新编高等院校信息管理与信息系统专业核心教材

信息系统安全导论

方摇勇摇刘嘉勇摇编著
戴宗坤摇罗万伯摇审校

北京·月球表面

图书在版编目（悦陨孕）数据

信息系统安全导论 辕方勇，刘嘉勇编著援—北京：电子工业出版社，圆园园猿
新编高等院校信息管理与信息系统专业核心教材
陨杂月晕 苑原缘园猿原园愿源远猿原圆

Ⅰ郾信…摇Ⅱ援①方…②刘…摇Ⅲ郾信息系统—安全技术—高等学校—教材摇Ⅳ郾栽孕猿园怨

中国版本图书馆 悦陨孕数据核字（圆园园猿）第 园苑远远猿源号

责任编辑：韩同平
印　　刷：
出版发行：电子工业出版社摇澡贼贼责：辕辕憎憎憎援责澡藻蚤援糟燥皂援糟灶
　　　　　北京市海淀区万寿路 员苑猿信箱摇邮编 员园园园猿远
经摇摇销：各地新华书店
开摇摇本：苑愿苑伊员园怨圆摇员辕员远摇印张：圆缘援缘摇字数：缘苑远千字
版摇摇次：圆园园猿年 源月第 员版摇圆园园猿年 源月第 员次印刷
印摇摇数：缘园园园册摇定价：猿圆援园园元

摇摇凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。联系电话：（园员园）远愿圆苑怨园苑苑

前　言

QIANYAN

本书针对高等院校信息管理与信息系统、计算机、通信、信息安全等专业的本科生和硕士研究生的教学特点，更加强调理论和工程技术应用相结合而编写的教材。

本书的重点在于给出信息系统安全的基础理论背景知识、信息系统安全体系结构、开放系统互连安全框架及其机制性技术、系统安全技术和基本知识。在系统安全技术方面，对信息系统的入侵与攻击技术、防火墙技术、入侵检测与监控技术、物理隔离技术及防病毒技术的主要内容进行了介绍，并给出了一部分具体的运用方案。本书特别通过对信息系统安全的五大安全服务和多种实现机制的较为完整而系统的介绍，使读者能系统地了解并掌握信息系统安全体系的构建方法、信息系统安全框架及其实现机制的主要内容。

本书由两部分构成。第一部分包括第1章，从信息系统和信息系统安全的层次结构引出与信息系统安全有关的问题，并从信息系统风险控制点及其对抗措施梗概和安全工程方法论方面为第二部分进行了必要的准备和铺垫。第二部分包括第2～6章，从信息系统安全体系的构建方法出发，对安全框架、安全服务和安全机制进行了较为详细的介绍，比较完整和系统地给出了信息系统安全体系的架构及支持技术。重点讨论了防火墙技术、入侵检测与漏洞扫描技术、物理隔离技术，同时对恶意程序与病毒对计算机及网络系统的威胁及其对策，以及技术实现方法进行了讲解，并对PKI做了较为详细的介绍。全书涉及的内容十分广泛，本科生或研究生在学习时，可根据学时数在内容、重点和深度方面进行选择。

本书由四川大学信息安全研究所组织编写，戴宗坤教授做了全书的结构设计和统筹，并由戴宗坤和罗万伯教授对全书进行了审校。方勇编写第1，4，6章及第5章的5.3节，其余部分由刘嘉勇编写。

