系统的组成要素出发，寻求综合解决信息安全问题的方案。信息系统自底向上由物理层（硬件层）、操作系统、网络、数据库、应用系统等构成，只有从信息系统硬件和软件的底层出发，确保信息系统各组成部分的安全，从整体上采取措施，才能确保整个信息系统的安全。因此，教材内容以保障信息系统各组成层次安全为一级主线，以各类安全技术在信息系统不同层次上的应用为二级主线进行优化重组，系统地介绍信息系统安全的基本概念、原理、技术、知识体系与应用，覆盖了信息的存储、处理、使用、传输与管理整个生命周期不同环节的安全威胁与相应的保护对策。

本书内容共有 12 章，第 1 章介绍当前信息系统安全形势、信息系统安全的基本概念、发展历史、主要目标和技术体系；第 2 章介绍密码学理论与应用，具体包括密码学的基本概念、密码体制的组成、分类以及设计原则、古典密码体制、对称密码体制、公钥密码体制等密码学基本理论，此外本章还简单介绍了密码学的应用，具体包括用于消息完整性校验的消息认证，用于防止信息抵赖的数字签名技术，以及对公钥进行有效管理和提供通用性安全服务的公钥基础设施技术；第 3 章介绍物理层面增强信息系统安全的方法和技术；第 4 章、第 5 章分别介绍信息系统安全基本技术中的身份认证和访问控制，身份认证是信息系统的第一道安全防线，其目的是确定用户的合法性，阻止非法用户访问系统，访问控制是根据安全策略对用户操作行为进行控制，其目的是为了保证资源受控、合法地使用；第 6 章介绍操作系统安全机制，重点介绍了存储保护、审计、最小特权等安全机制以及介绍主流操作系统 Windows 和 UNIX/Linux 操作系统的安全

机制；第7章介绍数据库安全机制，重点介绍数据库访问控制、审计、备份恢复、加密等安全技术，并以实际数据库管理系统SQL Server和Oracle为例，介绍安全技术在产品中应用情况；第8章介绍信息安全评估标准和我国的信息安全等级保护制度；第9章介绍信息安全风险评估的概念、工具、方法、流程；本书应用系统层安全从两个角度描述，一是防止应用程序对支持其运行的计算机系统的安全产生破坏，二是防止应用程序自身的安全漏洞被利用，这两部分内容分别体现在第10、11章，第10章介绍病毒、木马、蠕虫三类恶意代码的检测与防范技术，第11章介绍软件安全漏洞及防范措施，重点介绍了Web应用安全机制；第12章介绍信息安全新技术，包括云安全、物联网安全、移动安全等。

陈萍提出了教材的编写大纲，编写了其中第1、2、3、4、5、6、8、9、10、11章，赵敏负责编写第7、12章，张涛对教材编写提出了建设性的意见和技术支持。

由于作者自身水平有限，必有许多不足甚至错误之处，恳请读者和专家提出宝贵意见。

笔　者

2015.9

目　录

第1章　信息系统安全概述

随着计算机和网络技术的日益普及和广泛应用，信息的应用和共享日益广泛且更为深入，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。各种信息化系统已经成为国家基础设施，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。

与此同时，计算机信息系统的安全问题日益突出，情况也越来越复杂，针对计算机信息系统的攻击与破坏事件层出不穷，如果不对其加以及时和正确的保护，这些攻击与破坏事件轻则干扰人们的日常生活，重则造成巨大的经济损失，甚至威胁到国家安全。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，所以信息系统的安全问题已经引起许多国家的高度重视，人们不惜投入大量的人力、物力和财力来提高计算机信息系统的安全性。

本章对计算机信息系统安全问题进行了概述，1.1 节介绍目前信息系统面临的主要安全威胁，并指出安全问题的根源；1.2 节讲述信息系统安全的基本概念、发展历史、目标；1.3 节讲述信息系统安全防护的基本原则；1.4 节介绍信息系统安全的技术体系。

