网络与信息安全

身份鉴别

讨论议题

- 鉴别的基本概念
- 鉴别机制
- 鉴别与交换协议
- 典型鉴别实例

鉴别Authentication

- The property that ensures that the identity of a subject or resource is the one claimed. Authenticity applies to entities such as users, processes, systems and information.
- 鉴别就是确认实体是它所声明的。
- 鉴别是最重要的安全服务之一。鉴别服务提供了关于某个实体身份的保证。（所有其它的安全服务都依赖于该服务）
- 鉴别可以对抗假冒攻击的危险

鉴别的需求和目的

- 问题的提出
  - 身份欺诈
- 鉴别需求：
  某一成员（声称者）提交一个主体的身份并声称它是那个主体。
- 鉴别目的：
  使别的成员（验证者）获得对声称者所声称的事实的信任。

身份鉴别

- 定义：证实客户的真实身份与其所声称的身份是否相符的过程。
- 依据：
  - Something the user know (所知）
    - 密码、口令等
  - Something the user possesses（拥有）
    - 身份证、护照、密钥盘等
  - Something the user is (or How he behaves)
    - 指纹、笔迹、声音、虹膜、DNA等

- 协议
  - PAP
  - CHAP
  - Kerberos
  - X.509

鉴别协议

- 双方鉴别(mutual authentication)
- 单向鉴别(one-way authentication)

实体鉴别分类（1）

- 实体鉴别可以分为本地和远程两类。
  - 实体在本地环境的初始化鉴别（就是说，作为实体个人，和设备物理接触，不和网络中的其他设备通信）。
  - 连接远程设备、实体和环境的实体鉴别。
- 本地鉴别：需要用户的进行明确的操作
  远程鉴别：通常将本地鉴别结果传送到远程。
  （1）安全
  （2）易用

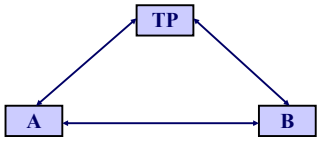
实体鉴别分类（2）

- 实体鉴别可以是单向的也可以是双向的。
  - 单向鉴别是指通信双方中只有一方向另一方进行鉴别。
  - 双向鉴别是指通信双方相互进行鉴别。

实体鉴别系统的组成

- 一方是出示证件的人，称作示证者P(Prover)，又称声称者(Claimant)。
- 另一方为验证者V（Verifier),检验声称者提出的证件的正确性和合法性，决定是否满足要求。
- 第三方是可信赖者TP（Trusted third party)，参与调解纠纷。
- 第四方是攻击者，可以窃听或伪装声称者骗取验证者的信任。

鉴别模型



实体鉴别与消息鉴别的差别

- 实体鉴别一般都是实时的，消息鉴别一般不提供时间性。
- 实体鉴别只证实实体的身份，消息鉴别除了消息的合法和完整外，还需要知道消息的含义。
- 数字签字是实现身份识别的有效途径。但在身份识别中消息的语义是基本固定的，一般不是“终生”的，签字是长期有效的。

对身份鉴别系统的要求

（1）验证者正确识别合法申请者的概率极大化。
（2）不具有可传递性（Transferability)
（3）攻击者伪装成申请者欺骗验证者成功的概率要小到可以忽略的程度
（4）计算有效性
（5）通信有效性
（6）秘密参数能安全存储
*（7）交互识别
*（8）第三方的实时参与
*（9）第三方的可信赖性
*（10）可证明的安全性

实现身份鉴别的途径

- 三种途径之一或他们的组合

（1）所知（Knowledge）:密码、口令
（2）所有（Possesses):身份证、护照、信用卡、钥匙
（3）个人特征：指纹、笔迹、声纹、手型、血型、视网膜、虹膜、DNA以及个人动作方面的一些特征
（4）你做的事情（如手写签名）

设计依据：
安全水平、系统通过率、用户可接受性、成本等

讨论议题

- 鉴别的基本概念
- 鉴别机制
- 鉴别与交换协议
- 典型鉴别实例

鉴别机制

- 非密码的鉴别机制
- 基于密码算法的鉴别
  - 采用对称密码算法的机制
  - 采用公开密码算法的机制
  - 采用密码校验函数的机制
- 零知识证明协议

非密码的鉴别机制

- A. 口令机制
  B. 一次性口令机制
  C. 基于地址的机制
  D. 基于个人特征的机制
  E. 个人鉴别令牌

A. 口令机制

- 口令或通行字机制是最广泛研究和使用的身份鉴别法。通常为长度为6~8的字符串。选择原则：易记、难猜、抗分析能力强。

- 口令系统有许多脆弱点：
  外部泄露
  口令猜测
  线路窃听
  危及验证者
  重放

对付外部泄露的措施

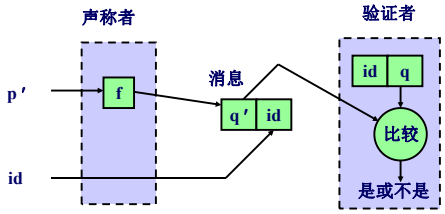
- 教育、培训；
- 严格组织管理办法和执行手续；
- 口令定期改变；
- 每个口令只与一个人有关；
- 输入的口令不再现在终端上；
- 使用易记的口令，不要写在纸上。

