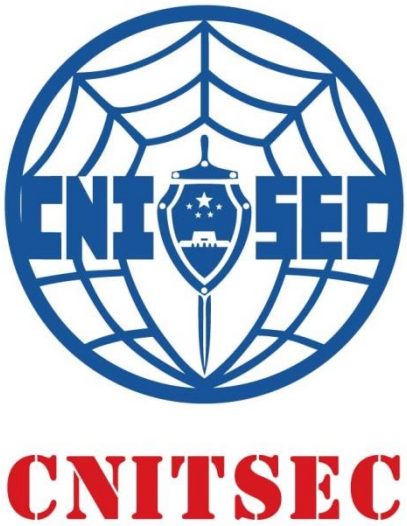
注册信息安全开发人员（CISD）

知识体系大纲



V2.0 版

目录

前言

信息安全作为我国信息化建设健康发展的重要因素，关系到贯彻落实科学发展观、全面建设小康社会、构建社会主义和谐社会和建设创新型社会等国家战略举措的实施，是国家安全的重要组成部分。在信息系统安全保障工作中，人是最核心、也是最活跃的因素，人员的信息安全意识、知识与技能已经成为保障信息系统安全稳定运行的重要基本要素之一。

注册信息安全开发人员（CISD）是对我国网络基础设施和重要信息系统的软件开发人员安全开发能力实施的一种资质评定。本大纲从我国国情出发，结合我国网络基础设施和重要信息系统安全保障的实际需求和特点，以知识体系的全面性和实用性为原则，明确规定了注册信息安全开发人员应当掌握的知识要点，是 CISD 教材编制，讲师授课，学员学习，以及考试命题的重要依据。

本大纲包含以下章节：

- 第 1 部分：注册信息安全开发人员（CISD）知识体系概述
- 第 2 部分：信息安全保障
  - ◆知识体：信息安全保障基本知识
  - ◆知识体：信息安全法规与政策
  - ◆知识体：访问控制技术
  - ◆知识体：密码学原理
  - ◆知识体：网络安全
  - ◆知识体：系统安全
  - ◆知识体：信息安全风险管理
  - ◆知识体：信息安全工程原理
- 第 3 部分：软件安全开发
  - ◆知识体：软件安全开发概论
  - ◆知识体：软件安全需求分析
  - ◆知识体：软件安全设计
  - ◆知识体：软件安全编码
  - ◆知识体：软件安全测试
  - ◆知识体：软件安全部署与安全开发项目管理

第 1 章 注册信息安全开发人员（CISD）知识体系概述

“注册信息安全开发人员”，英文为 Certified Information Security Developer ，简称 **CISD**，系经中国信息安全测评中心认定的信息安全开发人员，具备一定的软件安全开发知识和技术，能为软件全生命周期中提供安全保障。

CISD 知识体系使用组件模块化的结构，包括知识类、知识体、知识域和知识子域四个层次。

- **知识类：**是对信息安全保障知识领域的总体划分，包含信息安全专业人员需要掌握的知识类别；
- **知识体：**是知识类中由属于同一技术领域的知识内容构成的相对独立、成体系的知识集合；
- **知识域：**是对知识体进一步分解细化形成的完整的知识组件；
- **知识子域：**是构成知识域的基本模块，由一至多个具体知识要点构成。

本大纲规定了知识子域中每一个知识要点的内容和深度要求，分为“了解”、“理解”、和“掌握”三类。

- **了解：**是最低深度要求，学员只需要正确认识该知识要点的基本概念和原理；
- **理解：**是中等深度要求，学员需要在正确认识该知识要点的基本概念和原理的基础上，深入理解其内容，并可以进行进一步的判断和推理；
- **掌握：**是最高深度要求，学员需要正确认识该知识要点的概念、原理，并在深入理解的基础上灵活运用。

图 11 描述了 CISD 知识体系的结构：

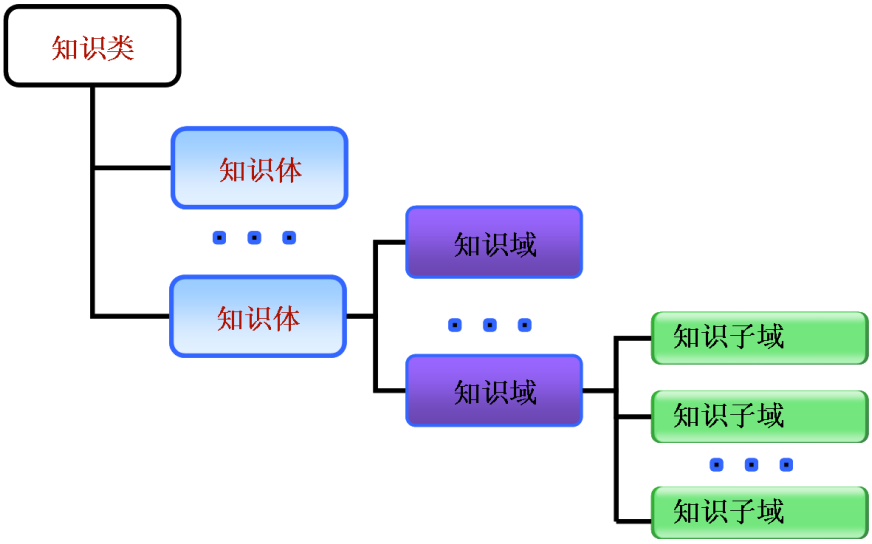


图 11：CISD 知识体系的组件模块结构

在整个注册信息安全开发人员（CISD）的知识体系结构中，共包括信息安全保障和软件安全开发两大知识类，其中软件安全开发知识类具体包括软件安全开发概述、软件安全需求分析、软件安全设计、软件安全编码、软件安全测试、软件安全部署与安全开发项目管理六个知识体，每个知识体包含多个知识域，每个知识域由一个或多个知识子域组成。

CISD 知识体系结构中，软件安全开发知识类的六个知识体分别为：

- **软件安全开发概述：**介绍软件安全保障的目标和基本要素，以及软件开发生命周期安全的基本思想，它是注册信息安全开发人员首先需要掌握的基础知识。
- **软件安全需求分析**:在软件需求分析阶段融入安全分析，阐述了常用的安全需求分析方法及其在实际开发过程中的应用。
- **软件安全设计：**介绍软件设计过程中应遵循的最小特权、职责分离、纵深防御、默认安全、减少攻击面、心理可接受等基本安全原则及其在实际开发过程中的应用，并阐述软件架构安全性分析方法和基于模式的软件安全设计方法的基本思想。
- **软件安全编码：**介绍通用安全编程准则，以及信息泄露、加密漏洞、溢出攻击、代码注入、跨站脚本等常见安全缺陷的形成原因与危害，以其防御措施。
- **软件安全测试：**介绍基于风险的安全测试思想，白盒安全测试的原理、特点及常用工具，模糊测试和渗透测试等黑盒安全测试的原理及方法。
- **软件安全部署与安全开发项目管理：**介绍软件安全加固、安装和配置评估，以及软件安全开发项目管理生命周期中的主要活动。

图 1-2 描述了 CISD 知识体系结构框架：

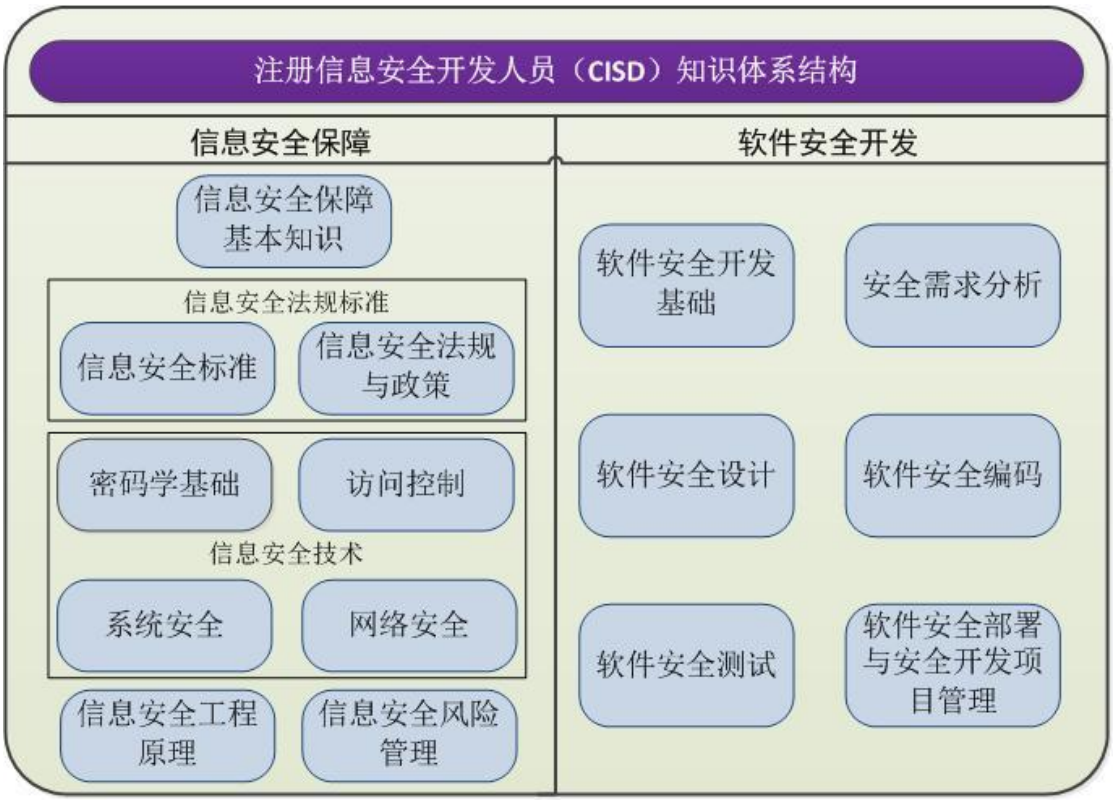


图 1-2 CISD 知识体系结构框图

CISD 考试题型均为单项选择题，共 100 题，每题 1 分，得到 70 分以上（含 70 分）为通过。

表 1-1：CISD 试题结构

知识类别	试题比重
信息安全保障	5%
信息安全政策与法规标准	5%
信息安全工程	5%
信息安全风险管理	10%
信息安全技术	25%
软件安全开发基础	5%
安全需求分析	10%
软件安全设计	10%