四川大学信息安全研究所全体同志为本书的编写提供了优越的工作环境和多方面的帮助。本书的编写还从其他同行的著作（包括网站）中得到了帮助。作者在此一并表示衷心的感谢。

由于作者水平有限，且本书涉及较多新概念、新内容和研究课题，再加上技术发展很

快，因此，本书中难免存在缺点和错误，诚望读者批评赐教，为推动我国信息系统安全工程高级技术人才的培养共同出力。

作　　者

于四川大学信息安全研究所

目　录

M U L U

第1章

绪　　论

本章基于信息系统的基本概念，描述了信息系统安全的内涵和方法论，指出了信息系统存在的风险和系统的安全需求、信息系统常见的威胁和防御策略，阐述了信息系统的安全要素。

1.1 信息系统概述

1.1.1 信息系统的定义

所谓系统，是指由相互联系、相互作用又相互依存的若干单元组成的，具有一个共同目标的有机整体；从数学角度看，系统又是具有某一或某些共同属性的元素的集合。

关于信息系统的概念存在多种视线角度的定义。信息系统这种与“信息”有关的“系统”，其比较流行的定义有：

①《大英百科全书》把“信息系统”解释为：有目的、和谐地处理信息的主要工具是信息系统，它对所有形态的信息（原始数据、已分析的数据、知识和专家经验）和所有形式的信息（文字、视频和声音）进行收集、组织、存储、处理和显示。

② 巴克兰德（M.Buckland）认为信息系统是“提供信息服务，使人们获取信息的系统，如管理信息服务、联机数据库、记录管理、档案馆、图书馆、博物馆等”。

③ 达菲（N.M.Dafe）等认为信息系统大体上是“人员、过程、数据的集合，有时候也包括硬件和软件。它收集、处理、存储和传递在业务层次上的事务处理数据和支持管理决策的信息”。

④ 中国学者吴民伟认为信息系统是“一个能为其所在组织提供信息，以支持该组织经营、管理、制定决策的集成的人机系统。信息系统要利用计算机硬件、软件、人工处理、分析、计划、控制和决策模型，以及数据库和通信技术”。

可见，对信息系统的定义是同中有异，异中有同。不过，如将信息系统涉及的功能与范围加以适当界定，就可大体统一为两种定义。广义的信息系统包括的范围很广，各种处理信息的系统都可称为信息系统，包括人体本身和各种人造系统；狭义的信息系统仅指基于计算机的系统，是人、规程、数据库、硬件和软件等各种设备、工具的有机集合，它突出的是计算机、网络通信、信息处理等技术的应用。本书所研究的内容则将信息系统划在后一种定义的范畴。

1.1.2 信息系统的发展过程

从概念上讲，信息系统在计算机问世之前就已存在。自 20 世纪初泰罗创立科学管理理论以后，管理科学与方法技术得到迅速发展。在它同统计理论和方法、计算机技术、通信技术等相互渗透、相互促进的发展过程中，信息系统作为一个专门领域迅速形成。

作为用计算机处理信息的人机系统，信息系统在近半个世纪以来得到了迅猛发展。信息系统的发展经历了以下几个阶段：

① 电子数据处理系统（EDPS, Electronic Data Processing System）。电子数据处理系统是用计算机模仿手工管理方式，进行事务性数据处理的系统，所以也被称为事务处理系统（TPS, Transaction Processing System）。这一阶段从 20 世纪 60 年代初开始，用计算机计算工资、打印报表等。电子数据处理系统有一些缺陷，局部模拟了人工系统，受限于当时计算机的处理能力和人们对计算机的认知程度，数据收集因速度慢且容易出错等成为该系统最薄弱的环节。

② 管理信息系统（MIS, Management Information System）。管理信息系统是在事务处理系统基础上发展起来的第二代信息系统，但两者有显著的区别：事务处理系统是处理和获取数据，仅涉及一个部门内的操作性活动；管理信息系统则为管理提供信息，是一个部门的管理工具，它强调管理方法和技术的应用，强调把信息处理的速度和质量扩大到组织机构的所有部门，从而增强组织机构中各职能部门的管理效率和能力。

③ 决策支持系统（DSS, Decision Support System）。决策支持系统是面向半结构化决策问题，支持中高级决策者决策活动的人机信息系统。它是辅助决策工作的一种信息系统，其重点在“支持”而非决策工作的自动化。

④ 办公自动化系统（OAS, Office Automation System）和多媒体信息系统（MMIS, Multimedia Information System）。严格地说，办公自动化系统和多媒体信息系统是电子数据处理系统（或事务处理系统）、管理信息系统和决策支持系统等几类信息系统的一种综合应用，它们并不是新型的信息系统。但是，正是办公自动化系统在 20 世纪 80 年代的广泛应用，以及多媒体信息系统在 20 世纪 90 年代的兴起，才使信息系统这一领域更加引人注目，而多媒体信息系统自身也成为各类信息系统应用的方向。

