中国高等教育学会工程教育专业委员会新工科“十三五”规划教材

Information System Security

信息系统安全

黄 杰 / 编著

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

中国高等教育学会工程教育专业委员会新工科“十三五”规划教材

Information System Security

信息系统安全

黄 杰 / 编著

ZHEJIANG UNIVERSITY PRESS
浙江大学出版社

图书在版编目(CIP)数据

信息系统安全 / 黄杰编著. -- 杭州 : 浙江大学出版社, 2020.1
ISBN 978-7-308-19784-7

Ⅰ. ①信… Ⅱ. ①黄… Ⅲ. ①信息系统—安全技术
Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2019)第266687号

信息系统安全

黄 杰 编著

责任编辑 吴昌雷
责任校对 刘 郡
封面设计 北京春天
出版发行 浙江大学出版社
(杭州市天目山路148号 邮政编码310007)
(网址:http://www.zjupress.com)
排 版 杭州朝曦图文设计有限公司
印 刷 杭州杭新印务有限公司
开 本 787mm×1092mm 1/16
印 张 17.25
字 数 410千
版 印 次 2020年1月第1版 2020年1月第1次印刷
书 号 ISBN 978-7-308-19784-7
定 价 45.00元

前　言

网络空间已成为继陆地、海洋、天空、外空之外的第五空间。“没有网络安全，就没有国家安全”“加强网络空间安全人才建设，打造素质过硬、战斗力强的人才队伍”“要培养造就世界水平的科学家、网络科技领军人才、卓越工程师、高水平创新团队”，网络空间安全人才的培养成为国家战略需求，而《信息系统安全》是网络空间安全人才培养的基本专业教材之一。“新工科”是在新科技革命、新产业革命、新经济背景下工程教育改革的重大战略选择，它服务于国家战略发展新需求，构筑国际竞争新优势，落实立德树人新要求。根据“网络空间安全新工科”的要求，参照《高等学校信息安全专业指导性专业规范》所列知识点，结合编者的教学、科研实践，编写了本教材。

本书中的信息系统安全，强调的是信息系统整体上的安全性，即为运行在其上的系统（应用）、处理的数据和执行的操作（行为）提供一个安全的环境，并针对该环境如何评估、如何管理以及出现安全事件后如何应对等整个环节所涉及的关键安全技术进行了讲解。本书内容共12章，分为3个部分：信息系统安全体系结构、信息系统关键安全技术、信息系统安全管理。其中第1章和第2章属于信息系统安全体系结构部分，第3章至第9章属于信息系统关键安全技术部分，而第10章至第12章属于信息系统安全管理部分。

第1章“信息系统安全概述”，它是全书的概论，从信息系统安全面临的挑战开始，介绍信息系统安全的基本概念、研究内容和研究方法，介绍信息系统安全的需求。本章是全书的基础，对后面章节的学习有指导作用。第2章“信息系统安全体系结构”，从系统的角度讨论系统安全，为此，首先探讨信息系统安全体系架构的模型，将信息系统安全体系结构分为技术体系、组织体系和管理体系，并在此基础上讨论其三维模型。然后，描述信息系统安全体系结构的发展历程。最后，讨论5种典型的信息系统安全体系结构，即基于协议的安全体系结构、基于实体的安全体系结构、基于对象的安全体系结构、基于代理的安全体系结构和基于可信计算的安全体系结构。

第3章至第9章分别讨论信息系统安全所涉及的关键安全技术。第3章“物理安全”，从环境安全和设备安全出发，讨论所涉及的安全技术，然后以GB 50174-2008标准为例，探讨物理安全等级保护的相关内容。第4章“身份认证技术”，它是系统安全的基础技术之一，本章主要是从公钥密码技术、生理特征识别技术和行为特征识别技术等三个方面，探讨身份认证方法。第5章“访问控制技术”，主要讨论访问控制的基本概念、分类和模型；讨论两类基于所有权的访问控制技术，即自主访问控制技术和强制访问控制技术，阐述它们的原理、特点和模型；讨论基于任务的访问控制技术，阐述它的原理、特点及其典型的模型；讨论基于角色的访问控制技术，阐述它的原理、特点、典型模型及其变种；讨论基于属性的访问控制技术等。第6章“操作系统安全”，分别讨论典型操作系统：Windows操作系统、Linux操作系统、Android操作系统的安全框架、安全模型和基本安全