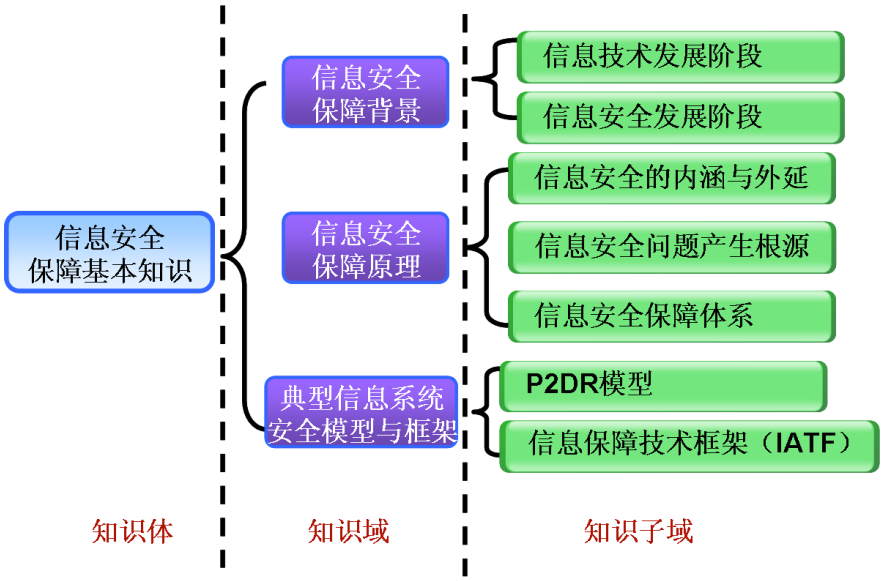
知识类别	试题比重
软件安全编码	10%
软件安全测试	10%
软件安全部署与安全开发项目管理	5%

第 2 章 知识类：信息安全保障

信息安全保障体系概述介绍了信息安全保障中的框架原理、政策法规、风险管理等管理内容，访问控制、密码学、系统安全、网络安全等技术内容，以及信息安全工程的原理，它是注册信息安全专业人员首先需要掌握的基础知识。通过本部分的学习，学员应当：

- 理解信息安全保障的意义和内涵；
- 了解信息安全相关政策法规；
- 理解风险管理的思想和方法；
- 掌握访问控制和密码学的基本知识；
- 掌握系统和网络安全的基本知识；
- 理解信息安全工程原理。

2.1 知识体：信息安全保障基本知识



图表 21：知识体：信息安全保障基本知识

2.1.1 知识域：信息安全保障背景

- 知识子域：信息技术发展阶段
  - 了解电报/电话、计算机、网络等阶段信息技术发展概况
  - 了解信息化和网络对个人、企事业单位和社会团体、经济发展、社会稳定、国家安全等方面的影响
- 知识子域：信息安全发展阶段
  - 了解通信保密、计算机安全和信息安全保障

- ◆ 了解各个阶段信息安全面临的主要威胁和防护措施

2.1.2 知识域：信息安全保障原理

- 知识子域：信息安全的内涵和外延
  - ◆ 理解信息安全的特征与范畴
  - ◆ 理解信息安全的地位和作用
  - ◆ 理解信息安全、信息系统和系统业务使命之间的关系
  - ◆ 理解信息安全的内因：信息系统的复杂性
  - ◆ 理解信息安全的外因：人为和环境的威胁
- 知识子域：信息安全保障体系
  - ◆ 理解安全保障需要贯穿系统生命周期
  - ◆ 理解保密性、可用性和完整性三个信息安全特征
  - ◆ 理解策略和风险是安全保障的核心问题
  - ◆ 理解技术、管理、工程过程和人员是基本保障要素
  - ◆ 理解业务使命实现是信息安全保障的根本目的

2.1.3 知识域：典型信息系统安全模型与框架

- 知识子域：P2DR 模型
  - ◆ 理解 P2DR 模型的基本原理：策略、防护、检测、响应
  - ◆ 理解 P2DR 数学公式所表达的安全目标
- 知识子域：信息保障技术框架
  - ◆ 理解 IATF 深度防御思想
  - ◆ 理解 IATF 对信息技术系统四个方面的安全需求划分及基本实现方法：本地计算环境、区域边界、网络及基础设施、支撑性基础设施

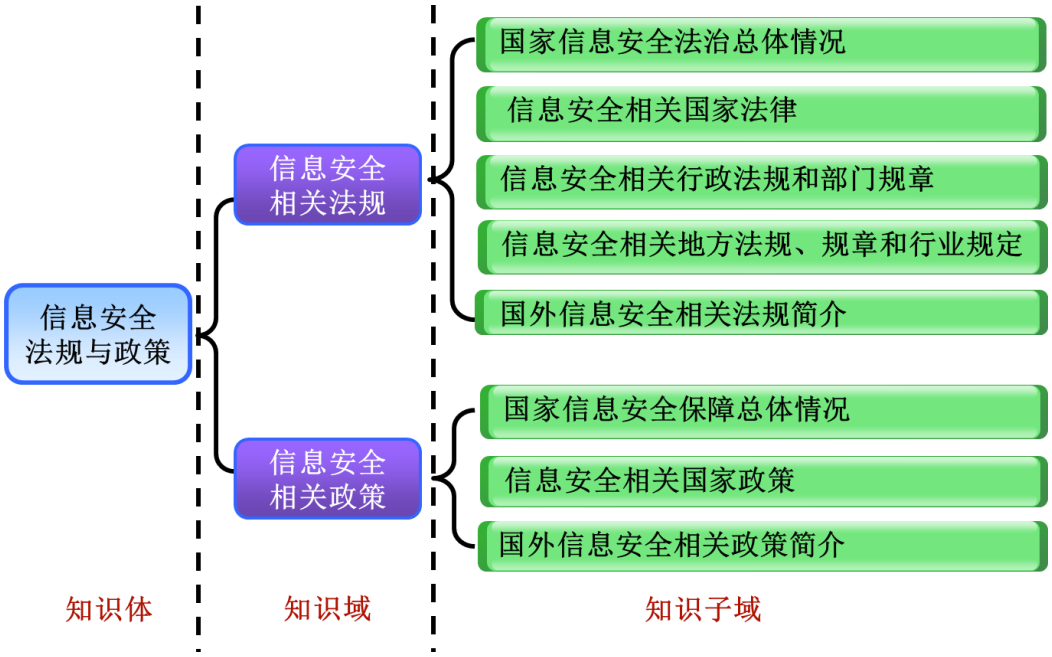
2.1.4 知识域：信息安全保障工作概况

- 知识子域：国外信息安全保障情况
  - ◆ 了解发达国家信息安全状况和信息安全保障的主要举措
  - ◆ 了解发达国家信息安全方面主要动态
- 知识子域：我国信息安全保障工作总体情况
  - ◆ 了解我国信息安全保障工作发展阶段
  - ◆ 理解国家信息安全保障基本原则
  - ◆ 了解国家信息安全保障建设主要内容

2.1.5 知识域：信息安全保障工作基本内容

- 知识子域：确定安全需求
  - 理解确定信息系统安全保障需求的作用
  - 理解确定信息系统安全保障需求的方法和原则
- 知识子域：设计和实施信息安全方案
  - 理解信息安全方案的作用和主要内容
  - 理解制定信息安全方案的主要原则
  - 理解信息安全方案实施的主要原则
- 知识子域：信息安全测评
  - 了解信息安全测评的重要性
  - 了解国内外信息安全测评概况
  - 理解信息安全产品测评方法和流程
  - 理解信息系统安全测评方法和流程
  - 了解服务商资质测评方法和流程
  - 了解信息安全人员资质测评方法和流程
- 知识子域：信息安全监控与维护
  - 理解在系统生命周期中持续提高信息系统安全保障能力的意义
  - 理解信息系统安全监控与维护的主要原则

