信息安全保障人员认证培训教材

信息安全技术应用

XIN XI AN QUAN JI SHU YING YONG

中国信息安全认证中心

◎主　编　张　剑　◎副主编　万里冰　秦潇潇

★★★ CISAW ★★★

电子科技大学出版社

信息安全保障人员认证培训教材

信息安全技术应用

XIN XI AN QUAN JI SHU YING YONG

中国信息安全认证中心

◎ 主　编　张　剑　◎ 副主编　万里冰　秦潇潇

★★★ CISAW ★★★

电子科技大学出版社

图书在版编目（CIP）数据

信息安全技术应用 / 张剑主编. -- 成都：电子科技大学出版社, 2015.4
ISBN 978-7-5647-2979-0

Ⅰ. ①信… Ⅱ. ①张… Ⅲ. ①信息安全-技术应用-研究-中国 Ⅳ. ①TP309

中国版本图书馆 CIP 数据核字 (2015) 第　　号

内 容 提 要

本书共分九章，首先介绍了CISAW信息安全保障模型，并依据CISAW模型中实体对象的划分，从实体对象安全技术、应用安全技术和信息安全技术领域应用三个层面进行组织。在实体对象安全部分，本书从为核心业务服务的数据、载体、环境和边界4个方面详细阐述了安全技术概念和基本原理。并在此基础上，重点描述典型安全技术的实际应用，以加强读者对信息安全技术的认知、提高信息安全技术应用的能力；在应用安全技术方面，本书主要分析了目前主流的物联网和云计算应用技术所面临的安全问题和针对安全问题所采取的具体措施；在领域应用方面，本书结合具体应用领域介绍了电子商务安全和医疗卫生信息安全，分析了典型安全问题，讨论了安全措施，并通过具体案例探讨了信息安全技术在领域内的应用。

信息安全技术应用

主　编　张　剑
副主编　万里冰　秦潇潇

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦　邮编：610051）
策划编辑：徐守铭
责任编辑：郭蜀燕　徐守铭
责任校对：刘　愚
主　　页：www.uestcp.com.cn
电子邮箱：uestcp@uestcp.com.cn
发　　行：新华书店经销
印　　刷：成都市川侨印务有限公司
成品尺寸：185 mm × 260 mm　　**印张** 18　　**字数** 387 千字
版　　次：2015 年 4 月第一版
印　　次：2015 年 4 月第一次印刷
书　　号：ISBN 978-7-5647-2979-0
定　　价：45.00 元

丛书编委会

编　写　组

主　编　张　剑

副主编　万里冰　秦潇潇

编　委　钱伟中　傅　翀　王　静　赵　辉　王湖南

序

2014年，我国提出了建设网络强国战略与目标。实现网络强国，培养和造就网络与信息安全人才队伍是关键。据调查，截至2014年年底，国内网络与信息安全人才缺口高达50万人，并呈现持续增长的趋势。加快人才培养是我国经济社会发展和信息安全体系建设中的一项长期性、全局性和战略性的任务。

作为我国专业信息安全认证机构和培训机构，中国信息安全认证中心以保障国家网络与信息安全为己任，于2011年推出了信息安全保障人员认证（CISAW）。CISAW认证是面向IT从业人员、在校学生，特别是与网络与信息安全密切相关的高级管理人员、专业技术人员推出的人员资格认证和专业水平认证。CISAW认证的推出和实施，为培养和造就我国网络与信息安全人才探索了一条有效途径，得到了业内专家和社会各界的好评。

推行CISAW认证，编写高质量的教材尤为重要。鉴于此，中国信息安全认证中心组织国内信息安全保障的专业技术和应用领域的专家，依据《信息安全保障人员认证考试大纲》要求，结合信息安全保障工作的各岗位知识和应用能力要求，共同编著了信息安全保障人员认证系列教材。本系列教材包括《信息安全技术》《信息安全技术应用》和《信息安全实验》3种基础教材；《软件安全开发》《信息系统安全集成》《信息安全管理》《信息安全咨询手册》《信息系统安全运维》《信息系统安全审计》《信息安全风险管理》《网络攻防技术》《业务连续性管理》《云计算安全》《物联网安全》和《工业控制安全》12种专业技术应用教材；《电子政务安全》《电子商务安全》《交通服务信息安全》《能源服务信息安全》《医疗卫生信息安

全》《教育服务信息安全》《金融服务信息安全》《通信服务信息安全》《宾馆服务信息安全》和《物流服务信息安全》10 种应用领域教材。

本系列教材以实用为首要原则，从统一的信息安全保障模型出发，构建了包括信息安全技术基础知识、信息安全专业技术知识和应用领域安全保障管理知识的完整信息安全保障知识体系。既是广大 CISAW 认证申请者的考试指导用书，同时也是广大信息安全保障工作者的工作指南和参考用书。

希望本系列教材的出版，能为广大信息安全保障从业者学习、工作和申请认证提供指导和帮助。

是为序。

中国信息安全认证中心主任　魏　昊

2014 年 12 月 28 日

前　言

本书从CISAW信息安全保障模型出发，由基本实体对象相关的安全技术、应用安全技术和信息安全技术领域应用三个层面内容组成，共9章。第1章概述介绍了信息安全相关的基本概念，并详细解析了张剑博士提出的CISAW信息安全保障模型；第2章至第5章围绕模型中“业务”这个核心内容安全属性的实现，阐述了数据、载体、环境和边界4个实体对象相关安全技术的基本原理、应用原理和应用实例；第6章和第7章介绍了目前主流的物联网安全和云计算安全的相关安全技术和应用技术；第8章和第9章结合具体应用领域介绍了电子商务安全和医疗卫生信息安全。