1.1　计算机信息系统安全问题

1.1.1　飞速发展的信息化

人类社会经历了农业社会、工业社会，现在已经进入到了信息社会，我国是信息大国，我国的信息化进程起步于 20 世纪 80 年代，经过 30 多年的建设，信息化已经具有一定的规模：信息网络（电信网、互联网和广播电视网）成为支撑经济社会发展的重要基础设施；信息产业成为重要的经济增长点；信息技术在国民经济和社会各领域得到了广泛应用。下面以互联网为例通过一组数据说明我国信息化的发展速度。

据中国互联网信息中心（CNNIC）统计，我国 2002 年网民数量为 5910 万人，截至 2015 年 6 月份达到了 6.68 亿，手机网民规模达 5.94 亿；中国互联网的普及率已经从 2005 年的 8.5%增加到了 2015 年的 48.8%，超过了全球平均水平，中国已经超越美国成为世界上互联网使用人数最多，发展速度最快的国家。

快速发展的信息化引起了人们生产方式、生活方式的巨大变化，极大地推动了人类社会的发展和人类文明的进步，电子政务、电子商务、网络课堂、电子邮件等已经与我们的生活息息相关，利用网络课堂我们可以随时随地聆听世界各地的名师讲课；利用电子商务，我们足不出户就可以购物等。信息化给我们的生活带来了极大的方便，社会对信息系统的依赖性也日益增强。

关于信息化，各国领导人均在不同场合下强调了其重要性：

谁掌握了信息，控制了网络，谁将拥有整个世界——美国著名未来学家阿尔温·托夫勒。

今后的时代，控制世界的国家将不是靠军事，而是信息能力走在前面的国家——美国前总统克林顿。

信息时代的出现，将从根本上改变战争的进行方式——美国前陆军参谋长沙利文上将。

1.1.2 信息安全形势严峻

信息化是一把双刃剑，信息化程度越高，信息安全威胁带来的危害也就越大。据美国金融时报报道，世界上平均每 20s 就发生一次入侵国际互联网的计算机安全事件。据《中国互联网状况》白皮书报道，我国被境外控制的计算机 IP 地址达 100 多万个，被篡改的网站 4.2 万个，被蠕虫病毒感染的计算机每月达 1800 万台，成为世界上被黑客攻击的主要受害国。信息安全已经渗透到国家的政治、经济、军事等领域。2013 年震惊全球的美国中央情报局前雇员斯诺登爆料的“棱镜门”事件，证实了美国一直以来对中国进行着全方位的监控，中国的信息安全形势十分严峻。信息安全对政治、经济、社会稳定、军事等都产生了巨大的影响。

1. 信息安全与政治

目前政府上网已经大规模地发展起来，电子政务工程已经在全国启动。政府网络的安全直接代表了国家形象。从 1999 年到 2001 年，我国一些政府网站曾遭受 4 次大的黑客攻击事件。

第 1 次在 1999 年 1 月左右，美国黑客组织“美国地下军团”联合波兰、英国的黑客组织及其他黑客组织，有组织地对我国的政府网站进行了攻击。

第 2 次是在 1999 年 7 月，李登辉提出两国论的时候。

第 3 次是在 2000 年 5 月，美国轰炸我国驻南联盟大使馆后。

第 4 次是在 2001 年 4 月至 5 月，美国战机撞毁王伟战机并侵入我国南海机场后。

从 2004 年以后，网络威胁呈现多样化，除传统的病毒、垃圾邮件外，危害更大的间谍软件、广告软件、网络钓鱼等纷纷加入互联网安全破坏者的行列，成为威胁计算机安全的帮凶。间谍软件的危害甚至超越传统病毒，成为互联网安全最大的威胁，因此目前，军队以及一些政府机关的计算机是不允许接入互联网的。