根据信息系统的特点，可以用表 1.1 来说明信息系统的各阶段。

表 1.1　信息系统的各阶段

阶段	系 统 类 型	特　　点
1	数据处理系统	完成机械任务
2	事务处理系统	用计算机处理代替手工程序
3	管理信息系统	提供用于管理决策过程的信息
4	决策支持系统	为决策提供信息，并成为实际决策过程的一个组成部分

1.2　信息系统安全

1.2.1　基本概念

信息系统安全，指的是信息系统的安全，而不是信息的系统安全。当人们谈及与计算机网络（或 Internet）有关的信息系统的安全时，往往说成是信息安全。一般意义上，信息

安全与信息系统安全是安全集与安全子集的关系，具有包含与被包含的关系。因为信息安全有着更广泛、更普遍的意义，它涵盖了人工和自动信息处理的安全。网络化与非网络化的信息系统安全，泛指一切以声、光、电信号、磁信号、语音及约定形式等为媒体的信息的安全，一般也包含以纸介质、磁介质、胶片、有线信道及无线信道为媒体的信息，在获取（包括信息转换）、分类、排序、检索、传递和共享中的安全。

在本书中，我们将信息系统安全定义为：确保以电磁信号为主要形式的、在计算机网络化（开放互连）系统中进行自动通信、处理和利用的信息内容，在各个物理位置、逻辑区域、存储和传输介质中，处于动态和静态过程中的机密性、完整性、可用性、可审查性和抗抵赖性，与人、网络、环境有关的技术安全、结构安全和管理安全的总和。这里的人指信息系统的主体，包括各类用户、支持人员，以及技术管理和行政管理人员；网络则指以计算机、网络互连设备、传输介质、信息内容及其操作系统、通信协议和应用程序所构成的物理的与逻辑的完整体系；环境则是系统稳定和可靠运行所需要的保障体系，包括建筑物、机房、动力保障与备份，以及应急与恢复体系。

从系统过程与控制角度看，信息系统安全就是信息在存取、处理、集散和传输中保持其机密性、完整性、可用性、可审计性和抗抵赖性的系统辨识、控制、策略和过程。

- 系统辨识是近代控制理论的一个方面，它研究如何建立系统的数学模型，内容包括模型类型的确定、参数估计方法和达到高精度估计的试验设计方法。
- 控制指信息系统根据变化进行调整，使信息系统保持特定的状态（即动态平衡状态）。因此，调整的方向和目标就是使信息系统始终处于风险可接受的幅度内，并且逐步收敛至风险趋于最小。
- 策略就是针对信息系统安全面临的系统脆弱性和各种威胁，进行安全风险分析，确定安全目标，建立安全模型和安全等级，提出控制对策，并对信息系统安全进行评估、制定安全保障和安全仲裁等对策。
- 过程指信息系统状态的变化在时间上的持续和空间上的延伸。过程和状态不可分割，两者相互依存、相互作用和相互制约。信息系统的状态决定和影响着过程，而过程又决定和影响着新的状态（或过程）。

上述定义源于两种研究方法，一是将信息系统的安全作为状态来研究；二是将信息系统的安全作为对状态的控制调节来研究，控制调节的目的就是使系统安全稳定在某一可控的特定状态内。

信息系统安全是一个多维、多层次、多因素、多目标的体系，虽然信息系统安全的惟一和最终目标是保障信息内容在系统内的任何地方、任何时候和任何状态下的机密性、完整性和可用性，但是离开了信息系统安全的体系，孤立地和单纯地寻求直接保护信息内容的方法，显然是舍本逐末。信息系统依附于国家、组织机构和个人，它是国家、组织机构和个人应用业务与管理体系的网络化映射，以及集体智慧、个人思维和行为能力的延伸。