2.2 知识体：信息安全法规与政策



图表 22：知识体：信息安全法规与政策

2.2.1 知识域：信息安全相关法律

- 知识子域： 国家信息安全法治总体情况
  - 了解信息安全法治建设的意义
  - 了解我国信息安全法律法规体系框架
- 知识子域： 信息安全相关国家法律
  - 了解《中华人民共和国宪法》有关信息安全的内容
  - 了解《中华人民共和国刑法》有关信息安全犯罪的规定
  - 了解《中华人民共和国治安管理处罚法》有关信息安全的内容
  - 掌握《中华人民共和国保守国家秘密法》的主要内容
  - 掌握《全国人民代表大会常务委员会关于维护互联网安全的决定》的内容
  - 理解《中华人民共和国电子签名法》的意义和作用
  - 了解《中华人民共和国侵权责任法》有关信息安全的内容
- 知识子域： 信息安全相关行政法规和部门规章
  - 了解信息安全相关行政法规，掌握涉及信息安全的相关内容
  - 了解信息安全相关部门规章，掌握涉及信息安全的相关内容

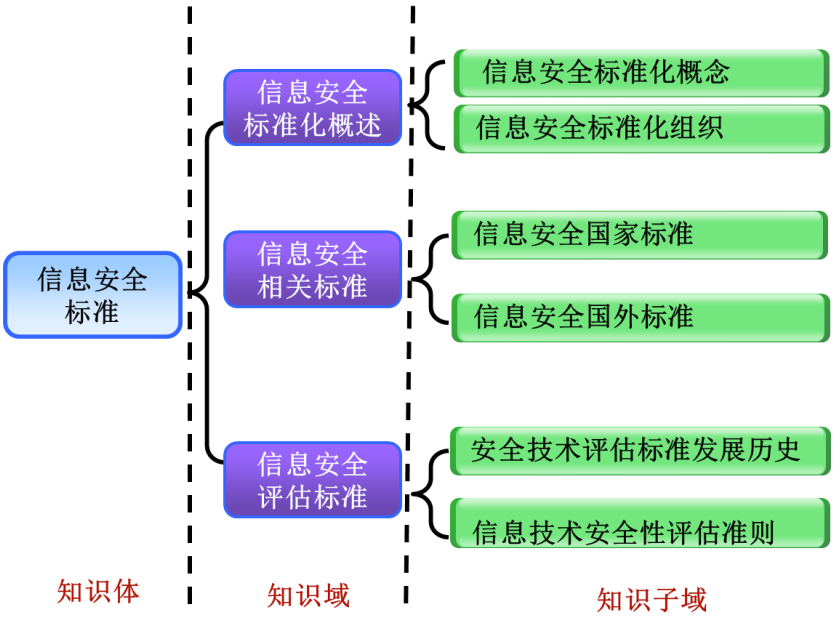
- 知识子域： 信息安全相关地方法规、规章和行业规定
  - ◆ 了解信息安全相关地方法规，掌握自身所在地方或密切相关地方涉及信息安全的相关内容
  - ◆ 了解信息安全相关地方规章，掌握自身所在地方或密切相关地方涉及信息安全的相关内容
  - ◆ 了解信息安全相关行业规定，掌握自身所在行业或密切相关行业涉及信息安全的相关内容
- 知识子域： 国外信息安全相关法规简介
  - ◆ 了解美国信息安全相关法规概况

2.2.2 知识域：信息安全相关政策

- 知识子域：国家信息安全保障总体情况
  - ◆ 掌握国家有关政策对信息安全保障工作的总体方针和要求
  - ◆ 掌握国家有关政策规定的加强信息安全保障工作主要原则
  - ◆ 掌握国家有关政策规定需要重点加强的信息安全保障工作
- 知识子域：信息安全相关国家政策
  - ◆ 了解信息安全相关国家政策，掌握风险评估等涉及信息安全的相关内容
  - ◆ 掌握信息安全等级保护政策体系，熟悉信息安全等级保护相关政策
- 知识子域：国外信息安全相关政策简介

  了解美国信息安全相关政策概况

2.3 知识体：信息安全标准



图表 23：知识体：信息安全标准

2.3.1 知识域：安全标准化概述

- 知识子域：信息安全标准化概念
  - 了解标准和标准化的基本概念和作用
- 知识子域：信息安全标准化组织
  - 了解国际信息安全标准化组织及其工作
  - 了解国外典型国家信息安全标准化组织及其工作
  - 熟悉我国信息安全标准化组织及其工作

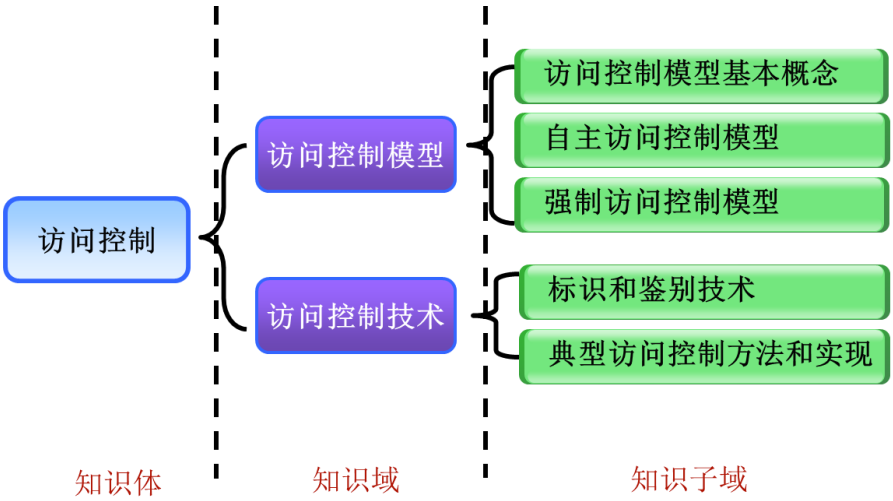
2.3.2 知识域：信息安全相关标准

- 知识子域：信息安全国家标准
  - 了解我国信息安全标准体系框架
  - 掌握信息安全等级保护标准体系，熟悉信息安全等级保护相关标准
- 知识子域：信息安全国外标准
  - 了解国际信息安全标准体系
  - 了解国外典型国家信息安全标准体系
  - 了解与自身工作密切相关的信息安全国际标准

2.3.3 知识域：信息安全评估标准

- 知识子域：安全技术评估标准发展历史
  - 了解安全技术评估标准发展过程
  - 理解 GB/T18336《信息技术安全性评估准则》（CC）的特点
- 知识子域：信息技术安全性评估准则
  - 了解 CC 的结构
  - 理解 CC 的术语（TOE、PP、ST、EAL）和基本思想
  - 了解使用 CC 进行信息技术产品安全性评估的基本过程
  - 了解通用评估方法（CEM）

2.4 知识体：访问控制



图表 24：知识体：访问控制与审计监控

2.4.1 知识域：访问控制模型

- 知识子域：访问控制基本概念
  - 理解标识、鉴别和授权等访问控制的基本概念
  - 理解各种安全模型的分类
- 知识子域：自主访问控制模型
  - 理解自主访问控制的含义
  - 理解访问控制矩阵模型，及其实现方法：访问控制列表、权能列表
  - 理解自主访问控制模型的特点
- 知识子域：强制访问控制模型
  - 理解强制访问控制的分类和含义
  - 掌握典型强制访问控制模型：Bell-Lapudula 模型、Biba 模型、Clark-Wilson 模型和 Chinese Wall 模型
  - 理解强制访问控制模型的特点

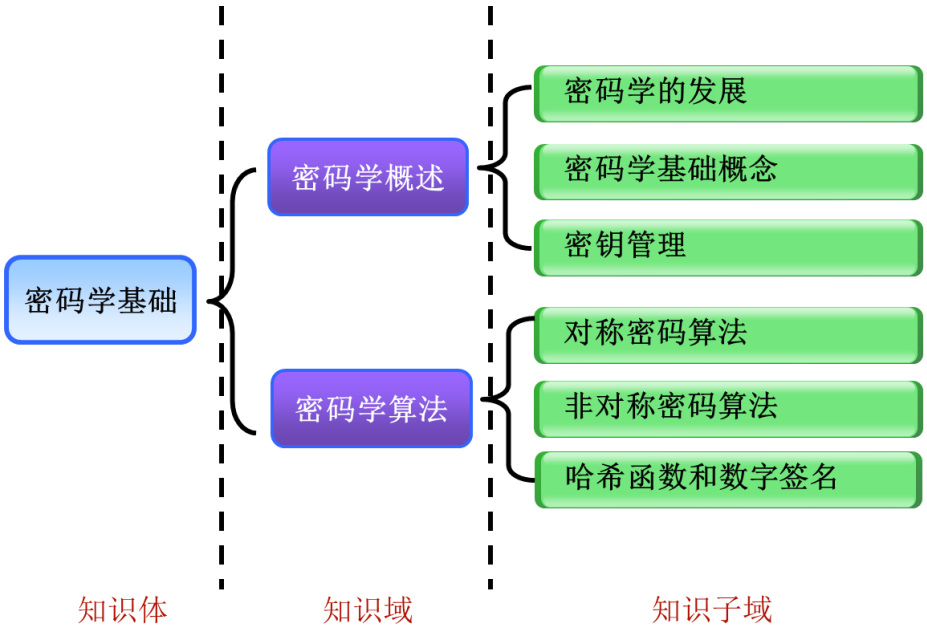
2.4.2 知识域：访问控制技术

- 知识子域：标识和鉴别技术
  - 理解账号和口令管理的基本原则
  - 了解生物识别技术及其实现（虹膜、指纹、掌纹等）

- ◆ 了解其他鉴别技术（令牌、票据等）
- ◆ 了解单点登录技术（SSO）及其实现（Kerberos 等）

- 知识子域：典型访问控制方法和实现
  - ◆ 理解集中访问控制的基本概念及其实现（RADIUS、TACACS、TACACS+和 Diameter 等）
  - ◆ 理解非集中访问控制的基本概念及其实现（域等）

