

## 一、信息安全概述

1. 掌握信息安全的基本概念；
2. 熟悉信息安全的威胁；
3. 掌握信息安全技术体系；
4. 掌握信息安全模型。

## 二、密码技术

1. 掌握古典密码；
2. 掌握序列密码的特点及代表算法；
3. 掌握分组密码的特点及代表算法；
4. 掌握公钥密码的特点、代表算法、用途；
5. 了解杂凑函数的特点；
6. 熟悉消息认证码与分组密码的关系；
7. 掌握密钥管理的方式。

## 三、标识与认证技术

1. 掌握标识；
2. 熟悉口令与挑战-响应技术；
3. 掌握在线认证服务技术；
4. 掌握公钥认证技术；
5. 掌握 PKI 技术。

## 四、授权与访问控制技术

1. 熟悉授权和访问控制策略的概念；
2. 掌握自主访问控制；
3. 掌握强制访问控制；
4. 了解基于角色的访问控制。

## 五、信息隐藏技术

1. 掌握隐藏信息的基本方法；
2. 掌握数字水印；
3. 了解数字隐写。

## 六、网络与系统攻击技术

1. 掌握网络与系统攻击技术的主要类型；
2. 掌握拒绝服务攻击的基本原理；
3. 掌握缓冲区溢出攻击的原理。

## 七、网络与系统安全防护与应急响应技术

1. 掌握防火墙技术原理；
2. 掌握入侵检测技术原理；
3. 了解应急响应技术。

## 八、安全审计与责任认定技术

1. 掌握审计系统;
2. 掌握事件分析与追踪;
3. 掌握数字取证;
4. 熟悉数字指纹与追踪码。

## 九、主机系统安全技术

1. 了解操作系统安全技术;
2. 了解数据库安全技术;
3. 掌握操作系统和数据库安全技术的异同点;
4. 熟悉可信计算技术的相关基本概念。

## 十、网络安全技术

1. 掌握 OSI 安全体系结构;
2. 熟悉 SSL/TLS 协议及主要解决的问题;
3. 熟悉 IPSec 协议及主要解决的问题。

## 十一、恶意代码检测与防范技术

1. 熟悉常见的恶意代码;
2. 掌握恶意代码的机理。

## 十二、内容安全及信息安全测评技术

1. 熟悉内容安全的概念及其常见技术;
2. 掌握评估准则及其主要模型与方法。

## 十三、信息安全管理技术

1. 了解信息安全规划;
2. 掌握信息安全风险评估;
3. 熟悉物理安全保障措施;
4. 掌握信息安全等级保护;
5. 熟悉 ISO 信息安全管理标准;
6. 掌握信息安全法规。

## 参考书目:

《信息安全技术概论》，冯登国、赵险峰编著，电子工业出版社，2009 年 4 月版。