第七章 PKI和密码学应用

7.1 非对称密码学

- 对称密码系统具有共享的秘钥系统，从而产生了安全秘钥分发的问题
- 非对称密码学使用公钥和私钥对，无需支出复杂密码分发系统

7.1.1 公钥与私钥

7.1.2 RSA（兼具加密和数字签名）

- RSA算法依赖于大质数在因素分解时固有的计算难度

7.1.3 El Gamal

- El Gamal优点： 公开发布，使用免费（扩展了Diffie-Hellman秘钥交换协议，支持消息的加解密）
- 缺点：算法加密的任何消息的长度都加倍

7.1.4 椭圆曲线密码系统(ECC)

- 1088位的RSA秘钥相当于160位的椭圆曲线密码系统的秘钥强度

7.2 散列函数

- 散列函数的用途： 产生消息摘要
- 散列函数的基本要求：
  i. 输入值可以是任意长度
  ii. 输出值具有固定长度
  iii. 散列函数在计算任何输入值要相对容易
  iv. 散列函数是单向的
  v. 散列函数是不会发生冲突的

7.2.1 SHA

- SHA-1不安全，SHA-2理论上不安全

7.2.2 MD2

- 非单向函数，已不再使用

7.2.3 MD4

- MD4存在消息摘要冲突，不是安全的散列算法

7.2.4 MD5

- 512位的消息分组，消息摘要128位
- 散列函数以及生成函数值的长度

表 7.2　散列算法记忆表

算法名称	哈希值的长度(单位为位)
HAVAL——一种 MD5 变种	128、160、192、224 和 256
HMAC	可变
MD2	128
MD4	128
MD5	128
SHA-1	160
SHA-224	224
SHA-256	256
SHA-384	384
SHA-512	512

7.3 数字签名

- 数字签名的目标
  - 可以向接收方保证、消息确实来自自己申明的发送者，且实施了不可否认性
  - 向接收方保证：消息在传输过程中没有改变
- 消息签名本身不提供隐私保护，只满足加密目标中的完整性和不可否认性

7.3.1 HMAC 基于散列的消息身份认证代码

- 实现了部分数字签名功能，保证了消息传输过程的完整性、但不提供不可否认性
- HMAC依赖一个共享的秘钥，所以不提供不可否认性

7.3.2 数字签名标准

- DSS标准加密算法
- 数字签名算法（DSA）
- RSA算法（既能数字签名又能加密！）
- 椭圆曲线数字签名算法(ECDSA)

7.4 公钥基础设施(PKI)

- 公钥加密主要优点是原本不认识的双方之间的通信变得很容易，受信任的公钥基础设施层次使这一点称为可能

7.4.1 证书

- 数字证书为通信双方提供了保证，保证在与之通信的人确实具有他们所宣称的身份

7.4.2 证书授权机构

- 证书授权机构(CA)将基础设施绑定在一起，中立的组织机构为数字证书提供公证服务

7.4.3 证书的生成与撤销

1. 注册
    - 采取某种方式向证书授权机构证明身份的过程被称为注册
2. 验证
    - 通过CA的公钥检查CA的数字签名来验证证书，接着检查证书没在CRL（证书撤销列表）
3. 撤销
    - 证书撤销原因：证书遭到破坏、证书被错误的发放、证书的细节发生变化、安全性关联发生变化
    - 证书撤销的技术：
    - 证书撤销列表：缺点是必须顶起下载并交叉参照，证书的撤销和通知用户撤销之间存在时间延迟
    - 联机证书状态协议:解决认证撤销列表的固有延迟

7.4.4 非对称秘钥的管理

- 选择加密系统
- 选择秘钥
- 使用公钥加密时，一定要保证私钥的机密性
- 秘钥在服务一段时期后应当停止使用
- 秘钥备份

7.5 密码学的应用

7.5.1 便携式设备

- 目前主流操作系统都包括磁盘加密功能、商业工具提供额外的功能和管理能力

7.5.2 电子邮件

1. 电子邮件规则

    - 邮件机密性，加密邮件
    - 邮件完整性，进行散列运算
    - 邮件身份认证和完整性，进行数字化签名
    - 邮件机密性、完整性、身份认证和不可否认性，对邮件加密和数字化签名
2. 电子邮件标准
    - 可靠隐私（PGP）商业版RSA、IDEA加密协议，使用MD5生成消息摘要；免费版使用Diff-Hellman秘钥交换，CAST128位的加密/解密算法以及SHA-1散列函数
    - S/MIME(安全多用途互联网邮件扩展协议)：依靠X.509证书交换密码系统秘钥，这一支持AES、3DES和RSA

