

目录

一. 信息安全基本概念

- 信息
- 信息熵
- 信息安全
 - 实体安全
 - 网络安全
 - 系统安全
 - 数据安全
 - 内容安全
- CIA 安全需求模型
 - 保密性
 - 完整性
 - 可用性
- 更多需求
 - 不可抵赖性
 - 可认证性
 - 可控性
 - 可审查性
 - 可存活性

二. 信息加密

- 密码技术的发展
 - 古典密码
 - 密码学
 - 公钥密码体制
 - 量子密码学
- 密码系统组成
 - 明文空间 M
 - 密文空间 C
 - 密钥空间 K
 - 加密算法 E
 - 解密算法 D
- 密码系统分类
- 密码系统安全性
- 古典密码
 - 塞塔式密码
 - 置换密码
 - 替代密码
 - 单表替代密码
 - 同音替代密码
 - 多表替代密码

- 多字母替代密码
- 一次一密方案 OTP
 - Verman 密码
- 转轮机
- 密码学
 - 序列密码（流密码）
 - 分组密码（块密码）
 - Feistel 网络
 - DES 加密算法
 - DES 工作模式
 - 电子密码本 ECB
 - 密码分组链接 CBC
 - 密码反馈 CFB
 - 输出反馈 OFB
- 公钥密码体制
 - 算法条件
 - 单向陷门函数
 - RSA 算法

三. 消息鉴别

- 基于消息摘要的消息鉴别
- 基于 MAC 的鉴别方法
- MAC 函数的设计要点
- 单向散列函数（哈希）
 - MD5 算法

四. 数字签名

- 数字签名的特性
 - 不可伪造性
 - 可信性
 - 不可更改性
 - 不可重用性
 - 抗抵赖性
- RSA 签名体制
- DSS 签名标准
 - DSA 签名算法
- 其他签名模式
 - 不可否认签名
 - 盲签名
 - 群签名
 - 代理签名
 - 指定证实人签名

五. 信息隐藏

- 信息隐藏分类

- 隐秘信道
- 伪装术
- 匿名通信
- 数字水印
 - 数字水印的特性
 - 数字水印的分类
 - 嵌入 / 提取过程
 - 空域水印技术
 - 最低有效位方法 LSB
 - Patchwork 方法
 - 文档结构微调
 - 变换域水印技术

六. 密钥管理

- 密钥生成管理
 - 产生模式
 - 有边界产生
 - 无边界产生
 - 产生形式
 - 手工产生
 - 自动产生
- 密钥建立管理
 - D-H 协议（基于协商）
 - 对称密钥的分配技术
 - 通信方 + 物理方法
 - 通信方 + 保密信道
 - 第三方 + 物理方法
 - 第三方 + 保密信道
 - KDC 模式
 - 公开（非对称）密钥的分配技术
 - 公钥发布
 - 量子密钥分配技术
 - BB84 协议
- 密钥存储管理
 - 整体保存
 - 分散保存
 - Shamir 门限方案

七. 网络攻击

- 系统安全漏洞扫描
- 网络监听（嗅探）
 - 共享式局域网的监听
 - 交换式局域网的监听
 - ARP 欺骗
 - IP 源地址欺骗

- 源路由选择欺骗
 - 网络监听的检测方法
 - 网络监听的防范方法
- 拒绝服务攻击
 - 拒绝服务攻击 DoS
 - SYN 泛洪
 - UDP 泛洪
 - Ping 泛洪
 - 泪滴攻击（碎片攻击）
 - Land 攻击
 - Smurf 攻击
 - 分布式拒绝服务攻击 DDoS
 - 拒绝服务攻击的防范方法
 - 主机设置
 - 网络设备设置
- 缓冲区溢出攻击
- SQL 注入攻击
- 计算机病毒
 - 主控模块
 - 感染模块
 - 触发模块
 - 破坏模块
 - 检测方法
- 木马程序

八. 防火墙

- 性能指标
- 优缺点
- 防火墙技术
 - 包过滤
 - 应用代理
 - 状态检测
 - 地址翻译 NAT
- 防火墙体系结构
 - 屏蔽路由器
 - 单宿主机网关
 - 双宿主机网关
 - 屏蔽子网网关

九. 入侵检测

- 入侵检测系统 IDS
- 入侵检测需求特性
 - 实时性要求
 - 可扩展性要求
 - 适应性要求

- 安全性要求
 - 有效性要求
- 性能参数
 - 误报率
 - 漏报率
- 入侵检测过程
 - 信息收集
 - 信息分析
 - 结果处理
- 通用模型
 - CIDE 模型
- 入侵检测分类
 - 数据
 - 基于主机的入侵检测 HIDS
 - 基于网络的入侵检测 NIDS
 - NIDS 抓包
 - 分析方法
 - 异常检测
 - 误用检测

十. 身份认证

- 身份证明系统
 - 示证者
 - 验证者
 - 攻击者
 - 可信赖者
- 基于口令的身份认证
 - 静态口令
 - 动态口令
 - 挑战 / 应答口令原理
 - S / Key 原理
- 基于密码的身份认证
 - Kerberos 认证模型
- 基于零知识证明的身份认证
 - 零知识洞穴协议
- 基于生物特征的身份认证技术

十一. 区块链

- 区块链的特性
 - 去中心化
 - 开放, 共识
 - 不可篡改, 可追溯
 - 交易透明, 双方匿名
- 区块链的分类
 - 公有链

- 私有链
 - 联名链
- 区块链的数据结构
 - Hash 指针
 - Merkle 梅根树
 - SPV 交易验证
- 比特币交易模型 UTXO
- 区块链交易产生过程
 - POW 原理
- 51% 攻击问题