普通高等教育“十一五”国家级规划教材

高·等·院·校·信·息·安·全·专·业·系·列·教·材

教育部高等学校信息安全类专业教学指导委员会与中国计算机学会教育专业委员会共同指导

顾问委员会主任：沈昌祥　编委会主任：肖国镇

Information Security Architecture

信息安全体系结构

冯登国　孙锐　张阳　编著　　蔡吉人　审

http://www.tup.com.cn

清华大学出版社

普通高等教育“十一五”国家级规划教材

高·等·院·校·信·息·安·全·专·业·系·列·教·材

Information Security Architecture

信息安全体系结构

冯登国 孙锐 张阳 编著

蔡吉人 审

清华大学出版社

北京

内 容 简 介

本书对信息安全涉及的各个层面进行了梳理和论证，并讨论了与安全技术和产品相关的内容，充分反映了信息安全领域的最新研究进展和发展趋势。本书主要从信息安全体系结构规划与设计、信息安全技术支撑、信息安全产品、信息安全标准、信息安全管理、人员能力成熟度模型以及信息安全应用案例等方面系统地论述了如何解决信息技术应用所带来的信息安全问题。本书也对信息安全体系结构的概念进行了详细分析和论述，并对构建信息安全体系结构的关键三要素（人、技术和管理）之间的关系进行了详细阐述。本书的特点是系统性强、内容覆盖面广、体系化程度高。

本书可作为计算机、通信、信息安全、密码学等专业的本科生和研究生的教材，也可供从事相关专业的教学、科研和工程技术人员参考。

图书在版编目（CIP）数据

信息安全体系结构/冯登国，孙锐，张阳编著. —北京：清华大学出版社，2008.9
（高等院校信息安全专业系列教材）
ISBN 978-7-302-17072-3

Ⅰ. 信… Ⅱ. ①冯… ②孙… ③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（2008）第 021494 号

责任编辑：张　民　顾　冰
责任校对：李建庄
责任印制：李红英

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
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
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：185×230　**印　张**：15　　**字　数**：304 千字
版　　次：2008 年 9 月第 1 版　　**印　次**：2008 年 9 月第 1 次印刷
印　　数：1～5000
定　　价：23.00 元

高等院校信息安全专业系列教材

编审委员会

出版说明

21世纪是信息时代，信息已成为社会发展的重要战略资源，社会的信息化已成为当今世界发展的潮流和核心，而信息安全在信息社会中将扮演极为重要的角色，它会直接关系到国家安全、企业经营和人们的日常生活。随着信息安全产业的快速发展，全球对信息安全人才的需求量不断增加，但我国目前信息安全人才极度匮乏，远远不能满足金融、商业、公安、军事和政府等部门的需求。要解决供需矛盾，必须加快信息安全人才的培养，以满足社会对信息安全人才的需求。为此，教育部继2001年批准在武汉大学开设信息安全本科专业之后，又批准了多所高等院校设立信息安全本科专业，而且许多高校和科研院所已设立了信息安全方向的具有硕士和博士学位授予权的学科点。

信息安全是计算机、通信、物理、数学等领域的交叉学科，对于这一新兴学科的培养模式和课程设置，各高校普遍缺乏经验，因此中国计算机学会教育专业委员会和清华大学出版社联合主办了“信息安全专业教育教学研讨会”等一系列研讨活动，并成立了“高等院校信息安全专业系列教材”编审委员会，由我国信息安全领域著名专家肖国镇教授担任编委会主任，共同指导“高等院校信息安全专业系列教材”的编写工作。编委会本着研究先行的指导原则，认真研讨国内外高等院校信息安全专业的教学体系和课程设置，进行了大量前瞻性的研究工作，而且这种研究工作将随着我国信息安全专业的发展不断深入。经过编委会全体委员及相关专家的推荐和审定，确定了本丛书首批教材的作者，这些作者绝大多数都是既在本专业领域有深厚的学术造诣、又在教学第一线有丰富的教学经验的学者、专家。