2008 年 5 月 1 日，我国颁布施行了《政府信息公开条例》，该《条例》的推行对政府信息化建设提出了新的要求，同时也对电子政务信息系统的网络安全提出了更高的要求。由于政府网站整体安全水平较低，往往是黑客攻击的重要目标，因此，作为政府对外形象的窗口、发布权威信息和与公众开放交流的平台，电子政务信息系统的网络安全管理是一个需要各级部门高度重视的问题。

2. 信息安全与经济

一个国家信息化程度越高，整个国民经济和社会运行对信息资源和信息基础设施的依赖程度也就越高，计算机犯罪造成的经济损失也就越大。1999 年 4 月 26 日，台湾大学生陈英豪编制的 CIH 病毒大爆发，据统计，我国受其影响的 PC 总量达 36 万台之多，经济损失高达 12 亿。2003 年的冲击波病毒(Worm_MSBLAST)造成了全球上百亿的经济损失，2006 年，能将计算机中的所有文件全部变成熊猫烧香图标的熊猫烧香病毒造成了上亿元的经济损失。表 1.1 列举了部分攻击事件造成的经济损失。

表 1.1　攻击事件造成的经济损失

年　份	攻击行为发起者	损 失 金 额
1998	CIH 病毒	8000 万美元
1999	梅利莎(Melissa)	全球约 3～6 亿美元
2000	Love Letter	88 亿
2001	红色代码	26 亿
2003	Worm_MSBLAST	上百亿
2006	熊猫烧香病毒	上亿
2007	网游大盗	千万

自从 1988 年计算机安全应急响应组(Computer Emergency Response Team,CERT)因 Morris 蠕虫事件成立以来,Internet 安全威胁事件逐年上升,近年来的增长态势变得尤为迅猛,从 1998 年到 2009 年,平均年增长幅度达到了 50%左右,这些安全事件带来了巨大的经济损失,以美国为例,其每年因为安全事件造成的经济损失超过 170 亿美元。

3. 信息安全与社会稳定

在互联网上散布虚假信息、有害信息对社会秩序造成的危害比起现实世界散布谣言所带来的危害更大,严重的会影响社会稳定。

1999 年 4 月,河南商都热线的一个 BBS 上,一张帖子发布虚假消息,说交通银行郑州支行行长携巨款外逃,造成社会动荡,3 天 10 万人上街排队,一天提款 10 多亿元。2010 年 8 月 10 日,一名 17 岁少年在"贴吧"上散布福建泉州地震的谣言,由于发布在知名度很高的网站上,引起全国各地网民关注,造成极为不良的影响,该少年 12 日下午即被警方抓获。

网络上的用户多种多样,尤其是近年来上网的用户越来越多,各种言论和服务很难规范。为了保证网上内容健康,2006 年 4 月 9 日,北京千龙网、新浪网等联合向全国互联网界发出文明办网倡议书,倡议互联网界文明办网,把互联网站建设成为传播先进文化的阵地。

4. 信息安全与军事

信息安全与军事紧密相关,在第二次世界大战中,美国破译了日本人的密码,几乎全歼山本五十六的舰队,重创了日本海军。信息时代的出现,从根本上改变了战争的进行方式,1991 年的海湾战争是一个分界点。1991 年海湾战争前,战争主要以机械化战争为主,而海湾战争后出现了以信息战为主的作战形态。下面介绍几个信息战的重要实例。

海湾战争:是 1991 年 1 月 17 日至 2 月 28 日,以美国为首的多国联盟在联合国安理会的授权下,为恢复科威特领土完整而对伊拉克进行的局部战争。美军通过向带病毒芯片的打印机设备发送指令,致使伊拉克军队系统瘫痪,轻易地摧毁了伊军的防空系统,多国部队运用精湛的信息技术,仅以伤亡百余人的代价取得了歼敌十多万人的成果。海湾战争被称为"世界上首次全面信息战",充分显示了现代高技术条件下"控制信息权"的关键作用。