2.5 知识体：密码学基础



图表 25：知识体：密码技术

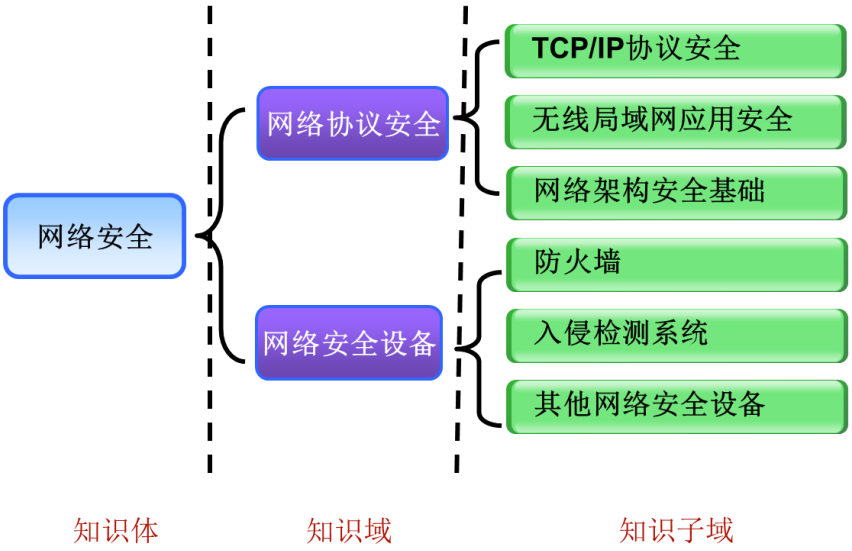
2.5.1 知识域：密码学概述

- 知识子域：密码学的发展
  - 了解密码学的发展阶段
  - 了解各阶段特点
- 知识子域：密码学基础概念
  - 理解密码编码学和密码分析学的概念
  - 了解科克霍夫原则和影响密码系统的安全性的基本因素：复杂程度、密钥机密性、密钥长度、初始化向量
  - 了解密码的基本类型：换位（置换）密码、替代（代换）密码、流密码、分组密码的概念
  - 掌握密码体制的分类
- 知识子域：密钥管理
  - 了解密钥管理的概念，包括密钥管理体制、密钥交换协议和密钥的产生、分配、更换和注销等

2.5.2 知识域：密码学算法简介

- 知识子域：对称密码算法
  - 理解对称加密算法的优缺点
  - 了解 DES、AES、IDEA 三种典型对称加密算法的工作原理
- 知识子域：对称密码算法
  - 理解对称加密算法的优缺点
  - 了解 DES、AES、IDEA 三种典型对称加密算法的工作原理
- 知识子域：非对称密码算法
  - 理解非对称密码算法的功能和优缺点
  - 理解掌握 RSA 公钥密码体制：RSA 的算法描述、RSA 的实现、RSA 的安全性、RSA 在应用中的问题
  - 了解其他非对称密码算法的特点：Diffie – Hellman、ELGamal、DSA、ECC 等
- 知识子域：哈希函数
  - 理解哈希（Hash）函数的作用
  - 了解 MD5 算法、SHA-1 算法的工作原理
  - 理解消息鉴别码、数字签名的原理和应用

2.6 知识体：网络安全



图表 26：知识体：网络安全

2.6.1 知识域：网络协议安全

- 知识子域：TCP/IP 协议安全
  - 理解开放互联系统模型 ISO/OSI 七层协议模型及其安全体系结构
  - 理解 TCP/IP 四层协议模型及协议安全架构
- 知识子域：无线局域网应用安全
  - 了解无线网络协议原理及其安全特性
- 知识子域：网络架构安全基础
  - 理解网络安全域划分应考虑的主要因素
  - 理解 IP 地址分配的方法
  - 理解 VLAN 划分的作用与策略
  - 理解路由交换设备安全配置常见的要求
  - 理解网络边界访问控制策略的类型
  - 理解网络冗余配置应考虑的因素

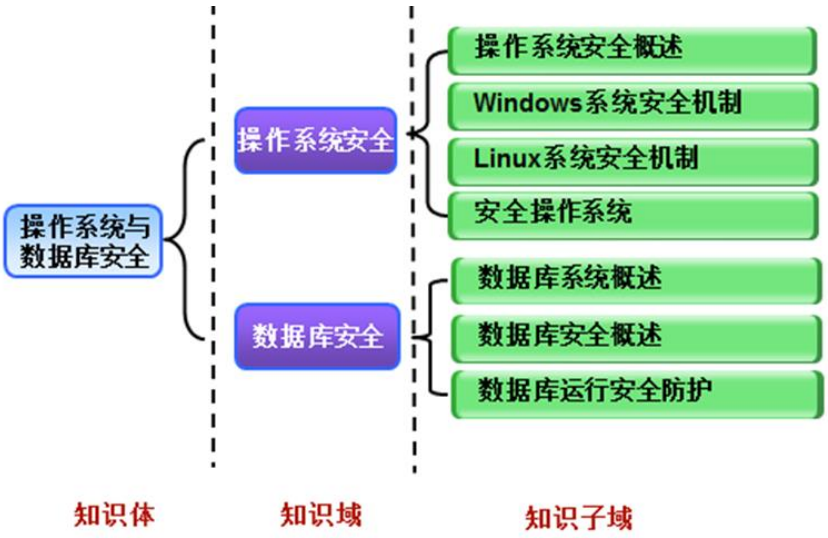
2.6.2 知识域：网络安全设备

- 知识子域：防火墙技术
  - 理解防火墙的作用、功能及分类
  - 理解包过滤技术、状态检测技术和应用代理技术等防火墙主要技术原理

- 了解防火墙的部署结构
- 了解防火墙的局限性

- 知识子域：入侵检测系统
  - 理解入侵检测系统的作用、功能及分类
  - 理解入侵检测系统的主要技术原理
  - 掌握入侵检测系统的部署结构
  - 理解入侵检测系统的局限性
- 知识子域：其它网络安全设备
  - 了解安全隔离与信息交换系统的原理、特点及适用场景
  - 了解入侵防御系统（IPS）原理与特点
  - 了解安全管理平台（SOC）的主要功能
  - 了解统一威胁管理系统（UTM）的功能与特点
  - 了解网络准入控制（NAC）的功能、组成及控制方式

2.7 知识体：系统安全



图表 27：知识体：系统安全

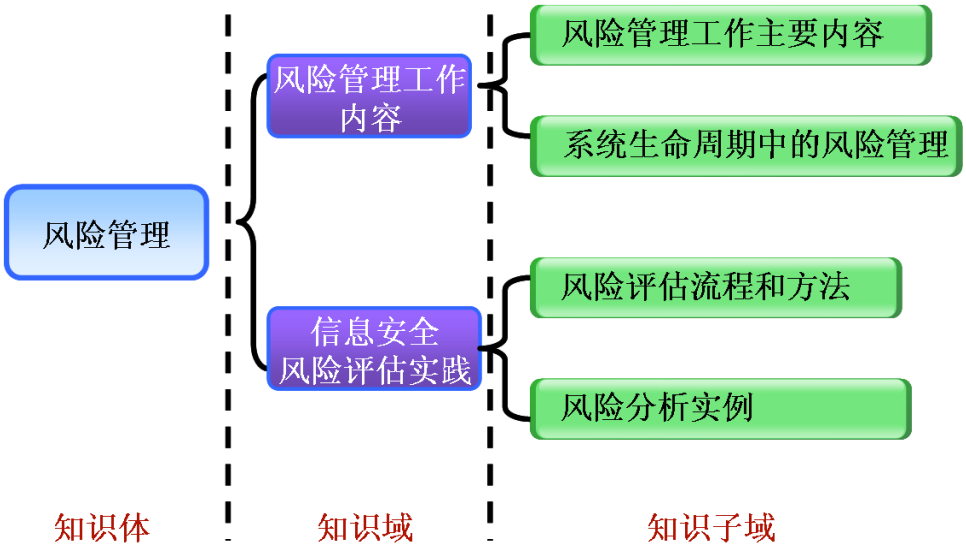
2.7.1 知识域：操作系统安全

- 知识子域：操作系统安全概述
  - 了解操作系统的作用与功能
  - 了解操作系统的主要安全设计机制
  - 理解操作系统的安全配置要点
- 知识子域：Windows 系统安全机制
  - 理解 Windows 系统标识与鉴别、访问控制、用户账户控制、安全审计、文件系统的安全机制和安全策略
  - 掌握 Windows 系统的安全配置方法
- 知识子域： Linux 系统安全机制
  - 理解 Linux 系统标识与鉴别、访问控制、安全审计、文件系统、特权管理的安全机制
  - 掌握 Linux 系统的安全配置方法
- 知识子域：安全操作系统
  - 了解安全操作系统的发展
  - 了解安全操作系统的设计原则

