密码理论与技术

典型安全方案概览

消息认证和数字签名方案

基本概念：参阅Stallings教程11.2和13.1

典型安全问题

- 保密性问题
- 保护通过不可信任的信道所传输的信息不被泄露。
- 认证性(完整性)问题
- 保护通过不可信任的信道所传输的信息不被篡改。
- 秘密交换问题
- A、B通过不可信任的信道交换一组消息，最终生成第三方未知的共享秘密。
- ……

典型的认证类方案

- 消息认证码方案：对称类方案
  （*Message Authentication Code:MAC*）
- 数字签名方案：非对称方案/公钥方案
  （*Digital Signature*）

对称认证方案(1)

- 问题：A如何通过不可信任的信道，完全可信任地向B传递信息（抗篡改）
- A(K)　　A和B共享K　　B(K)

消息M　　2.传递M和σ

1.认证计算：

σ =MAC(K,M)

3.核实计算：

验证1=Vf(K,M, σ)

若1≠Vf(K,M, σ)

则拒绝接受M

对称认证方案(2)

- 特　点:
- 密钥生成算法KG, 认证码生成算法MAC, 认证码验证算法Vf均公开.
- 密钥K保密(仅通信双方知道且共享)
- 安全性(抗伪造):

攻击者F未知 K ,则

$P[(M^*,\sigma^*) \leftarrow F(|K|, MAC, Vf, KG):$

$Vf(K,M^*,\sigma^*)=1]$极小。

数字签名方案(1)

- 问题：如何通过不可信任的信道，完全可信任地传递信息（抗伪造）
- 接收方：A　　pk公开　　发布方：B(sk)

3.核实计算：

1=Vf(pk,M,t)

2.签字计算：

t=Sig(sk,M)

数字签名方案(2)

- 特　点:
- 密钥生成算法KG, 签字算法Sig, 验证算法Vf均公开。
- KG生成一对密钥，一个公开(pk),一个保密(sk)
- 私钥sk仅为签字方持有(通信双方不共享任何秘密)
- 一致性要求：　Vf(pk,Sig(sk,M))=1恒成立
- 安全性(抗伪造):

若攻击者F未知 sk，则

$P[(M^*, \sigma^*) \leftarrow F(pk, Sig, Vf, KG):$

$Vf(pk, M^*, \sigma^*)=1]$ 极小。

数字签名方案(3)

- ElGamal (1985)

- (1)公钥/私钥生成算法KG(k, g, q)，q是k位素数，g是q的原根:
- $x \leftarrow {}^{\$}F_q^*$; $y \leftarrow g^{-x} \bmod q$;
- 公钥vk←y; 私钥sk←x;

- (2)签名算法Sig^H(sk, M), 其中私钥sk=x，H是某个公开的安全散列函数
- $K \leftarrow {}^{\$}F_q$; $r \leftarrow g^K \bmod q$; $h \leftarrow H(M,r)$; $s \leftarrow (K+xh) \bmod (q-1)$;
- 注意这是一个随机算法，随机性来源于随机变量K。
- 对消息M的数字签名σ=(r,h,s)。

- (3) 验证算法Vf^H(vk, M, (r,h,s))，其中公钥vk=y:
- 若h= H(M,r) 且 $r=g^s y^h \bmod q$均成立，则接受M，否则拒绝M。

数字签名方案的应用：公钥证书

- 问题：

  如何将公钥与持有者可靠地联系起来？

工具：公钥证书及其管理协议(x.509/RFC2553)

机制：发布者对下辖用户的公钥做数字签名

用户#i的公钥证书$M(i)$是包含其公钥PK(i)及其安全属性的电子文件。

公钥发布者A以期私钥 sk(A) 生成数字签名$\sigma(i)$ =Sig(sk(A), $M(i)$)。

发布者发布完整的证书文件[$M(i)$, $\sigma(i)$]。

公钥PK(i)的使用者用A的公钥vk(A)验证证书文件的数字签名。

其他基础类安全方案(1)

- 无须公钥证书的公钥加密方案
- 无须公钥证书的签名方案
- (2001, Pairing-based/ECC, Identity-based Crypt.)
- 组群加密方案
- 组群签字方案

(2000, Group Crypt.)

- 密钥时变加密方案
- 密钥时变签字方案
- 等

其他基础类安全方案(2)

- IBE(Identity-based Encryption)：通用框架

- 一个IBE方案Π=(Setup, UKG, E, D)是一组算法，其中：
- (1)Setup是全局密钥生成算法，输出全局公钥-私钥偶(mpk, msk)；
- (2)UKG是用户私钥生成算法，以全局私钥msk、用户身份标识*a*为输入，输出*a*的私钥usk(*a*)；
- (3)E是加密算法，以全局公钥mpk、用户身份标识*a*和消息M为输入并输出密文y；
- (4)D是解密算法，以全局公钥mpk、用户私钥usk(*a*)和密文y为输入并输出明文M。

其他基础类安全方案(3)

- IBE(Identity-based Encryption)：通用框架(续)

- (1)所有以上算法须满足一致性关系：对任何k、a和M，若
- P[(mpk,msk)←Setup(k);
- usk(a)←UKG(msk,a);
- y←E(mpk, a, M);
- 则　　D(mpk, usk(a), y)=M]=1恒成立
- (2)由于IBE方案的特殊结构，在刻画其保密性质时需要考虑所谓合谋攻击，这时攻击者可能(通过非法入侵或合谋)持有某些合法用户a^1,…,a^n的私钥usk(a^1),…usk(a^n).
- **IBE方案的保密性要求**：如果攻击者不持有私钥usk(a)，无论事先能获得多少usk(a^1),…usk(a^n)(a^1,…,$a^n \neq a$)都无法从密文E(mpk, a, M)有效获取关于明文M的信息。