ch11 公钥基础设施

- PKI 体系结构的组成 P9
  - 保证公钥真实性 P19
  - PKI 作用 P20~22
  - CA P23~25
  - RA P28
  - 证书库 P29
  - 安全服务器 P30
  - 密钥备份和恢复系统 P31
  - 证书撤销列表 P32
  - PKI 应用接口系统 P33
  - CA 的信任关系 P34
  - PKI 信任模式 P35~36
  - CA 的层次结构 P37
- CA的信任模型 P38
  - 1. 单CA信任模型：基本信任模型，也是目前许多组织或单位在Intranet中普遍使用的一种模型
  - 2. 层次信任模型：层次信任模型也称为分级信任模型，它是一个以主、从CA关系建立的分级PKI结构
  - 3. 分布式信任模型：分布式信任模型也称为网状信任模型，在这种模型中CA间存在着交叉认证
  - 4. 桥CA的信任模型：桥CA信任模型也称为中心辐射式信任模型，被设计成用来克服层次信任模型和分布式信任模型的缺点，并连接不同的PKI系统。
  - 5. WEB信任模型：Web信任模型构建在Web浏览器的基础上，浏览器厂商在浏览器中内置了多个根CA，每个根CA相互间是平行的，浏览器用户同时信任多个根CA并把这些根CA作为自己的信任锚。Web信任模型通过与相关域进行互连而不是扩大现有的主体群来使用户实体成为在浏览器中所给出的所有域的依托方。
  - 严格层次结构模型 P40~42
  - 层次模型的优缺点 P45
  - CA
  - 分布式信任模式 P46
  - 交叉验证 P47~48
  - 桥 CA 信任模型 P49
  - Web CA 信任模式 P50 & P54
  - 以用户为中心的信任模式 PGP P56
- PKI 安全问题 P59
  - 1. 数字证书颁发过程中的安全问题：证书的合法性难以保证，误发证书，恶意颁发证书，钓鱼网站证书
  - 2. 数字证书维护过程中的安全问题：证书的有效性难以验证，证书过期，证书撤销
  - PKI 证书撤销 P63
    - 私钥泄露、密钥更换、用户变化时，需要 撤销证书
    - CA 维 护 CRL (Certificate Revocation List) ，未到期但已撤销证书列表
    - 检查CRL的URL内嵌在用户证书，浏览器 安全访问URL查询证书状态, 确定是否被 CA 撤销
    - 在线证书状态协议 OCSP (online certificate status protocol)是CRL之外维护PKI证书安全的另一个协议
  - 中心化监督带来的问题 P64
- PKI安全问题的解决思路 P66
  - **建立监督机制** P67~68
  - 建立证书状态日志 P69
  - 证书撤销列表 P70
  - 在线证书状态 P71
  - 证书区块链 P72
- PKI 主要应用 P76
  - 数字证书使用