机制。第7章“数据库系统安全”，从数据库的安全问题出发，详细分析数据库的安全策略和安全机制，重点讲解数据库的加密机制、数据库审计、数据库的备份与恢复技术。第8章“入侵检测”，主要讲解入侵检测的基本概念、分类和作用，入侵检测技术的常用方法，以及两种类型的入侵检测系统，即基于网络的入侵检测系统和基于主机的入侵检测系统，最后讲解了入侵检测系统的评估方法。第9章“可信计算”，主要讲解可信计算的基本概念、特征和应用。然后从可信计算基和可信计算平台讲解可信计算技术，讲解静态可信认证、动态可信认证，以及信任链。

第10章至第12章分别对信息系统安全管理、评估和应急处理方面进行了讨论。第10章“信息系统安全管理”，从信息系统安全管理的概念和标准出发，分别讲解系统安全管理的措施和安全审计的方法。第11章“信息系统安全风险评估和等级保护”，主要讲解信息系统安全评测方法和技术，系统安全风险评估模型和系统的安全等级保护等。第12章“信息安全应急响应”，从应急响应的概念出发，讲解应急预案和响应的制定方法，以及应急响应处置机制等。

本书作为网络空间安全专业必修课教材，适用于有操作系统、数据库系统、密码学、计算机组织与结构、计算机网络等相关基础的读者，也可作为大学基础专业课教学使用。

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

目　录

第1章

信息系统安全概述

信息技术的飞速发展不仅促进了社会经济的发展和进步，而且正全面改变人们的生产生活方式，同时也为网络空间安全带来了新的威胁和挑战。信息系统是信息和信息技术的载体，它已经成为国家重要基础设施乃至整个经济社会的神经中枢，一旦遭受攻击，将导致能源、交通、金融、水利、医疗、教育、新闻、国防等基础设施的瘫痪，从而带来灾难性后果，严重危害国家政治经济、社会稳定和国防安全。

信息安全主要包括四个层面，即系统安全、数据安全、内容安全和行为安全，其中数据安全和内容安全就是传统的信息安全，即狭义信息安全，它强调的是信息本身的安全属性，而系统安全是本书主要研究的内容，即信息系统安全，它是信息安全的首要问题。信息系统安全强调信息系统整体上的安全性，即为运行在其上的系统（应用）、处理的数据和执行的操作（行为）提供一个安全的环境。本章是全书的概论，将从信息系统安全面临的挑战开始，介绍信息系统安全的基本概念、研究内容和研究方法，介绍信息系统安全的需求。本章是全书的基础，对后面章节的学习有指导作用。

1.1 信息系统安全面临的挑战

1.1.1 信息系统的发展历程

信息系统是指信息产生、存储、处理、传输和使用的人-机一体化计算机系统，包括：计算机硬件、软件、固件、网络和人员。信息系统的发展与计算机技术和网络技术的发展密不可分，了解信息系统的发展历程，有助于了解信息系统安全目标的演化过程，进一步理解信息系统安全的内涵。

1.用户独占单机系统

这个时期是从20世纪40年代中期到60年代中期。其间产生了世界上第一台计算机，它是由成千上万的晶体管组成，只能识别0和1，操作人员只能通过纸带或磁带输入机完成程序和数据（穿孔的纸带或卡片）的输入，只有程序运行完毕并取走结果后，下一

个用户才能使用该机器，属于单用户单进程系统。此时，需要考虑的信息安全问题仅仅是物理安全问题，即：计算机电路被恶意修改或破坏，造成数据处理出错，但这不是严格意义上的信息安全问题，而且这种安全问题防范比较简单，只要严格管理设备就可以了。

60年代中期，计算机采用了小规模集成电路系统，CPU的处理能力更加高效，尽管此时计算机还是单用户独占，但用户提交的作业已经可以通过操作系统实现多进程并行处理了。此时，信息系统安全问题除了上述的物理安全外，还存在不同进程的保护问题，即：一个进程的数据不能写入另一个进程的地址空间。但这种问题只会引起数据处理的错误，不会产生数据机密性被破坏的问题，这是因为，此时只有一个用户使用该系统。