本系列教材是我国第一套专门针对信息安全专业的教材，其特点是：

① 体系完整、结构合理、内容先进。

② 适应面广：能够满足信息安全、计算机、通信工程等相关专业对信息安全领域课程的教材要求。

③ 立体配套：除主教材外，还配有多媒体电子教案、习题与实验指导等。

④ 版本更新及时，紧跟科学技术的新发展。

为了保证出版质量，我们坚持宁缺毋滥的原则，成熟一本，出版一本，并保持不断更新，力求将我国信息安全领域教育、科研的最新成果和成熟经验反映到教材中来。在全力做好本版教材，满足学生用书的基础上，还经由专家的推荐和审定，遴选了一批国外信息安全领域优秀的教材加入到本系列教材中，以进一步满足大家对外版书的需求。热切期望广大教师和科研工作者加入我们的队伍，同时也欢迎广大读者对本系列教材提出宝贵意见，以便我们对本系列教材的组织、编写与出版工作不断改进，为我国信息安全专业的教材建设与人才培养做出更大的贡献。

“高等院校信息安全专业系列教材”已于 2006 年初正式列入普通高等教育“十一五”国家级教材规划（见教高[2006]9 号文件《教育部关于印发普通高等教育“十一五”国家级教材规划选题的通知》）。我们会严把出版环节，保证规划教材的编校和印刷质量，按时完成出版任务。

2007 年 6 月，教育部高等学校信息安全类专业教学指导委员会成立大会暨第一次会议在北京胜利召开。本次会议由教育部高等学校信息安全类专业教学指导委员会主任单位北京工业大学和北京电子科技学院主办，清华大学出版社协办。教育部高等学校信息安全类专业教学指导委员会的成立对我国信息安全专业的发展将起到重要的指导和推动作用。“高等院校信息安全专业系列教材”将在教育部高等学校信息安全类专业教学指导委员会的组织和指导下，进一步体现科学性、系统性和新颖性，及时反映教学改革和课程建设的新成果，并随着我国信息安全学科的发展不断修订和完善。

我们的 E-mail 地址是：zhangm@tup.tsinghua.edu.cn；联系人：张民。

清华大学出版社

本书序

21世纪，人类社会已进入信息时代。信息时代的重要特征是信息的获取、传输、处理等的高速发展。伴随信息化的发展，信息安全作用更加突出，成为全球关注的热点问题。为培养高层次信息安全人才，我国的一些高等院校设置了信息安全专业，并出版了或准备出版一系列信息安全教材。冯登国教授等编著的《信息安全体系结构》是高等院校信息安全专业规划教材之一。这是一本具有系统性、先进性和实用性等鲜明特点的教材。

（1）系统性。信息安全的发展，人们已认识到它不仅是安全技术和产品的问题，而是一个涉及信息安全策略、整体架构、完整流程以及涵盖技术、产品、人员、过程、管理等诸多因素的复杂系统。本书从信息安全整体性出发，系统论述了信息安全的体系结构规划和设计、技术支撑、产品、标准、管理、人员等各个方面以及它们之间的关联，使读者能从更高的层次上去领会信息安全问题。

（2）先进性。信息领域的对抗是一个永恒的命题，信息安全是一个不断发展的过程，它不会永远停留在一个水平上。研究信息安全问题不仅要能满足当前的需求，而且要求在信息安全问题迅速变化中及时适应新的要求。该书在每个部分不仅系统介绍了当前的发展状况，而且分析了它们的发展趋势，这对启发读者的思考是十分重要的。

（3）实用性。理论联系实际是学习的一条重要原则。本书为帮助读者全面了解信息安全的应用状况，较为系统、完整地介绍了国内外信息安全相关的技术标准、管理标准和法律法规，介绍了国外的人员能力成熟度模型，还提供了若干信息安全应用案例，内容丰富，可读性强。

以上这些特点，反映了《信息安全体系结构》是一本很好的信息安全教材，相信它的出版定会引起读者的广泛兴趣。

蔡吉人
中国工程院院士
2008年6月

前言

21世纪以来，随着信息技术的不断革新和广泛应用，人类社会已经步入真正的信息时代。信息技术使我们的工作更为便捷，生活更加舒适，获取信息的途径空前地增多。然而，我们不得不关注我们现在究竟生活在一个什么样的信息社会中？我们每天接触的形式多样、功能或简单或复杂的信息系统与信息网络是否具备令人满意的安全性和可靠性？是否能够及时为我们提供正常的服务？我们对这些网络与信息系统产生如此高度的依赖性，是否会在未来的某个时刻使我们的生活陷入困境？是否会像某些科幻片里讲述的那样，人类费尽心血不断尝试和改进的技术，对人类的发展而言也会带来无法控制的灾难？