科索沃战争:是 1999 年 3 月 24 日至 6 月 10 日,北约对南斯拉夫的空袭行动。在此次战争中美国的电子专家成功侵入了南联盟防空体系的计算机系统,当南联盟军官在计算机屏幕上看到敌机目标的时候,天空上其实什么也没有,通过这种方法,美军成功迷惑了南联盟,使南联盟浪费了大量的人力物力资源。

随着计算机和网络技术的发展，当前的军事战争是信息化战争，信息对抗的攻防能力已成为国防力量之一，利用病毒等作战的典型战例除了前述的海湾战争、科索沃战争外，2007年爱沙尼亚拆除了第二次世界大战苏联将士雕像，引起与俄罗斯的紧张关系，爱沙尼亚遭受网络攻击，政府、报纸银行、企业网站全部瘫痪。2010年为了打击伊朗的核武器制造计划，美国、以色列研发“震网”(Stuxnet)蠕虫，导致伊朗60%的计算机感染，离心机多次出现故障，从而延迟了伊朗的核武器制造计划。

面对严峻的信息安全形势，各个国家纷纷出台各项政策以增强信息系统安全防护能力，减少信息安全问题带来的损失。2003年美国发布了《国家网络安全战略》，正式将网络安全提升至国家安全的战略高度；2009年5月美国奥巴马新政府公布了《网络空间策略评估》，指出美国存在诸多网络安全隐患，表示将制定新的综合方案来保护国家信息基础设施。网络空间又称赛博空间(Cyberspace)，已经成为继陆、海、空、天之后新的战场空间，为了确保在未来网络战中拥有绝对的信息优势，2009年美国成立网络司令部，招募4000名黑客，组建特种部队，该部队主要担负网络攻防任务，并计划于2030年左右完成网络战部队的全面组建，英、俄、日、韩等国也已经组建或正在组建网络战部队。我国是受黑客攻击的主要受害国之一，为了提升网络信息安全防护能力，自2002年起相继召开了“国家信息安全保障体系战略研讨会”、“信息安全保障发展战略研讨会”等，并先后成立了多个研究机构和重点实验室，开展信息安全防护相关技术的研究。

1.1.3 信息系统安全问题的根源

按照我国颁布的《计算机信息系统安全保护等级划分准则》的定义，计算机信息系统是指由计算机及其相关的配套设备、设施(含网络)构成的，按照一定的应用目标和规格对信息进行采集、加工、存储、传输、处理的人机系统。

一个计算机信息系统由硬件、软件以及使用人员三部分组成。其中硬件系统包括组成计算机、网络的硬设备及其他配套设备。软件系统包括操作平台软件、应用平台软件和应用业务软件。操作平台软件通常是指操作系统和语言及其编译系统；应用平台软件通常是指支持应用开发的软件，如数据库管理系统及其开发工具、各种应用编译和调试工具等；应用业务软件是指专为某种应用开发的软件。

信息系统之所以是脆弱的，从技术的角度来看主要原因有以下三个。

1. 网络和通信协议的脆弱性

因特网技术给全球信息共享带来了方便，但是基于TCP/IP协议栈的因特网及其通信协议在设计时，只考虑了互联互通和资源共享问题，存在大量安全漏洞。例如要建立一个完整的TCP连接，必须要在两台通信的计算机之间完成三次握手过程，如图1.1所示，如果三次握手不能够完成，将处于半开连接状态(Half-open)，如图1.2所示，此时服务器端口一直处于打开状态以等待客户端的通信，这个特性往往会被攻击者利用。SYN Flooding拒绝服务攻击就是利用了TCP协议三次握手中的脆弱点进行的攻击，在SYN Flooding攻击中，攻击者向目标机发送大量伪造源地址的TCP SYN报文，这些报文的源地址是虚假的，或者是根本不存在的，当目标机收到这样的请求后，向源地址回复ACK+SYN数据包，由于源地址是假的IP地址，因此没有任何响应，于是目标机继续发送ACK+SYN数据包，并将该半开放连接放入端口的积压队列中，虽然一般系统都有默认的回复次数和超时时间，但由于端