7.5.3 Web应用

- SSL协议，SSL的目标是建立安全的通信通道
    - POODLE攻击（贵宾犬攻击）的攻击表明在TLS的SSL 3.0反馈机制中存在重大缺陷，很多机构放弃对SSL的支持，依靠TLS的安全性。
- 隐写术和水印
    - 隐写术：使用密码学技术在另一条消息内嵌入秘密消息的方法
    - 水印：检测拷贝并且跟踪拷贝来源

7.5.4 数字版权管理(DRM)

- 音乐、电影、电子书、视频游戏、文档

7.5.5 网络连接

1. 链路加密
    - 链路加密使用软件或硬件解决在两个点之间建立一条安全隧道
    - 端到端加密有终于保护双方之间的通信安全，并且可以独立于链路加密实施
    - 链路加密和端到端的加密区别：链路加密中，所有的数据都会被加密，下一条重新解密然后加密，降低了路由速度，端到端的加密不加密头、尾、地址和路由数据，容易被嗅探和偷听者攻击
    - SSH是一个端到端的加密
2. IPSec（Internet密钥交换（IKE）解决了在不安全的网络环境（如Internet）中安全地建立或更新共享密钥的问题。）
    - IPSec通过公钥密码学提供加密、访问控制、不可否认性以及消息身份认证，并且一般使用IP协议
    - IPSec组件：
        - 身份验证头(AH),提供完整性和不可否认性的保证、提供身份认证和访问控制，并可以防止重放攻击
        - 安全封装有效载荷(ESP) 提供数据包内容的机密性和完整性，提供有限的身份认证，防止重放攻击

    - IPSec两种操作模式：
        - 运输模式：只有数据包有效载荷被加密，为对等通信设计
        - 隧道模式：整个数据包都会被加密，为网关间通信设计
3. ISAKMP（网络安全关联秘钥管理协议）
    - 通过协商、建立、修改和删除安全关联为IPSec提供后台的安全支持服务
    - ISAKMP基本要求：
        - 对通信对等进行身份关联
        - 建立并管理安全关联
        - 提供秘钥生成机制
        - 防止遭受威胁
4. 无线互联

- 有限等价隐私（WEP）
    - WiFi安全访问：通过TKIP（临时秘钥完整协议）消除危害WEP的密码学弱点（客户端到无线接入点）

7.6 密码学攻击

- 分析攻击：试图降低算法复杂性的代数运算，关注算法本身的逻辑
- 实现攻击：利用密码学系统的实现中的弱点，涉及错误与权限，编写加密系统程序所使用的方法
- 统计攻击：试图发现驻留密码学应用程序的硬件或操作系统中的漏洞
- 蛮力攻击：尝试有可能的、有效的秘钥或密码组合，彩虹表和转为蛮力涉及和开发的专业化、可扩展的硬件
- 频率分析和仅知密文攻击：拥有加密后的密文信息，即仅知密文攻击；频率分析就是一种已证明可行的对抗简单密码的技术
- 已知明文攻击：攻击者具有已加密消息的副本以及用以产生密文的明文消息
- 选定密文攻击：攻击者能够解密所选的部分密文信息，并且可以使用已解密的部分消息来发现秘钥
- 选定明文攻击：攻击者能够加密所选的明文信息，可以分析加密算法输出的密文
- 中间相遇攻击：针对使用两轮加密的算法
- 中间人攻击：怀有恶意的人置身于通信双方之间的位置并截获所有的通信
- 生日攻击：冲突攻击或逆向散列匹配，寻找散列函数一一对应特性中的缺陷，基于两个不同的消息使用相同的散列函数产生共同的消息摘要的概率
- 重放攻击：拦截通信双方的加密消息，重放捕捉的信息以打开新的会话