不断地有来自世界各地的报道，表明这种依赖的确面临风险。北美大断电，海底电缆故障，航空系统瘫痪，计算机病毒泛滥，数以万计的信用卡账户信息被盗……即使在中国，近些年来类似的事件也层出不穷，危害明显增大。几十年前，信息安全研究与应用主要局限于军队和某些特殊需要。那时，很少有人会预料到，今天会有那么多种类的信息安全产品“飞入”到寻常百姓家。

那么，面对这种变化，面对这些事件，面对这些网络和信息系统，人们在反思：究竟应该如何设计、建设它们？如何对它们自身及其用户进行必要的管理？如何让我们精心研究、设计和开发的技术与产品帮助我们更方便、快捷地工作，更舒心、惬意地生活？

本书试图从体系结构规划与设计、相关技术与产品的设计和应用等方面回答这个问题。此外，鉴于信息安全管理的重要性日益显著，书中也覆盖了与之相关的研究内容，尤其是有关风险评估、等级保护、信息安全管理体系建设等方面的内容。

19世纪英国著名的哲学家、社会学家和教育学家赫·斯宾塞说过：“科学是系统化了的知识”。本书在写作过程中，也一直希望能够对信息安全体系结构所涉及的各方面内容进行梳理，尤其是涉及技术与产品的内容。然

而，鉴于信息安全研究不断深入、技术挑战快速出现，以及相关产业的迅速跟进，我们只能力所能及地挑选现阶段相对成熟、具有代表性的内容进行介绍。书中内容没有涉及一些新技术、新产品，例如，反垃圾邮件技术与产品、反间谍软件技术与产品、IT 审计技术与产品（服务），以及其他许多集成有信息安全功能的技术与产品（例如，带有 SSL 安全通信功能的安全负载均衡设备）。

本书多次作为中国科学院研究生院开设的研究生课程“信息安全体系结构”的授课教材加以使用。选修该课程的研究生们提出了许多宝贵意见，尤其是李立、马强、宋翊麟、张辰、黄非、薄立兴、杨清峰、周芃、张铁赢、卢山、陈波、韩钰、崔兴华、周志勇、初晓博、李昊、魏冰、吴微微、黄亮、王雷、孙彬、敬成、付允等，部分内容借鉴了他们的作业报告，在此表示衷心的感谢，这些教学实践对本书的形成具有十分重要的意义。

爱因斯坦有句名言，“学校的目标始终应当是：青年人在离开学校时，是作为一个和谐的人，而不是作为一个专家”。我们真心希望，这些研究生们，以及认真阅读这本书的所有读者，都能够在成为一个和谐的人的基础上，对信息安全体系结构的知识有一个较为全面的了解，并在今后的学习和工作中学以致用，尽快地成长为信息安全某个具体领域的专家，为我国的信息安全事业作出贡献。

本书在写作过程中得到了清华大学出版社的大力支持和国家重点基础研究发展规划项目（项目编号：2007CB311202）的资助，也得到了业界同行的鼓励和帮助，在此表示衷心的感谢。

作者

2008 年 7 月

目 录

第1章 概　述

1.1 基本概念

1.1.1 体系结构

什么是体系结构？它是由英文单词 architecture 翻译而来。在英语中，architecture 最常用的解释就是“建筑”。可见，与任何一个“建筑”相类似，一个体系结构应该包括一组组件以及组件之间的联系。从系统工程的观点来看，任何复杂的系统都是由相对简单的、具有层次结构的基本元素组成。这些基本元素彼此之间存在着复杂的相互作用，某些元素还可能具有非常复杂的内部结构。

上述的朴素解释能够帮助我们理解体系结构的重点所在，即元素及其关系。在更为严格的学术意义上的解释中，各类体系结构的侧重点不一而同地都落在“元素及其关系”这几个看似简单的字上。例如，ANSI/IEEE STD 1471-2000 使用的体系结构的定义是：“一个系统的基本组织，通过组件、组件之间和组件与环境之间的关系以及管理其设计和演变的原则具体体现。”这里，“组件”即前面所说的“元素”，“组件之间和组件与环境之间的关系”即前面强调的“关系”。