2.7.2 知识域：数据库安全

- 知识子域：数据库系统概述
  - 了解数据库基本概念和主要功能
  - 了解构化查询语言 SQL 的功能
  - 了解数据库管理系统（DBMS）的一般架构
- 知识子域：数据库安全概述
  - 了解数据库的安全需求
  - 了解数据库的常见安全措施：用户标识和鉴别、访问控制、数据加密和安全审计
  - 理解数据库完整性要求，理解 DBMS 为了实现完整性保护必须提供：定义完整性约束条件的机制、完整性检查的方法和违约处理的机制
  - 理解数据库备份和恢复机制的重要性，了解常见的数据冗余技术和数据库恢复策略
- 知识子域：数据库运行安全防护
  - 理解数据库威胁与防护特点
  - 理解数据库事前安全防护、事中安全监控以及事后安全审计的方法

2.8 知识体：信息安全风险管理



图表 28：知识体：信息安全风险管理

2.8.1 知识域：信息安全风险管理工作内容

- 知识子域： 风险管理工作主要内容
  - 掌握建立背景的主要工作内容
  - 掌握风险评估的主要工作内容
  - 掌握风险处置的主要工作内容
  - 掌握批准监督的主要工作内容
  - 掌握监控审查的主要工作内容
  - 掌握沟通咨询的主要工作内容
- 知识子域： 系统生命周期中的风险管理
  - 掌握系统规划阶段的风险管理工作
  - 掌握系统设计阶段的风险管理工作
  - 掌握系统实施阶段的风险管理工作
  - 掌握系统运行维护阶段的风险管理工作
  - 掌握系统废弃阶段的风险管理工作

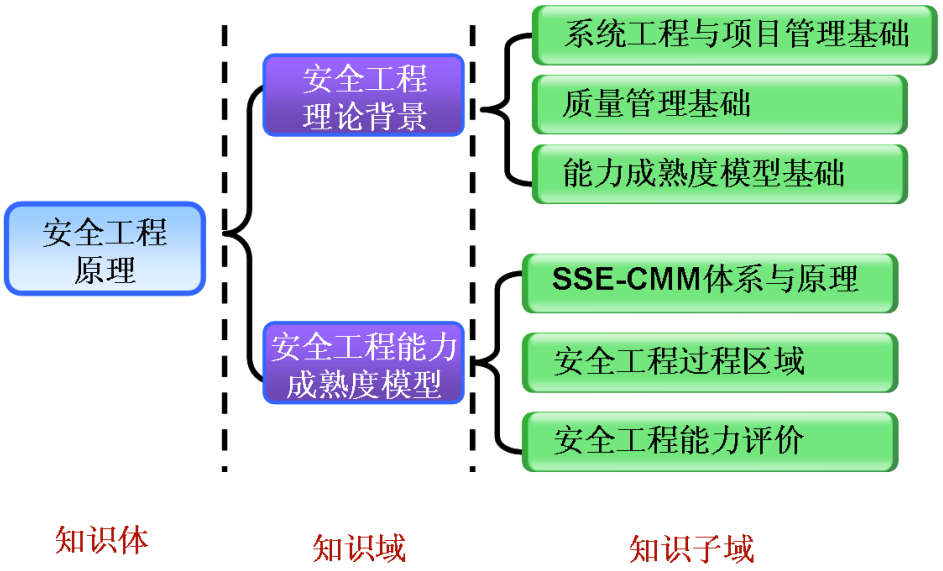
2.8.2 知识域：信息安全风险评估实践

- 知识子域：风险评估流程和方法
  - 掌握国家对开展风险评估工作的政策要求

- ◆ 理解风险评估、检查评估和等级保护测评之间的关系
- ◆ 掌握风险评估的实施流程：风险评估准备、资产识别、威胁评估、脆弱性评估、已有安全措施确认、风险分析、风险评估文档记录
- ◆ 理解定量风险分析和定性风险分析的区别及优缺点
- ◆ 理解自评估和检查评估的区别及优缺点
- ◆ 掌握典型风险计算方法：年度损失值（ALE）、矩阵法、相乘法
- ◆ 掌握风险评估工具：风险评估与管理工具、系统基础平台风险评估工具、风险评估辅助工具

- 知识子域：风险分析实例
  - ◆ 了解典型信息系统风险评估实践过程

2.9 知识体：信息安全工程原理



图表 29：知识体：信息安全工程原理

2.9.1 知识域：安全工程理论背景

- 知识子域： 系统工程与项目管理基础
  - 了解系统工程基本思想
  - 了解项目管理基本概念和要素
- 知识子域：质量管理基础
  - 了解质量管理基本概念
- 知识子域：能力成熟度模型
  - 理解“能力成熟度模型”基本思想
  - 了解能力成熟度模型的应用范围
  - 了解“过程能力方案”和“组织机构成熟度方案”的区别

2.9.2 知识域： 安全工程能力成熟度模型

- 知识子域： SSE-CMM 体系与原理
  - 了解 SSE-CMM 的适用范围
  - 了解过程、过程区域和过程能力的概念
  - 了解域维/安全过程区域与能力维/公共特征的关系
- 知识子域： 安全工程过程区域
  - 了解过程类、过程区域和基本实施的关系

- ◆ 理解风险过程、工程过程和保证过程的含义
- ◆ 了解各个安全工程过程区域的含义

- 知识子域： 安全工程能力评价
  - ◆ 理解能力级别、公共特征和通用实施的关系
  - ◆ 理解各个信息安全工程能力级别的含义

第 3 章 知识类：软件安全开发

软件安全开发首先讲授了传统软件开发的局限和当前软件安全开发的发展，然后按照整个软件开发的生命周期依次介绍了软件安全需求分析、安全设计、安全编码、安全测试，以及安全部署与安全开发项目管理方面的知识。它是注册信息安全开发人员需要重点掌握的基础知识。通过本部分的学习，学员应当：

- 了解软件安全开发的发展，国内外的相关政策和标准；
- 掌握各软件安全开发模型的基本思想；
- 理解典型安全需求分析方法；
- 掌握软件安全设计的原则及其在安全设计方法中的运用；
- 掌握典型安全缺陷及其防御措施；
- 掌握模糊测试、渗透测试等各类测试的原理和特点；
- 理解软件安全开发过程中项目管理生命周期的主要活动。

3.1 知识体：软件安全开发基础

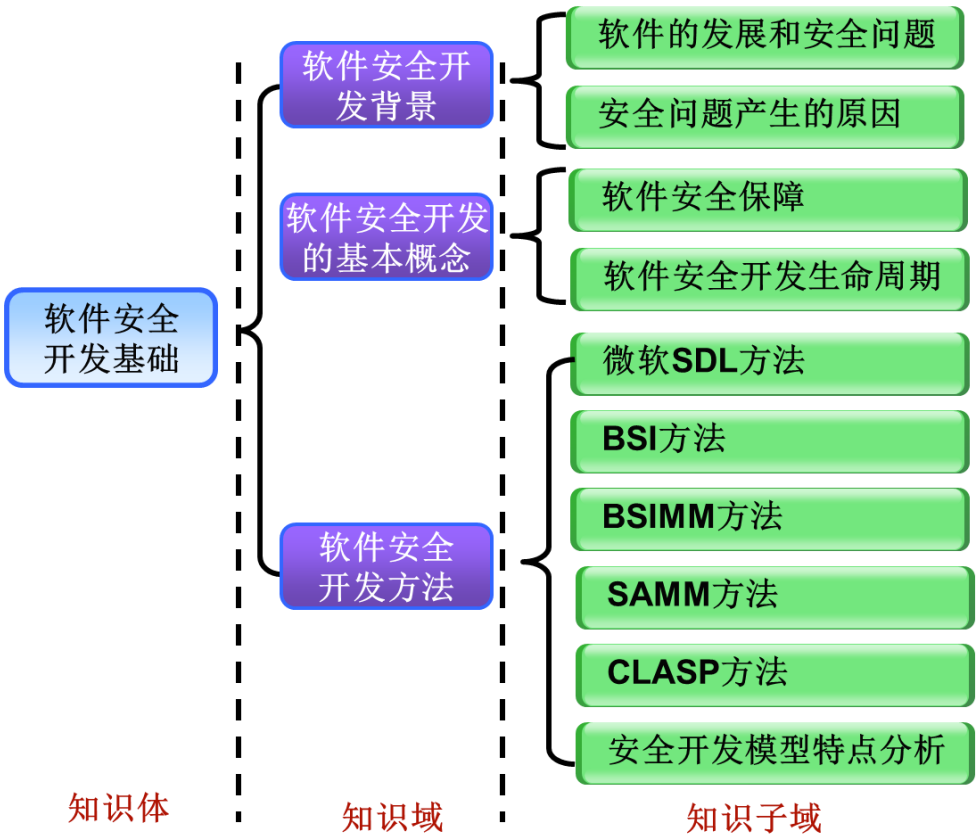


图 3-1：知识体：软件安全开发基础

3.1.1 知识域：软件安全开发背景

- 知识子域：软件的发展和安全问题
  - 了解当前软件的安全问题
  - 了解安全问题对软件属性的危害
- 知识子域：软件安全问题产生的原因
  - 理解软件自身的安全漏洞
  - 了解软件面临的外部威胁