为此，需要将信息系统安全的完整内涵与信息安全方法论匹配起来，有必要从方法论的角度去理解和构造信息系统安全体系或模式。

信息系统安全方法的要点是：①信息系统是一项系统工程，由信息系统功能性工程与确保信息系统按照管理者要求的可靠、稳定、有序地实现其功能的安全性工程有机地结合起来；②信息系统功能性工程的各组件要素应具备相应的支持功能和履行功能的能力；③信息系统功能性工程各组件要素，在实现系统功能过程中确保信息内容机密性、完整性和可用性可能存在的自身固有的脆弱性、缺陷和漏洞，以及可能遭到来自系统内部和外部的对系统的骚扰、入侵，对信息的窃听、截获、注入和修改等威胁与攻击；④针对上述问题，信息系统安全性工程从物理安全、环境安全、操作系统安全、通信安全、传输安全、应用安全及用户安全等方面，恰当地采用各种安全技术机制，在相应的信息系统功能性工程各组件要素上构建安全框架，直接或间接提供必要的安全服务。

很显然，信息系统安全性工程是一个嵌入到功能性工程中的分布式的集中管理分布式控制体系，是功能性工程的保障体系。这里有两个问题需要特别强调，一是系统工程（含安全性工程）内各组件要素可以是物化的设备和实体，也可以是虚化的设备和实体；二是各组件要素所提供的安全服务的强度级别应高于或等于信息系统总的安全强度级别。

1.2.2 信息保密与信息系统安全

就信息安全和信息系统安全而言，保证信息（内容）的保（机）密性是系统安全的基本目标之一。因此从信息保密性角度来看，信息（系统）安全涵盖了信息保密的内容。但是，保密作为一个特殊、独立的概念，在各个国家的各个历史进程中，作为涉及国家安全、社会稳定的信息和控制函数，具有对时间、空间的强制性和时效性特点。因此，与一般意义的信息安全中的机密性比较，虽然都是针对未授权者而言的，但保密却具有与一般意义上的信息保密性不同的其他特殊含义；同时保密技术还具有自己相对独立、更为广泛和完整的体系，以及国家对抗性特点，由此决定了保密技术和保密管理体系本身具有国家机密性特点。

在强调信息系统安全和保密时，是将保密作为安全策略的一部分而不仅是信息保密（机密）性指标来定义的。作为安全策略，保密还涉及对信息系统的信息密级进行划分和管理，对涉密网络和非涉密网络进行界定和管理，对保密技术和产品进行保密管理，对具有对抗性和敏感性的保密技术主体和客体实施控制等。显然，作为安全策略，保密是信息系统安全的功能性和管理性保障。国家对保密工作历来十分重视，从技术到管理形成了一个完整的体系。保密在信息系统安全中的作用和地位是不可取代的。

1.3 影响信息系统安全的因素

所谓信息系统的风险，是指对某个脆弱性可能引发某种成功攻击的可能性及其危害性的测度。当某个脆弱的资源价值较高，同时受到成功攻击的概率大时，风险也就越高；反之，当某个脆弱的资源价值较低，同时受到成功攻击的概率小时，风险也就越低。风险分析是信息系统安全需求分析的依据。通过风险分析可明确风险的类型及其影响范围，使系统针对可能的风险采取相应的防护措施体系。

信息系统的风险分析可分为三个层次。首先是对信息系统的静态风险分析，在系统设计和运行前对其可能面临的风险进行分析，分析信息系统存在的薄弱点，易于受到攻击的点或范围，并界定信息系统最宽松的安全边界；其次是对系统的动态风险分析，在系统运行过程中进行测试、跟踪并记录其有关活动，以发现系统运行期新出现的风险或原有风险的变化；最后是在系统运行后进行的风险分析，提供相应的系统风险分析报告。

风险分析是信息系统安全需求的依据，安全需求则是制定和实施安全策略的依据。对一个完整体系的信息系统安全来说，由于风险具有时间动态性和空间分布性，因此安全需求也必须是时间动态的和空间分布的。一般来说，由于人们对风险有一个认识过程，因而安全需求总是滞后于风险的发生和发展。但信息系统安全体系的研究者和设计者的最高目标，则是从研究信息系统风险的一般规律入手，认识与掌握信息系统风险状态和分布情况的变化规律，提出安全需求，建立起具有自适应能力的信息安全模型，从而驾驭风险，使信息系统风险被控制在可接受的最小限度内，并渐近于零风险。实际上，零风险永远是一个可期不可达的目标，因此信息系统安全的成功标志是风险的最小化、收敛性和可控性，而不是零风险。