1964 年，G. Amdahl 首次提出了“体系结构”的概念。这一概念的产生促使人们对计算机系统开始有了统一而清晰的认识，并进一步为计算机系统的设计与开发奠定了基础。四十多年过去了，体系结构已经与系统软件、应用软件和程序设计语言有了紧密结合，并且相互作用。伴随着计算机科学、网络与通信技术的飞速发展，围绕体系结构的研究与应用也得以迅速发展，内涵和外延都得到了极大的丰富，涉及网络计算、芯片设计、信息安全产品研发与应用等领域。例如，网络计算体系结构已经成为一种主要的计算模式，芯片级体系结构的研究也是当前一个具有很大挑战性的问题。

目前，对于体系结构的定义，结合前面的最基本定义，不同的机构有着不尽相同的具体定义。例如，信息管理体系结构（TAFIM）提出了一个技术体系结构的定义，即“组件、接口、服务及其相互作用的框架”，从软件工程的角度提出了描述信息系统的四个视图，即“计算视图、数据管理视图、通信视图、安全视图”。开放组织体系结构框架（TOGAF）认

为体系结构包括基础体系结构、标准信息库和体系结构开发方法(ADM),并在此基础上定义了体系结构描述标记语言 ADML。IEEE 的体系结构计划研究组(APG)指出,体系结构可以被认为是“组件＋连接关系＋约束规则”,并建议针对体系结构的描述建立指导性文档。

一般来说,最常见的关于体系结构的分类是将其分为硬件体系结构和软件体系结构两大类。

硬件体系结构的定义由计算机科学中的计算机体系结构发展而来。在计算机科学中,硬件体系结构通常包含了计算机组成原理与设计、计算机系统结构、数字逻辑与数字电路等一系列内容。其中,计算机组成原理与设计是指根据各种计算模型研究计算机的工作原理,并按照器件、设备和工艺条件来设计、制造具体的计算机;计算机系统结构是指对计算机系统的软件、硬件功能进行分配;数字逻辑与数字电路主要涉及数制、码制和逻辑代数,以逻辑代数为工具,对各类组合电路、同步时序电路、异步时序电路的基本逻辑单元进行分析和设计,并对存储器和可编程逻辑器件的性能和特点进行刻画。由于这里提到的各种“元素”,大多是客观可见的组件,例如,逻辑电路元器件。总的来说,硬件体系结构比较容易理解。

随着各种计算机硬件产品(例如,硬件防火墙、硬件 VPN 等)的出现,硬件体系结构不再局限于计算机科学领域,而是成为这些多样化的硬件产品设计、实现、应用和维护过程中不断出现的术语,指的是这些硬件的物理组成部件及其相互关系。当然,这里的“物理组成部件”与计算机体系结构中的“元素”有很多相同之处。

通俗地讲,软件体系结构指的是软件系统在其分析和设计过程中确立的系统中基本元素相互作用的方式。这些基本元素是实现软件系统功能必须的元素。严格地讲,软件体系结构是具有一定形式的结构化元素,即构件的集合,包括处理构件、数据构件和连接构件。处理构件负责对数据进行加工,数据构件是被加工的信息,连接构件把体系结构的不同部分组合连接起来。这一定义注重区分处理构件、数据构件和连接构件,这一方法在其他的定义和方法中基本上得到了保持。

与上述分类方法不同的是,信息系统体系结构则不再区分为硬件和软件,而是从信息系统设计与开发的角度,考虑其组成元素及其彼此间的关联和相互作用。

另外一个经常出现的相关概念是企业体系结构(EA)。这是帮助一个企业理解自己的组成结构及其原理的概念性工具。企业体系结构提供了企业的结构图,是企业业务和技术变化的规划工具。一般来说,企业体系结构表现为一整套相互关联的模型,这些模型描述了企业的结构和功能。企业体系结构主要用于系统化的信息技术规划和架构,以及对它们进行改进的决策过程。EA 中的各个模型以逻辑方式排列,可以使企业的详细信息处于不断增长的过程中。这些信息包括目的和目标、过程和组织、系统和数据以及使用的技术。