3.1.2 知识域：软件安全开发的基本概念

- 知识子域：软件安全保障
  - 理解软件安全保障的定义
  - 理解软件安全保障的目标
  - 了解软件安全保障与风险管理的关系
- 知识子域：软件安全开发生命周期
  - 了解传统软件生命周期的缺陷
  - 理解软件安全开发生命周期的概念和目标

3.1.3 知识域：软件安全开发方法

- 知识子域：安全开发生命周期（微软 SDL）
  - 了解微软 SDL 的发展历史
  - 理解微软 SDL 的概念
  - 掌握微软 SDL 流程的 7 个阶段
- 知识子域：BSI（Build Security In）方法
  - 理解 BSI 方法的概念
  - 理解 BSI 软件安全方法的三根支柱
  - 掌握 BSI 软件安全接触点模型
- 知识子域：BSIMM（Build Security In Maturity Model）方法
  - 理解 BSIMM 方法的概念
  - 了解 BSIMM 方法的发展历史
  - 掌握 BSIMM 软件安全开发框架的 4 大领域 12 项实践
- 知识子域：软件成熟度模型（SAMM）方法
  - 理解 SAMM 的目的与作用
  - 掌握 SAMM 的总体结构
  - 了解 SAMM 的成熟度评估方法
- 知识子域：综合的轻量应用安全过程（CLASP）
  - 了解 CLASP 的概念

- 理解 CLASP 的特点
- 了解 CLASP 的角色和描述

- 知识子域：软件安全开发模型特点分析
  - 理解微软 SDL 方法的特点
  - 理解 BSI 系列方法的特点
  - 理解 CLASP 方法的特点
  - 理解 SAMM 的特点

3.2 知识体：安全需求分析

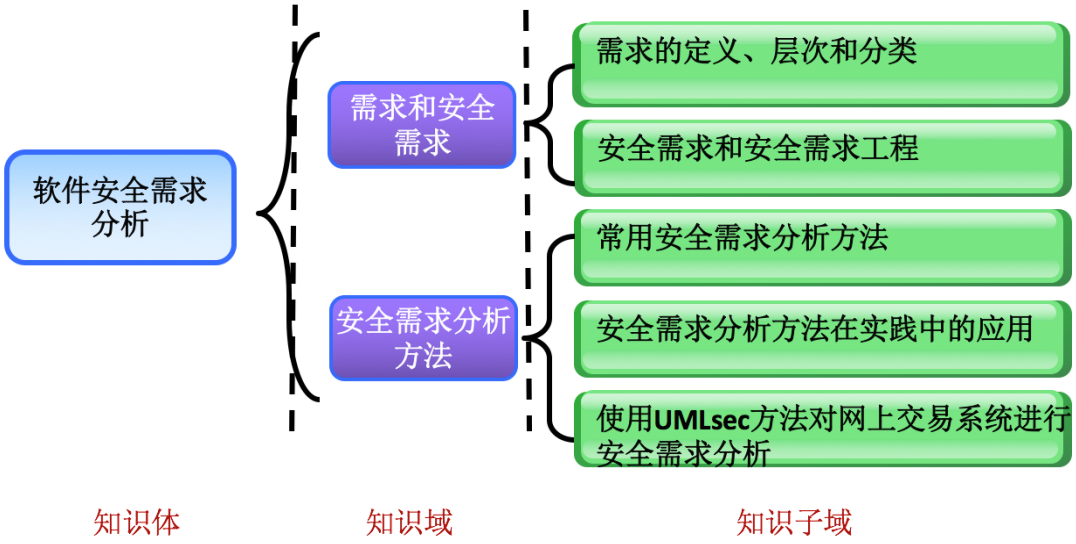


图 32：知识体：安全需求分析

3.2.1 知识域：需求和安全需求

- 知识子域：需求的定义、层次及分类
  - 了解需求问题的提出以及需求分析对于成功软件项目的重要性
  - 了解几种经典的需求的定义
  - 了解需求的三个不同层次及类型
- 知识子域：安全需求和安全需求工程
  - 了解需求与安全需求联系和区别
  - 理解主流的学者对安全需求的定义
  - 理解应用安全需求工程的重要性

3.2.2 知识域：安全需求分析方法

- 知识子域：常用安全需求分析方法

- 了解误用和滥用案例和 SEUARE 过程模型等需安全需求分析方法的基本原理和主要步骤
- 理解误用/滥用案例和 SEUARE 过程模型等安全需求分析方法的背后思想

- 知识子域：安全需求分析方法在实践中的应用
  - 理解 SDL 在需求分析阶段所使用的主要方法和注意事项
  - 理解七个接触点在需求分析阶段所使用的主要方法和注意事项
  - 理解 CLASP 在安全需求分析中的应用
  - 理解 IBM 软件安全开发生命周期中强调的安全需求
  - 理解 CC 标准在安全需求分析过程中的作用
- 知识子域：使用 UMLsec 方法对网上交易系统进行安全需求分析
  - 了解 UMLsec 的定义
  - 理解 UMLsec 的安全属性的添加
  - 理解 UMLsec 的安全属性在安全需求分析中的应用

3.3 知识体：软件安全设计

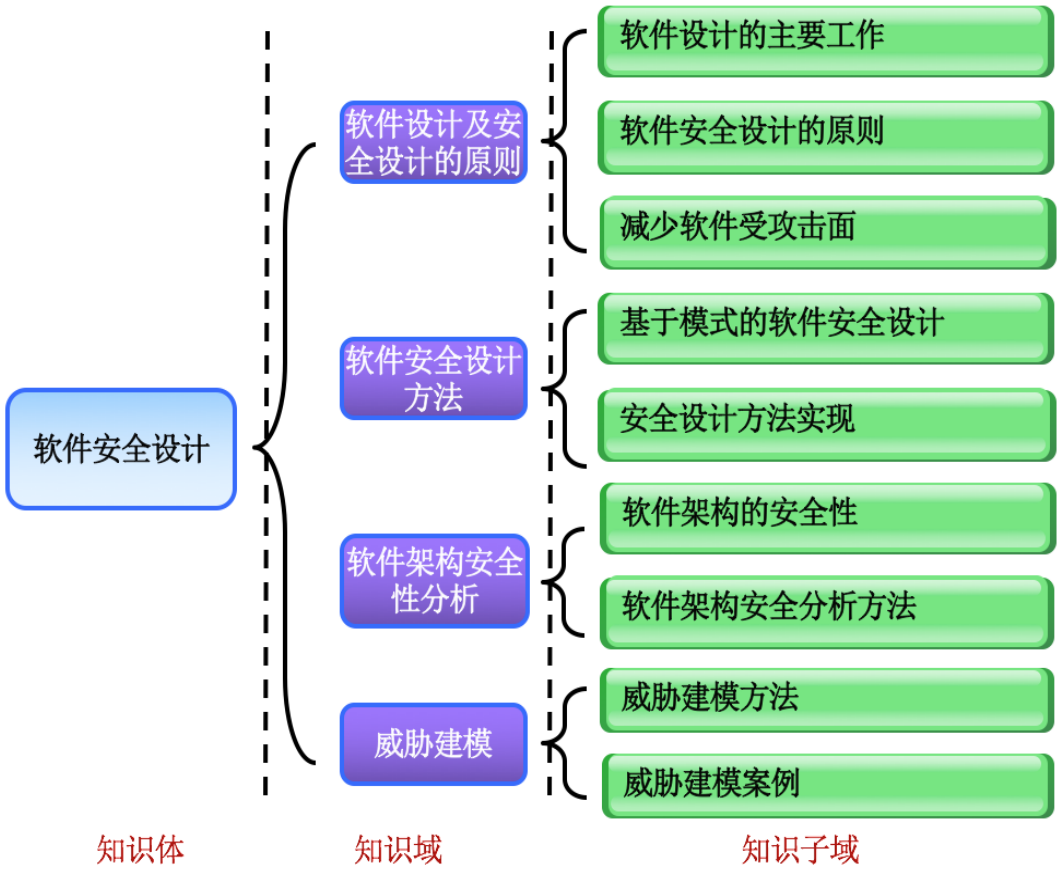


图 33：知识体：软件安全设计

3.3.1 知识域：软件设计及安全设计的基本原则

- 知识子域：软件设计的主要工作
  - 理解架构和设计在软件开发中的重要性
  - 了解软件设计的一般过程
- 知识子域：软件安全设计的原则
  - 掌握软件安全设计的最小特权、职责分离、纵深防御、默认安全、减少攻击面、心理可接受和隐私保护原则的思想及其运用
- 知识子域：减少软件受攻击面
  - 理解攻击面和减少攻击面在软件开发中的重要性
  - 理解汽车远程攻击面分析例子