本书按照信息安全保障人员认证考试大纲的要求进行编写，在适合广大申请认证考试的人员使用的同时，也适合所有从事与信息技术相关的工作人员和期望了解信息安全技术相关知识的人员使用。《信息安全技术》是与本书相关的专业级（II级）基础教程，也是本书的重要参考资料，感兴趣的读者可通过其获得更为全面和深入的基础知识。

本书由张剑、万里冰、秦潇潇、钱伟中、傅翀、王静、赵辉、王湖南等共同编写完成。

本书在成书过程中得到了《信息安全保障人员认证考试用书》编委会的指导，得到了中国信息安全认证中心、四川省中认信安技术服务有限公司、四川亚和企业咨询服务有限公司的大力支持，在此表示衷心感谢。

本书在编写过程中，参考或引用了国内外同行的文献资料，在此向这些文献资料的作者表示衷心感谢。

本书力图通过较小的篇幅比较完整地、正确地介绍信息安全相关的基本技术应用的同时，为了能够扩大读者面，尽量使用简单、实用和易于理解的方式进行阐述。但由于水平有限、时间紧迫，尽管我们进行了多次研讨和修订，书中仍难免存在疏漏和错误。在此，恳请广大读者和同行批评指正，以便我们再版修订时加以改正和完善。

张　剑

2014 年 12 月 31 日

目　录

第 1 章 概 述

近年来，信息技术的普及应用给人民生活带来了新的模式和诸多便利。信息技术支撑着政府和社会各行各业的主要业务，这给信息安全保障提出了严峻的挑战，使得信息安全保障成为关乎国家安全、国家信息化建设的重要课题。

本书以信息安全技术应用为题，以 CISAW 信息安全保障模型为核心和主线来组织各个章节，在介绍信息安全及相关技术同时，重点突出技术应用相关内容。

本章在介绍信息安全基本概念的基础上，主要介绍本书的核心模型——CISAW 信息安全保障模型。

1.1 基本概念

为更好地理解本书的核心模型，本章首先介绍相关的基本概念，并回顾信息安全的发展历程。

1.1.1 信息定义

早在 1948 年，C. E. Shannon 博士在“通信的数学理论”一文中，从数学的角度对信息进行了相关描述，他对信息的定义可以理解为：“信息是消除不确定性的东西”。

我们认为信息是一种通过信息系统进行加工和处理的对象。信息通过一定数据形式展现，进而通过一定的载体进行存储和传输。信息作为一种对象，和自然界中的事物一样，有产生、发展和消亡的过程，我们称之为生命周期。信息的生命周期包括了信息的产生、存储、传输、处理和销毁等诸多环节。信息系统正是信息在生命周期中的生存环境，即：信息是信息系统的处理对象，信息系统是信息赖以生存的环境。

就信息系统而言，我国国家标准 GB/Z20986—2007《信息安全事件分类分级指南》中认为，信息系统是“由计算机及其相关的和配套的设备、设施（含网络）构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统”。

我们认为信息系统是为信息生命周期提供服务的各类软硬件资源的总称。

1.1.2 安全定义

通俗地讲，所谓安全就是“不出事或感觉不到要出事的威胁”。可见，安全关系到两件事：一件是已经发生的事，即安全事件；另一件是未发生但可能引发安全事件的事，即安全风险。例如：操作系统遭受漏洞型病毒攻击事件属于已经发生的安全事件，而操作系统没有更新补丁而存在被攻击的系统漏洞则是属于系统的脆弱性，是可能导致安全事件的安全风险。

根据上述观点，要解决安全问题必须从这两个方面入手，做好安全事件的处理和应对，同时做好安全威胁的防范和脆弱性的避免，降低安全风险以减少损失。

1.1.3 信息安全定义

信息安全是本书的基本词汇。GB/T22080—2008/ISO/IEC27001：2005《信息安全管理体系要求》中将其定义为：“保持信息的机密性、完整性、可用性；另外也可包括诸如真实性、可核查性、不可否认性和可靠性等”。

我们认为信息安全是信息系统抵御意外事件或恶意行为的能力，这些事件和行为将破坏由信息系统所提供的可用性、完整性、真实性、机密性、不可否认性等安全特性。对这些安全特性的理解和定义将在下面的几个小节中进行详细介绍和说明。

1.1.4 可用性

可用性，在国家标准 GB/T9387.2—1995 和公安部标准 GA/T 391—2002 中，被定义为“根据授权实体的请求可被访问与使用”。

在 ISO/IEC27001：2005 标准中，可用性（Availability）的定义为：“根据授权实体的要求可访问和利用的特性”。

普遍接受的系统安全准则（Generally Accepted System Security Principles，GASSP）认为：“可用性是数据的一个特征，指的用户可以在合适的时间以要求的方式访问和使用信息与信息系统”。

国家电信联盟（International Telecommunication Union，ITU）CNI/03 文档中指出，可用性指“使网络在极端环境下运行，也能够在任何时间访问网络上的数据”。

《美国法典》第 44 篇第 3542 节中指出，可用性指“确保及时和可靠地访问和使用信息”。

美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）特别出版物 SP 800－37 的 2002 V1 版本中，可用性的定义为“确保授权用户和/或系统过程可以及时可靠地访问信息、服务和 IT 资源，并能防止拒绝服务（Deny of Service，DoS）”。

可用性要求包括信息、信息系统和系统服务都可以被授权实体在适合的时间、要