尽管这个时期已经出现了操作系统，但功能单一，在执行每个作业任务时，计算机系统仍然属于单用户独占状态，此时只要管理得当，不存在真正意义上的信息系统安全问题。

2.多用户主机共享系统

这个时期是从20世纪60年代中期到70年代末期。60年代中期，人们开始采用小规模集成电路制造计算机，用户可以在一台主机上同时完成多个作业，“多道程序”操作系统完成对多个作业的控制，此时操作系统具有作业调度管理、处理机管理、存储器管理、外部设备管理和文件系统管理等功能。而随后出现的分时操作系统使得多用户同时使用一台主机成为可能，此时多个用户可以通过只有显示器和键盘的终端设备同时使用主机，CPU、内存和硬盘等都可以共用。终端设备通过网络与主机连接，这是计算机网络的萌芽阶段，属于“单计算机网络”。此时计算机系统的安全问题已经不再局限于物理安全，还包括用户的数据可能被窃取、篡改，用户的身份可能被冒用，用户的访问权限可能被修改。

70年代中后期，计算机网络已经不再局限于“单计算机网络”，许多“单计算机网络”相互连接从而形成多个单主机系统相互连接的计算机网络。尽管此时的信息系统仍然属于“单计算机系统”，但是由于网络的连接，使得单个主机所遭受的安全风险成倍增加，不仅可能遭受来自本主机用户的上述安全威胁，还可能遭受来自其他主机用户的上述安全威胁。

这个阶段信息系统的安全主要由操作系统管理，即：由操作系统实现用户的身份认证和访问控制，以及事后的安全审计。

3.多用户联网信息系统

这个时期是20世纪80年代早期到90年代中期。大规模集成电路和超大规模集成电路在计算机系统中广泛使用，计算机的性能迅速提升，价格大幅降低，小型计算机和个人计算机应运而生。计算机上出现了磁盘操作系统(DOS)，计算机作为信息处理系统开始广泛应用于社会生活和工作的各个领域。同时计算机网络也从封闭的局域网发展为万维网，以太网产生。国际标准化(ISO)制定了开放系统互连(OSI)标准，从而产生了以资源共享为目标的计算机网络。此时，人们不仅能够通过计算机系统执行多进程，而且还可以通过网络远程访问和控制其他机器的数据和文件，实现计算机之间的协同工作，信息系统开始走向了网络化。但总的说来，此时的信息系统属于集中管理的系统。

这个时期由于网络的开放性，理论上，网络上的任何一台计算机都能够访问特定的

信息系统，此时的信息系统安全问题更加复杂，其遭受的安全威胁不仅来自局域网内部，更多的是来自外部网络。但是由于信息系统仍然是集中式管理，系统的边界非常清晰，因此，安全管理相对容易，防火墙技术可以抵御大部分网络威胁。

4.分布式信息系统

这个时期是从20世纪90年代中期开始至今。尽管集中式信息系统维护方便、管理简单，只要保护好中央计算机系统，信息系统的安全防护相对容易，但随着用户数量的增加和用户需求的差异化，集中式信息系统越来越复杂，运行速度越来越慢，很难实现对每个用户的需求和资源单独配置，这时出现了分布式信息系统。大型信息系统都采用分布式架构，如：网上银行服务信息系统、大型电子商务服务信息系统和云服务系统等。

分布式信息系统是指以计算机网络为基础，硬件或软件等组件分布在不同的网络计算机上，彼此之间仅仅通过消息传递进行通信和协调的信息系统。当用户向分布式信息系统提交服务请求时，他并不需要知道这个服务或数据来自哪个服务器，更无须关心服务器所在的位置。这时，我们会发现分布式信息系统的边界是模糊的。再如云服务系统，特别是公有云服务系统，不同用户或企业存储其上的数据或信息可能共用处理器、内存、磁盘，甚至网线，信息系统的边界更加模糊，或根本就没有，此时，以防火墙技术为中心的传统安全防护手段不再适用，需要全新的信息安全理念和架构。