3.3.2 知识域：软件安全设计方法

- 知识子域：基于模式的软件安全设计
  - 了解设计模式在软件设计阶段中的运用
  - 了解安全模式在软件安全开发中的作用
  - 理解典型安全模式的基本原理
- 知识子域：基于模式的软件安全设计
  - 了解 SDL 软件安全开发流程中的安全设计的主要思想和方法
  - 了解七个接触点软件安全开发流程中的安全设计的主要思想和方法
  - 了解 IBM 软件安全开发生命周期中软件安全开发流程中的安全设计的主要思想和方法

3.3.3 知识域：软件架构安全性分析

- 知识子域：软件架构的安全性
  - 理解软件架构的含义和基本原理
  - 理解软件架构的安全性的内容
  - 了解软件安全架构的构建主要步骤
- 知识子域：软件架构安全分析方法
  - 理解软件架构安全性分析的原理及其作用
  - 了解软件架构安全性的形式化方法和工程化方法的主要思想和特点

3.3.4 知识域：威胁建模

- 知识子域：威胁建模方法
  - 了解威胁建模的主要方法：基于树结构的威胁表示法，基于网结构的威胁表示法和基于图结构的威胁表示法

- 掌握威胁建模的 STRIDE 方法的主要步骤

● 知识子域：威胁建模案例

- 理解对网上书店进行威胁建模的步骤
- 掌握威胁建模基本方法，能够进行简单的分析

3.4 知识体：软件安全编码

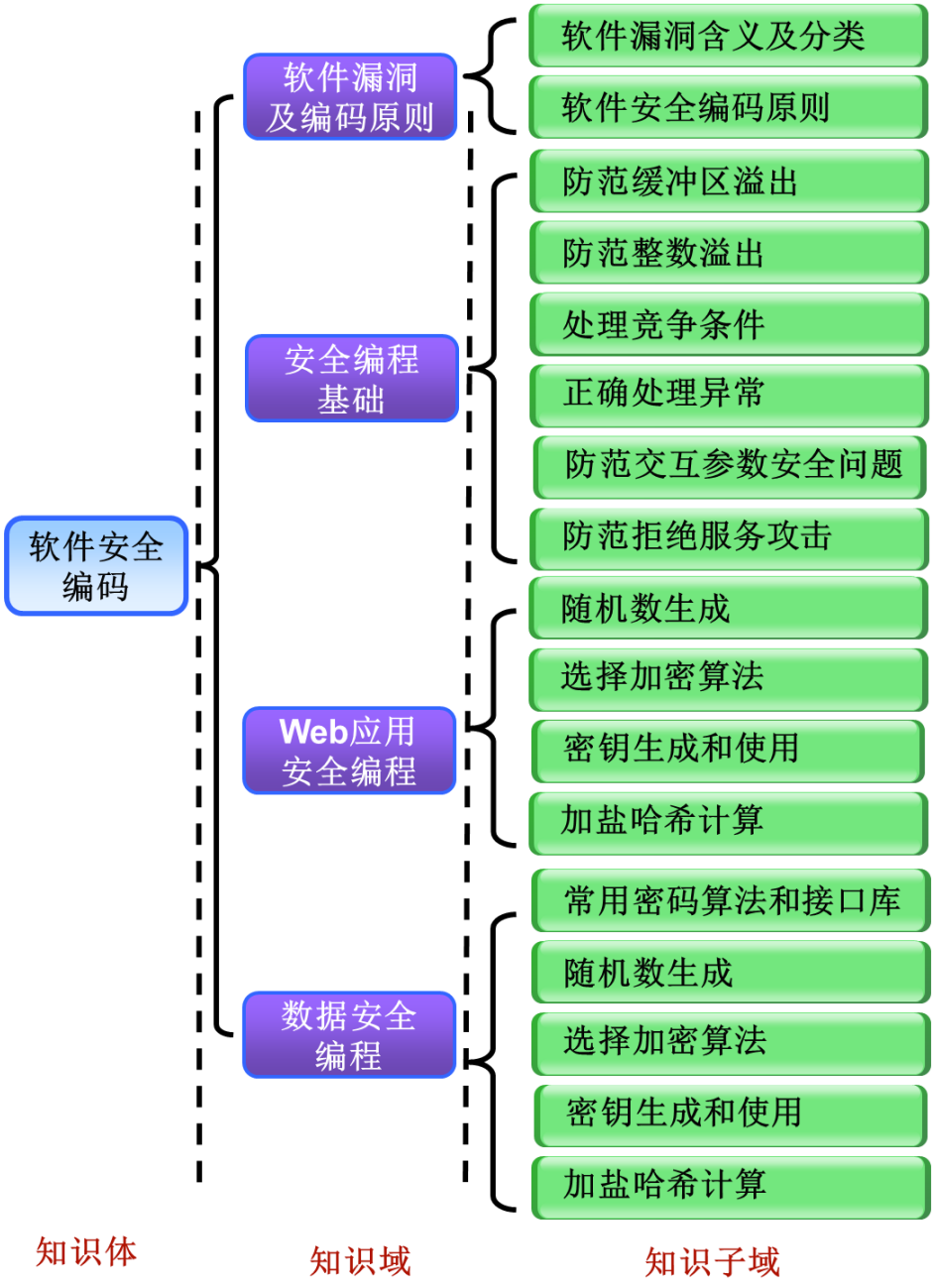


图 3-4：知识体：软件安全编码

3.4.1 知识域：软件漏洞与编码原则

- 知识子域：软件漏洞含义及分类
  - 了解中国国家信息安全漏洞库
  - 了解国家信息安全漏洞共享平台
  - 了解美国国家漏洞数据库
  - 理解“七界”分类法
  - 理解 Web 应用漏洞 Top 10
- 知识子域：软件安全编码原则
  - 理解常见的安全编码实践原则，如：规范编码、代码简洁、处理警告、验证输入、净化数据、最少反馈、检查返回、加强检查、安全编译

3.4.2 知识域：安全编程基础

- 知识子域：防范缓冲区溢出
  - 理解缓冲区溢出的概念和成因
  - 理解缓冲区溢出导致的后果
  - 掌握防范缓冲区溢出的方法
- 知识子域：防范整数溢出
  - 理解整数溢出的概念和成因
  - 掌握避免整数溢出的方法
- 知识子域：处理竞争条件
  - 理解竞争条件问题的概念和后果
  - 掌握处理竞争条件的解决方法
- 知识子域：正确处理异常
  - 理解异常处理不当的情形和后果
  - 理解通用异常处理的编码建议
- 知识子域：防范交互参数安全问题
  - 了解环境变量的安全隐患和应对方法
  - 理解防范文件名和文件内容攻击的安全措施
  - 了解对命令行数据的安全检查
- 知识子域：防范拒绝服务攻击
  - 了解拒绝服务攻击的目的
  - 理解拒绝服务攻击的应对措施

3.4.3 知识域：Web 应用安全编程

- 知识子域：防范 SQL 注入攻击
  - 理解 SQL 注入的原理与条件

- 掌握防范 SQL 注入的常用方法

- 知识子域：防范 XSS 跨站脚本攻击
  - 理解跨站脚本攻击的原理
  - 理解跨站脚本攻击的攻击形式
  - 掌握防御 XSS 跨站脚本攻击的方法
- 知识子域：避免重定向漏洞
  - 理解造成重定向漏洞的原因
  - 理解重定向漏洞的解决方法
- 知识子域：避免跨站请求伪造漏洞
  - 理解跨站请求伪造漏洞的原理
  - 了解 CSRF 攻击的流程及实现
  - 理解 CSRF 攻击的防御方法

3.4.4 知识域：数据安全编程

- 知识子域：常用密码算法和接口库
  - 了解密码算法的选择方法
  - 理解常用密码库
  - 了解我国商用密码算法接口
- 知识子域：随机数生成
  - 理解缓冲区溢出、整数溢出等攻击的成因与危害
  - 掌握输入验证、替换危险的函数等防御措施
- 知识子域：选择加密算法
  - 理解选择加密算法的注意事项
  - 理解编写加密代码的正确流程
- 知识子域：密钥生成和使用
  - 了解密钥管理方面易犯的错误
  - 理解密钥管理应当遵循的策略
- 知识子域：加盐哈希计算
  - 了解哈希算法和盐值的概念
  - 理解加盐哈希算法的运算原理
  - 理解保证哈希计算安全强度的方法