口积压队列的大小有限，如果不断向目标机发送大量伪造 IP 的 SYN 请求，就会形成通常所说的端口被“淹”的情况，使目标机不能提供正常的服务功能。

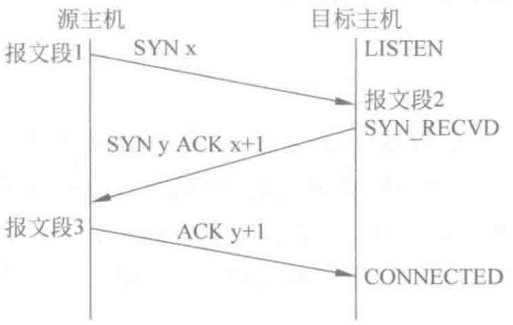

图 1.1　TCP 连接成功

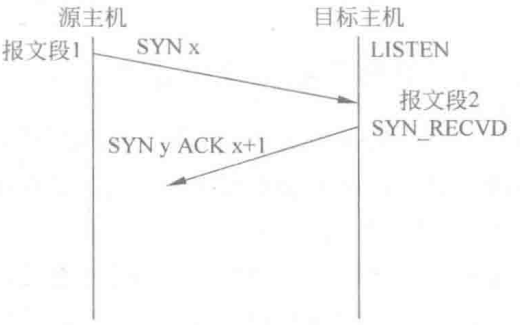

图 1.2　TCP 半连接状态

2. 信息系统的缺陷

信息系统主要由硬件和软件构成，硬软件自身的缺陷客观上导致了计算机系统在安全上的脆弱性。计算机硬件系统由于生产工艺的原因，存在电路短路、断线、接触不良、电压波动的干扰等安全问题；而计算机软件的问题主要受人们认知能力和实践能力的局限性，在系统设计和开发过程中会产生许多错误、缺陷和漏洞，成为安全隐患，而且系统越大、越复杂，这种安全隐患越多。有专家指出：程序每千行中至少有一个缺陷，而目前一个大型软件通常有数百万甚至数千万行语句，这就意味着一个软件可能有几万个差错，随着系统的功能越做越强大，复杂性也不断增加，错误会越来越多。

3. 黑客的恶意攻击

人的因素是影响信息安全问题的最主要因素，人的恶意攻击也称为黑客攻击。早在 20 世纪 60 年代至 70 年代，黑客一词是褒义的，他们是独立思考、奉公守法的计算机迷，典型代表有微软的盖茨、苹果公司的伍茨和乔布斯。当今黑客是指专门闯入计算机系统、网络、电话系统和其他通信系统，具有不同的目的，非法入侵和破坏系统、窃取信息的攻击者。

随着网络的发展，黑客组织越来越扩大化，现在跨地区、跨国界的大型黑客组织已经出现，行动越来越公开化，如每年的黑帽(Black Hat)大会就是全球最大规模的黑客聚会。2008 年 8 月，第 12 届 BlackHatUSA 大会在美国内华达州拉斯维加斯的凯撒皇宫酒店揭开帷幕，在为期两天的会议中，共有来自全球的超过 4500 名参会者针对各种攻击技术进行广泛交流，美国政府也借此会议乘机招募黑客人才。2009 年 3 月，在加拿大温哥华市举行了名为 Pwn2Own 的 2009 年全球黑客大赛，包括 IE8 在内的多套软件被攻破。同时由于存在大量公开的黑客站点，获得黑客工具非常容易，黑客技术也越来越易于掌握，黑客案件越来越频繁化，网络面临的威胁也越来越大。据权威机构调查显示，计算机攻击事件正以年 50%以上的速度增加。如 2008 年上半年，国内外黑客组织对我国网站攻击频繁，平均每天就有数百起网站被黑以及网页被篡改的事件发生，其中来自土耳其的黑客组织 reDMin、sinaritx 等表现活跃。