1.1.2　信息系统安全风险和威胁

信息系统安全威胁是指由于信息系统存在软、硬件缺陷或系统集成缺陷，或软件协议等安全漏洞，以及信息安全管理中潜在薄弱环节，信息系统的组成要素和功能可能遭受破坏或无法实现预期目标的可能性。信息系统的安全风险是“绝对的”，无论是否意识到，安全风险都存在，它与人的行为密切相关。信息系统的任何安全风险或不确定事件都可能造成损失。

1.信息系统的安全风险

信息系统的安全风险主要来源于系统的脆弱性，即安全漏洞，而且这种安全风险是全方位的，动态变化的。

(1)电磁泄漏。电磁泄漏是指寄生(杂散)电磁能量或谐波通过地线、电源线、信号线或空间向外扩散。任何处于工作状态的信息系统的设备都存在不同程度的电磁泄漏，如果这些泄漏携带了设备处理的信息，则称为电磁信息泄漏。利用专有设备，这些信息被接收后都能被还原。

信息系统的设备电磁泄漏主要有两个途径：一是通过电磁波向空中发射电磁信号，称为辐射泄漏。设备的印刷电路板、传输线和显示器中出现电流变化时，都会产生磁场，从而将电磁波向空中辐射出去。二是传导泄漏，即通过各种线路将电磁能量传导出去，如电源线、信号线、地线或机房网线等将电磁信号传导出去，造成电磁泄漏。

(2)芯片的脆弱性。一颗集成电路芯片是由成千上万，甚至上亿的晶体管构成，如：Intel 酷睿2四核Q6600的CPU内核，其晶体管数量是5亿8200万个。如果芯片存在设计缺陷，甚至是人为在某些晶体管上加上“后门”，那么必然会导致处理的信息被泄露。

芯片的脆弱性属于硬件安全问题，它与软件脆弱性不同。软件的脆弱性是由于人的疏忽造成的，既可能是设计者也可能是使用者。这种脆弱性的解决途径可以通过软件的不断升级，或规范使用者行为的方式解决，但是芯片的脆弱性很难在后天补救。

以微处理器的两大安全漏洞——“Meltdown”（崩溃）和“Spectre”（幽灵）为例，这两个漏洞能让黑客窃取计算机的全部内容，包括移动设备、个人计算机，以及云服务器。“Meltdown”漏洞破坏了用户和操作系统之间的基本隔离，允许低权限的用户“越界”访问核心内存。目前的解决办法是采用软件升级或系统打补丁，但计算机的运行速度会下降30%左右。而“Spectre”（幽灵）破坏了不同应用程序之间的隔离，其问题的根源在于“推测执行（speculative execution）”这一优化技术，允许低权限的应用程序访问核心内存。针对此类漏洞可能需要重新设计处理器。

（3）操作系统的安全漏洞。操作系统的安全漏洞是指操作系统软件在设计上的缺陷或错误。这些漏洞一旦被不法者利用，就能通过网络植入木马或病毒，从而攻击甚至控制整个信息系统，窃取系统中的重要资料和信息，甚至破坏系统。产生漏洞的原因主要是由于程序员的能力和经验不足，或某种不可告人的目的而导致系统产生的漏洞，也可能是为了后期的调试，故意留下的“后门”；或是由于硬件设计缺陷或不兼容性导致的硬件漏洞，使程序员在程序设计时无法弥补这些硬件漏洞，从而使硬件问题通过软件表现出来。

以Windows操作系统的两个漏洞——BadTunnel漏洞和Unicode漏洞为例。BadTunnel漏洞是Windows历史上影响最广泛的漏洞，涵盖所有的Windows系统。该漏洞为原始设计问题，当用户打开一个网址，或者打开任意一种Office文件、PDF文件或者其他格式的文件，或者插上一个U盘，攻击者都可以利用该漏洞劫持整个目标网络，获取权限提升。Unicode漏洞是在IIS4.0/5.0中，Unicode字符解码时的一个漏洞，可以导致用户远程通过IIS错误地打开或执行Web根目录以外的文件，如CMD.EXE，从而随意执行和更改目标计算机上的任意文件。

（4）数据库的安全漏洞。数据库是信息系统常见的数据存储工具，里面存储了大量有价值的或敏感的数据，特别是在大数据时代，数据库被广泛应用于各种场景中。在传统的信息系统建设中，数据库安全往往被忽略，这主要是由于在传统的安全防护体系中，数据库处于被保护的核心位置，不易被外部攻击，因此从表面上看已足够安全。但不断涌现的数据泄露事件，暴露了这种防御思想的致命缺陷，如：Equifax公司1.43亿信用卡信息泄露，5000万名Uber客户个人信息泄露和京东50亿条公民信息泄露等。

