密钥管理与密码协商

主要内容

（1）对称密码体制的密钥管理

Ø密钥分类

Ø密钥分配

（2）公钥密码体制的密钥管理

Ø公钥的分配

Ø数字证书

ØX.509证书

Ø公钥基础设施PKI

对称密码体制的优缺陷

1. 优点：加密速度快,保密度高
2. 缺陷：

（1）密钥是保密通信的关键，发信方必须安全、妥善的把密钥送到收信方，不能泄露其内容，密钥的传播必须安全，怎样才干把密钥安全送到收信方是对称加密体制的突出问题。

（2）n个合作者，就需要n各不同的密钥，假如n个人两两通信需要密钥数量n(n-1)，使得密钥的分发复杂。

（3）通信双方必须统一密钥，才干发送保密信息，假如双方不相识，这就无法向对方发送秘密信息了。

（4）难以处理电子商务系统中的数字署名认证问题。对开放的计算机网络，存在着安全隐患，不适合网络邮件加密需要。

非对称密码体制的优缺陷

1. 缺陷：加密算法复杂，加密和解密的速度比较慢
2. 优点：

（1）公钥加密技术与对称加密技术相比，其优势在于不需要共享通用的密钥。

（2）公钥在传递和公布过程中虽然被截获，因为没有与公钥相匹配的私钥，截获的公钥对入侵者没有太大意义。

（3）密钥少便于管理，N个顾客通信只需要N对密钥，网络中每个顾客只需要保存自己的解密密钥。

（4）密钥分配简朴，加密密钥分发给顾客，而解密密钥由顾客自己保存。

密钥管理简介

全部的密码技术都依赖于密钥。

密钥的管理本身是一种很复杂的课题，而且是确保安全性的关键点。

密钥管理简介

密钥管理涉及确保产生的密钥具有必要的特征，通信双方事先约定密钥的措施以及密钥的保护等。

密钥管理措施实质上因所使用的密码体制（对称密码体制和公钥密码体制）而异。

密钥的生命周期

1. 全部的密钥都有生存期。
2. 密钥的生存周期：授权使用该密钥的周期。
3. 原因：

（1）拥有大量的密文有利于密码分析；一种密钥使用得太多了，会给攻击者增大搜集密文的机会；

（2）假定一种密钥受到危机或用一种特定密钥的加密/解密过程被分析，则限定密钥的使用期限就相当于限制劫难性后果影响的范围。

密钥的管理

一种密钥主要经历下列几种阶段：

1）产生（可能需要登记）

2）分配

3）启用/停用

4）更新/替代

5）撤消

6）销毁

密钥的管理

1.密钥的产生

“好”密钥的特征：

- 防止使用特定密码算法的弱密钥
- 随机、等概率的比特序列
- 足够的复杂度

（1）密钥产生的技术

- 硬件技术:
- 软件技术：
- X9.17三重DES密钥产生算法。

（2）不同类型密钥的产生措施

主密钥：真随机数

密钥加密密钥：高保真随机数、主密钥控制下的某种算法

会话密钥：随机数发生器

（3）密钥的登记

将产生的密钥与特定的使用捆绑在一起，例如，用于数字署名的密钥，必须与署名者的身份捆绑在一起。这个捆绑必须经过某一授权机构来完毕。

2. 密钥的注入

- 键盘输入
- 软盘输入
- 专用密钥注入设备

3. 密钥的存储

（1）存储方式：

- 用口令加密后存储在本地软盘或硬盘中
- 存储在网络目录服务器中
- 存储在智能卡中
- USB key存储

（2）保护措施

- 由一种可信方来分配；
- 将一种密钥提成两部分，委托给两个不同的人；
- 经过机密性（例如，用另一种密钥加密）和/或完整性服务来保护。

在网络安全中，用最终一种措施造成密钥层次的概念。这个概念一般出目前密钥管理之中。

4. 密钥的使用与控制

在当代网络安全实现中，有许多用于不同目的的不同密钥。例如，初始密钥用于加密和解密数据，而密钥加密密钥用于保护所分配的别的密钥。

除了秘密保存密钥之外，有时密钥分配过程也是很主要的，因为该过程确保打算用于一种目的的密钥不能和用于另一种目的的密钥交替使用。这就要求将密钥值和密钥的正当使用范围封装在一起。

5. 密钥的更新

6. 密钥的吊销与销毁

（1）密钥撤消:在特定的环境中是必须的。

撤消的原因:与密钥有关的系统的迁移怀疑一种特定的密钥已受到威胁；密钥的使用目的已经变化（提升安全级别）

(2)密钥销毁：清除一种密钥的全部踪迹。

一种密钥的值在被停止使用后可能还要连续一段时间，例如，一条记载的加密数据流包括的信息可能依然需要保密一段时间。为此，使用的任何密钥的秘密性都需要保持到所保护的信息不再需要保密为止。

密钥管理要到达目的

在遇到如下威胁时，仍能保持密钥关系和密钥：

- Ø危及秘密密钥的机密性（攻击机密性）
- Ø危及秘密密钥或公钥的真实性（欺骗）
- Ø危及密钥或公钥的未授权使用

秘密密钥的分配

- 基于对称密码体制的密钥分配

- 基于公钥密码体制的密钥分配

基于对称密码体制的密钥分配

对称密码体制的主要商业应用起始于八十年代早期，尤其是在银行系统中，采纳了DES原则和银行工业原则ANSI数据加密算法(DEA)。实际上，这两个原则所采用的算法是一致的。

基于对称密码体制的密钥分配

伴随DES的广泛应用带来了某些研究话题，例如怎样管理DES密钥。从而造成了ANSI X9.17原则的发展，该原则于1985年完毕，是有关金融机构密钥管理（批发）的一种原则。

基于对称密码体制的密钥分配

金融机构密钥管理需要经过一种多级层次密钥机构来实现。

用于加密大部分数据的密钥需要频繁更改（例如，每天更改一次或每次会话更改一次）。显然，这不适应于经过手工密钥分配系统来完毕，因为这种系统的代价太高。

对称密钥分配

1. 密钥分配问题是对称加密的关键问题。
2. 密钥分配的几种措施
   - ü密钥由A选择，并亲自交给B
   - ü第三方选择，并亲自交给A和B
   - ü用近来使用的密钥加密新密钥并发给对方
   - ü使用秘密信道
3. 密钥使用的规模：N(N+1)/2

密钥的分层管理

ANSI X9.17三层密钥层次构造：

1）主密钥，经过手工分配；

2）密钥加密密钥，经过在线分配；

3）初始密钥或数据密钥。

用主密钥保护密钥加密密钥的传播，用密钥加密密钥保护初始密钥的传播。

主密钥是通信双方长久建立密钥关系的基础。有两类基本的构造：

（1）点到点构造

（2）密钥中心

使用对称密码技术分配对称密钥的措施在许多环境中依然使用。

然而，人们倾向于使用公钥密码或DH密钥分配措施分配对称密钥。