1.3.1 信息系统自身的安全脆弱性

信息系统本身由于系统主体和客体的原因可能存在不同程度的脆弱性，就为各种动机的攻击提供了入侵、骚扰或破坏信息系统可资利用的途径和方法。所谓信息系统的脆弱性，是指信息系统的硬件资源、通信资源、软件及信息资源等，因可预见或不可预见甚至恶意的原因而可能导致系统受到破坏、更改、泄露和功能失效，从而使信息系统处于异常状态，甚至崩溃瘫痪等的根源和起因。具体分析如下。

1．硬件组件

信息系统硬件组件的安全隐患多来源于设计，主要表现为物理安全方面的问题。各种计算机或网络设备（如主机、CRT、电缆、hub、路由器、微波线路等），除难以抗拒的自

然灾害外，温度、湿度、尘埃、静电、电磁场等也可以造成信息的泄露或失效。信息系统在工作时，向外辐射电磁波，易造成敏感信息的泄露。由于这些问题是固有的，除在管理上强化人工弥补措施外，采用软件程序的方法见效不大。因此在设计硬件或选购硬件时，应尽可能减少或消除这类安全隐患。

2．软件组件

软件组件的安全隐患来源于设计和软件工程中的问题。软件设计中的疏忽可能留下安全漏洞；软件设计中不必要的功能冗余及软件过长、过大，不可避免地存在安全脆弱性；软件设计不按信息系统安全等级要求进行模块化设计，导致软件的安全等级不能达到所声称的安全级别；软件工程实现中造成的软件系统内部逻辑混乱，导致垃圾软件，这种软件从安全角度看是绝对不可用的。

软件组件可分为三类，即操作平台软件、应用平台软件和应用业务软件。这三类软件以层次结构构成软件组件体系。操作平台软件处于基础层，维系着系统组件运行的平台，因此操作平台软件的任何风险都可能直接危及或被转移或延伸到应用平台软件。所以，对信息系统安全所需的操作平台软件的安全等级要求不得低于系统安全等级要求，特别是信息系统的安全服务组件的操作系统安全等级必须至少高于系统安全一个等级，强烈建议安全服务组件的操作系统不得直接采用商业级和/或普遍使用的操作系统。应用平台软件处于中间层次，是在操作平台支撑下运行的支持和管理应用业务的软件。一方面，应用平台软件可能受到来自操作平台软件风险的影响；另一方面，应用平台软件的任何风险可直接危及或传递给应用业务软件。因此，应用平台软件的安全特性也至关重要。在提供自身安全保护的同时，应用平台软件还必须为应用软件提供必要的安全服务功能。应用业务软件处于顶层，直接与用户或实体打交道。应用业务软件的任何风险都直接表现为信息系统的风险，因此其安全功能的完整性及自身的安全等级，必须大于系统安全的最小需求。一般来说，外购的商业化应用业务软件比自制应用业务软件更安全些。

3．网络和通信协议

在当今的网络通信协议中，局域网和专用网络的通信协议具有相对封闭性，因为它不能直接与异构网络连接和通信。这样的“封闭”网络本身基于两个原因比开放式的 Internet 的安全特性好，一是网络体系的相对封闭性降低了从外部网络或站点直接攻入系统的可能性，但信息的电磁泄露性和基于协议分析的搭线截获问题仍然存在；二是专用网络自身具有较为完善、成熟的身份鉴别，访问控制和权限分割等安全机制。

安全问题最多的网络和通信协议是基于 TCP/IP 协议栈的 Internet 及其通信协议。因为任何接入 Internet 的计算机网络以及利用公共通信基础设施构建的内联网/外联网，在理论上和技术实践上已无真正的物理界限，同时在地缘上也没有真正的国界。国与国之间、组织