数据库出现安全漏洞的原因很多，主要可以归结为以下几个方面：

①数据库自身存在安全缺陷。数据库中的数据是存储在物理文件中的，无论是数据文件、备份文件还是日志文件，虽然其自定义了存储格式，但其文件的组织结构是公开的，只要得到这些数据文件，就能获取存储的数据。此外，还包括提权漏洞、缓冲区溢出漏洞和系统注入漏洞等。

②错误部署和配置。数据库的错误或不严谨部署与配置，使得数据库面临安全风险。数据库部署后，其出厂设置和薄弱的配置，使其非常容易遭受来自外部的攻击。如由于数据库部署问题，使其暴露在公共网络中，成为被直接攻击的目标。而共享服务账

号由于难以被监控和权限较大，可能带来很大的安全风险。不必要的服务和应用，增加了攻击者可以利用的攻击面。

③SQL注入。SQL注入不仅仅是最常见的数据库漏洞，而且是其头号安全威胁。通过SQL注入可以使攻击者通过SQL查询语句注入攻击代码，从而达到读取敏感数据，修改数据，执行管理操作乃至向操作系统发出指令等目的。由于程序员在开发过程中不注意书写规范，对SQL语句和关键字没有进行过滤，从而导致应用程序可以提交恶意代码到服务器后正常运行。

(5)通信协议的安全漏洞。现代信息系统是以计算机网络为基础的，网络连接是其基本的功能和特性，如果此时应用于信息系统的通信协议存在安全漏洞，那必然会威胁到系统本身的安全。通信协议出现安全漏洞主要是以下几个原因：

①协议的开放性。通信协议的开放性是为了方便网络互联，但是这也为非法入侵者提供了便利，他们可以假冒合法的用户篡改信息，窃取报文内容，甚至攻击信息系统。

②协议的设计缺陷。有些通信协议，如TCP/IP协议，在设计之初，并没有考虑其安全问题。信息系统针对TCP/IP协议提供的服务是基于IP地址进行认证和授权的，但由于IP地址缺乏有效的认证和保密机制，因此，系统无法阻止攻击者伪造IP地址。

③代码实现的缺陷。为了解决TCP/IP协议的先天安全缺陷，人们采取了很多措施，其中SSL(安全套接层)协议就是使用最为普遍的安全协议，它位于传输层和应用层之间，可以说是TCP/IP协议的安全补丁。OpenSSL是实现SSL协议的开源代码，能实现网络通信的高强度加密，然而它在2014年却爆出了严重的安全漏洞，使得黑客可以任意监控登录的用户名和密码。

(6)移动存储介质的安全漏洞。移动存储介质具有体积小、携带方便、容量大和通用性强的特点，因此被广泛应用于数据存储的载体。如果移动存储介质在信息系统之间随意使用，极易造成病毒感染和传播，引发泄密事件。也有可能将内部介质非法带出使用，造成数据外泄。为此，可以对移动存储介质实施分密级保护，规定不同密级实体之间的访问规则，如高密级移动存储介质不能在低密级信息系统上使用，高密级电子文件不能存储在低密级存储设备上，等等。对移动存储介质的安全防护主要还是通过管理的手段，这部分内容不在本书的讨论范围内。

2.信息系统的安全威胁

信息系统的安全威胁主要来源于自然因素和人为因素。自然因素造成的威胁是一种偶发性威胁，它由不可抗力或偶发性事件构成，具有发生概率小、随机性大的特点，如断电、鼠害、设备的自然老化、电磁干扰、恶劣的场地环境和地震洪灾等意外事故或自然灾害，这部分内容不是本书的研究内容。与自然因素的威胁相比，人为因素的威胁是精心设计的人为攻击威胁，难防备，种类多，数量大。从对信息的破坏性上看，这种威胁类型可以分为被动威胁和主动威胁。本书主要研究人为因素对信息系统造成的安全威胁，归纳起来主要包括以下几个方面：