3.5 知识体：软件安全测试

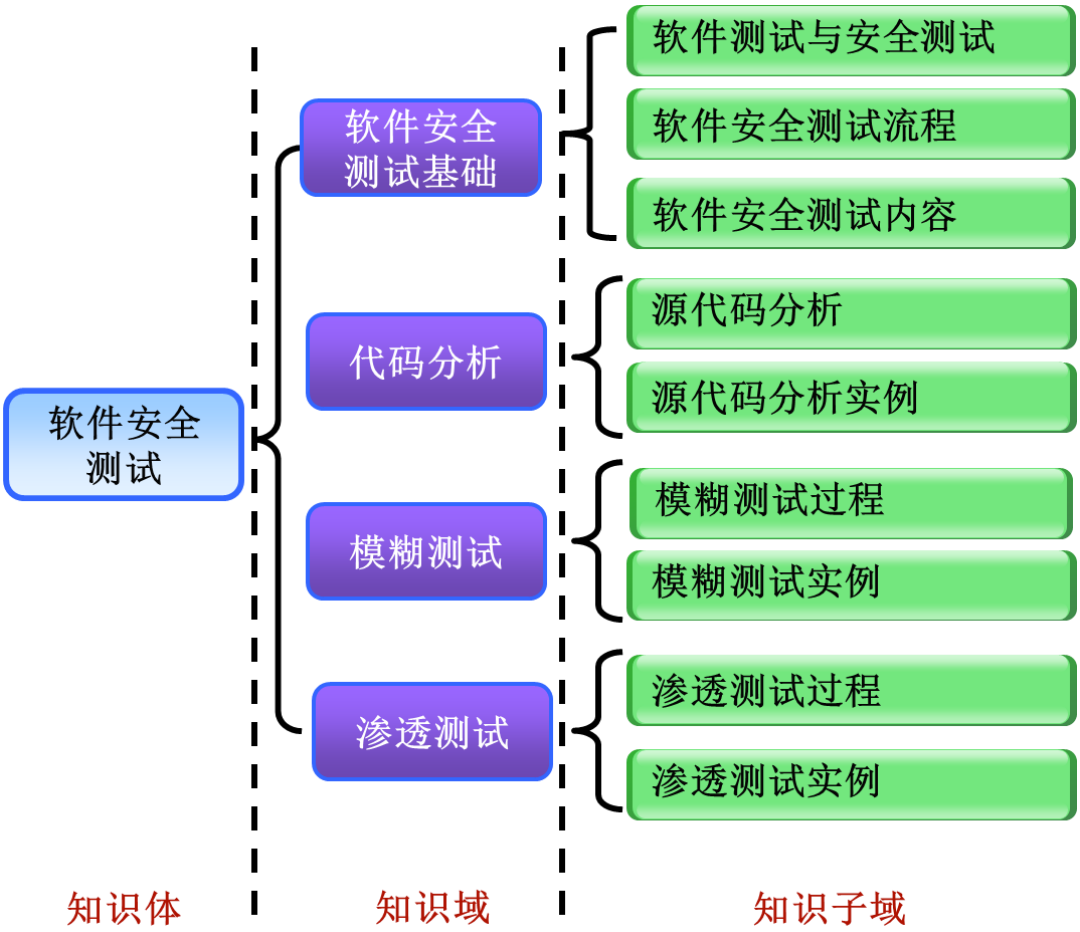


图 3-5：知识体：软件安全测试

3.5.1 知识域：软件安全测试基础

- 知识子域：软件测试与安全测试
  - 了解软件测试的基本概念
  - 理解安全测试的基本概念
  - 理解安全测试与软件测试的区别
- 知识子域：软件安全测试流程
  - 了解安全测试流程
  - 理解安全测试的原则
- 知识子域：软件安全测试内容
  - 理解安全功能验证
  - 理解安全策略验证
  - 理解威胁缓解措施验证

- 理解系统实现安全验证

3.5.2 知识域：代码分析

- 知识子域：源代码分析
  - 了解代码分析的两种分类
  - 理解源代码分析的意义
  - 掌握源代码分析的流程
- 知识子域：源代码分析实例
  - 了解源代码分析工具
  - 理解使用工具分析代码

3.5.3 知识域：模糊测试

- 知识子域：模糊测试过程
  - 了解模糊测试的基本概念
  - 理解模糊测试的过程
  - 了解模糊测试的方法
- 知识子域：模糊测试实例
  - 了解模糊测试工具
  - 理解使用工具进行模糊测试的过程
  - 了解模糊测试的方法

3.5.4 知识域：渗透测试

- 知识子域：渗透测试过程
  - 了解渗透测试的基本概念
  - 理解渗透测试的作用
  - 理解渗透测试的过程
- 知识子域：渗透测试实例
  - 了解渗透测试的常用工具
  - 理解渗透测试的方法

3.6 知识体：软件部署和项目管理安全

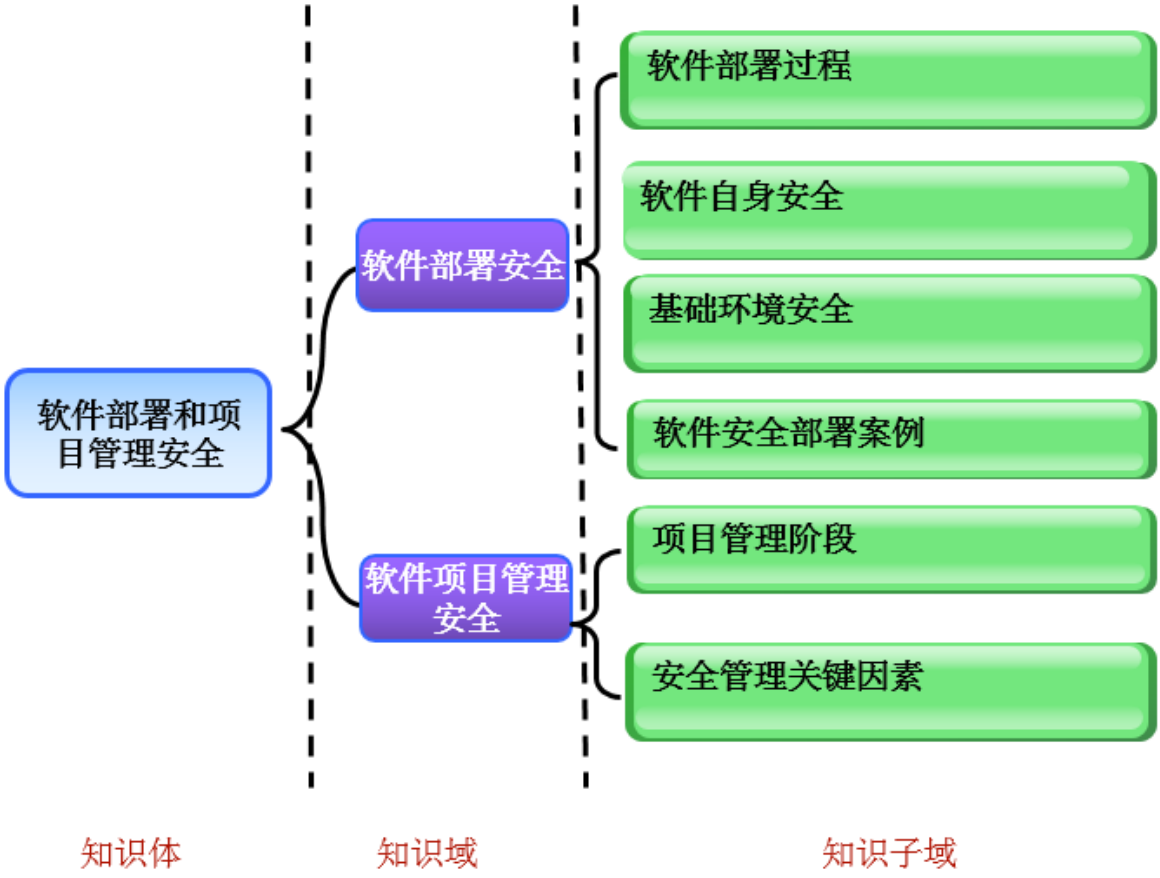


图 36：知识体：软件部署和项目管理安全

3.6.1 知识域：软件部署安全

- 知识子域：软件部署过程
  - 了解软件部署的一般过程
- 知识子域：软件自身安全
  - 了解软件安装配置的基本模式
  - 了解加强软件自身安全防护的安全策略
  - 了解漏洞修复的基本过程
- 知识子域：基础环境安全
  - 了解一些应用系统常见安全威胁
  - 了解基础环境软件配置方法
  - 了解基础环境漏洞处理方法
- 知识子域：软件安全部署案例

- ◆ 了解案例分析过程
- ◆ 理解案例体现的安全部署思想

3.6.2 知识域：软件项目管理安全

- 知识子域：项目管理阶段
  - ◆ 了解项目管理四个阶段的基本内容
- 知识子域：安全管理关键因素
  - ◆ 了解安全团队模型
  - ◆ 了解软件项目管理的风险识别和风险应对措施
  - ◆ 了解软件安全质量管理实施措施

附件 1：国家注册信息安全开发员（CISD）认证培训课程安排

时间		课程内容
第一天	上午	信息安全保障基本知识
	下午	信息安全风险管理
第二天	上午	信息安全法规与政策、信息安全标准
	下午	访问控制
第三天	上午	密码学基础
	下午	网络安全
第四天	上午	系统安全
	下午	信息安全工程原理
第五天	上午	软件安全开发基础
	下午	安全需求分析
第六天	上午	软件安全设计
	下午	软件安全编码
第七天	上午	软件安全测试
	下午	软件安全部署与安全开发项目管理
第八天	上午	实验案例一
	下午	实验案例二
第九天	上午	考试