(1)物理攻击。物理攻击是通过物理接触信息系统及其周边设备的方式，对信息系统的硬件、软件和数据产生破坏。如人为(有意)电磁干扰，攻击者人为将电磁波能量引入信息系统的电气或电子部分，使系统的正常工作受到干扰，运行出现紊乱，甚至电子线

路遭到破坏。或通过获取系统的登录账号和密码,攻击信息系统,窃取有价值或秘密信息。或信息系统安装了携带恶意代码或病毒的软件后,被攻击或破坏,不过这种攻击行为往往发生在互联网发展的早期,其中最著名的事件是20世纪80年代初,苏联克格勃间谍从一家外国公司盗取了一套急需的工业控制软件,并将该软件用在整条泛西伯利亚天然气管道上进行测试,但他们不知道的是美国情报机构早已经在软件中放置了逻辑炸弹等着他们上当。1982年6月,软件中暗藏的逻辑炸弹被触发,泛西伯利亚天然气管线发生了相当于3000吨TNT炸药当量的特大爆炸,连当时的卫星都能观测到。而在1999年3月,美国使用了尚在试验中的微波武器对南联盟进行轰炸,造成南联盟部分地区通信设施瘫痪3个多小时。伊拉克战争中,美军于2003年3月26日,用电磁脉冲弹空袭伊拉克国家电视台,造成其信号转播中断。

(2)网络攻击。网络攻击是目前最常见的安全威胁,它是利用网络设备或协议存在的漏洞或安全缺陷对信息系统的硬件、软件及其数据进行攻击的行为。攻击者通过寻找系统的弱点,以非授权的方式达到破坏、假冒、伪造、篡改和窃取数据信息等目的。

网络攻击的破坏程度与信息化程度成正比。据中国互联网络信息中心(CNNIC)发布的《中国互联网络发展状况统计报告》显示:截至2019年6月,我国网民规模达8.54亿,互联网普及率达61.2%,而手机网民规模达8.47亿,网民使用手机上网的比例达99.1%。"提速降费"推动移动互联网流量大幅增长,用户月均使用移动流量达7.2GB,为全球平均水平的1.2倍。而据国家互联网应急中心(CNCERT)报告,2019年上半年,我国境内互联网上用于MongoDB数据库服务的IP地址约2.5万个,其中存在数据泄露风险的IP地址超过3,000个,涉及我国一些重要行业。"零日"漏洞收录数量占比43.3%,同比增长34.0%。我国境内峰值超过10Gbps的大流量分布式拒绝服务(DDoS)攻击事件数量平均每月约4,300起,同比增长18%,而且随着我国"感知中国""智慧城市"和"一带一路"建设,信息化程度还将进一步提高,因此我国面临网络攻击的威胁将与日俱增。

从目前的形势看,网络攻击的动机已经从早期的炫耀技术转向了获取利益目的,无目的蠕虫扩散行为已成为过去,针对特定群体的信息窃取、勒索甚至是破坏行为成为网络攻击的新趋势。其攻击行为的组织性更强,目标更加明确和直接,入侵者的专业能力更强,甚至在攻击过程中有严格的分工,同时攻击的目的性更强,以获取巨额经济利益或政治利益为目的。

(3)恶意代码。恶意代码又称恶意软件,是指在用户不知情或未授权情况下潜入信息系统,在信息系统上安装运行,对信息系统产生威胁或潜在威胁的计算机代码。恶意代码包括:计算机病毒、木马、蠕虫、僵尸、逻辑炸弹、后门、广告软件、勒索软件、间谍软件和恶意共享软件等。恶意代码的共同特点是它们都是计算机程序,都带有恶意的目的,但只有通过执行才能发挥作用。恶意代码的传播方式有多种,既可以通过软件漏洞传播,也可以通过社会工程中的某种方式传播,还可以通过文件或邮件传播。

恶意代码一旦入侵信息系统,轻则引起信息系统资源的过度消耗,侵占系统的存储空间,使系统的运行速度或网络连接能力下降,影响系统的性能,重则引起系统瘫痪,危害系统中的数据文件安全存储和使用,甚至泄露用户的隐私。对于上述已有的恶意代码,其防范手段或技术主要包括:恶意代码分析技术、误用检测技术、权限控制技术和完