对付口令猜测的措施

- 教育、培训；
- 严格限制非法登录的次数；
- 口令验证中插入实时延迟；
- 限制最小长度，至少6~8字节以上
- 防止用户特征相关口令，
- 口令定期改变；
- 及时更改预设口令；
- 使用机器产生的口令。

对付线路窃听的措施

- 使用保护口令机制：如单向函数。



主要缺陷及对策

- 攻击者很容易构造一张q_i与p_i对应的表，表中的p_i尽最大可能包含所期望的值。
- 随机串（Salt）是使这种攻击变得困难的一种办法。
- 在口令后使用随机数。
- 只能保护在多台计算机上使用相同口令或在同一计算机上使用同一口令的不同用户。

B．一次性口令机制

- 一次性口令机制确保在每次认证中所使用的口令不同，以对付重放攻击。
- 确定口令的方法：
  （1）两端共同拥有一串随机口令，在该串的某一位置保持同步；
  （2）两端共同使用一个随机序列生成器，在该序列生成器的初态保持同步；
  （3）使用时戳，两端维持同步的时钟。

强度

（1）没有器件而知道口令p_i，不能导致一个简单的攻击；
（2）拥有器件而不知道口令p_i，不能导致一个简单的攻击；
（3）除非攻击者也能进行时间同步，否则重放不是一个简单的攻击；
（4）知道q_i（例如通过浏览验证者系统文件）而不知道设备安全值I_{SV}，不能导致一个简单的攻击。

SKEY验证程序

- 其安全性依赖于一个单向函数。为建立这样的系统输入一随机数R，计算机计算f（R）, f（f（R））， f（f（f（R））），…共计算100次，计算得到的数为x_1, x_2, x_3 …. x_{100}，A打印出这样的表，随身携带，计算机将x_{101}存在A的名字旁边。
- 第一次登录，键入x_{100},
- 以后依次键入x_i，计算机计算f(x_i)，并将它与x_{i+1}比较。

C、基于地址的机制

- 基于地址的机制假定声称者的可鉴别性是以呼叫的源地址为基础的。
- 在大多数的数据网络中，呼叫地址的辨别都是可行的。
- 在不能可靠地辨别地址时，可以用一个呼叫–回应设备来获得呼叫的源地址。
- 一个验证者对每一个主体都保持一份合法呼叫地址的文件。
- 这种机制最大的困难是在一个临时的环境里维持一个连续的主机和网络地址的联系。地址的转换频繁、呼叫—转发或重定向引起了一些主要问题。
- 基于地址的机制自身不能被作为鉴别机制，但可作为其它机制的有用补充。

D．基于个人特征的机制

- 生物特征识别技术主要有：
  1）指纹识别；
  2）声音识别；
  3）手迹识别；
  4）视网膜扫描；
  5）手形。

这些技术的使用对网络安全协议不会有重要的影响。

E．个人鉴别令牌

- 物理特性用于支持认证“某人拥有某东西”，但通常要与一个口令或PIN结合使用。
- 这种器件应具有存储功能，通常有键盘、显示器等界面部件，更复杂的能支持一次性口令，甚至可嵌入处理器和自己的网络通信设备（如智能卡）。
- 这种器件通常还利用其它密码鉴别方法。

设计鉴别协议

- 介绍在设计认证协议时特别需要注意的问题，并给出抵抗这些攻击的具体设计策略。
- 鉴别和密钥交换协议的核心问题有两个：
  – 保密性
  – 时效性
- 为了防止伪装和防止暴露会话密钥，基本鉴别与会话密码信息必须以保密形式通信。这就要求预先存在保密或公开密钥供实现加密使用。
- 第二个问题也很重要，因为涉及防止消息重放攻击。

A、重放

常见的消息重放攻击形式有：

1、简单重放：攻击者简单复制一条消息，以后在重新发送它；

2、可被日志记录的复制品：攻击者可以在一个合法有效的时间窗内重放一个带时间戳的消息；

3、不能被检测到的复制品：这种情况可能出现，原因是原始信息已经被拦截，无法到达目的地，而只有重放的信息到达目的地。

4、反向重放，不做修改。向消息发送者重放。当采用传统对称加密方式时，这种攻击是可能的。因为消息发送者不能简单地识别发送的消息和收到的消息在内容上的区别。

1）针对同一验证者的重放：非重复值

2）针对不同验证者的重放：验证者的标识符

B．非重复值的使用

- 非重复值的使用：
  1）序列号：计数的策略：对付重放攻击的一种方法是在认证交换中使用一个序数来给每一个消息报文编号。仅当收到的消息序数顺序合法时才接受之。但这种方法的困难是要求双方必须保持上次消息的序号。

  2）时间戳：A接受一个新消息仅当该消息包含一个时间戳，该时间戳在A看来，是足够接近A所知道的当前时间；这种方法要求不同参与者之间的时钟需要同步

  3）验证者发送随机值（如询问）：不可预测、不重复

时间戳

- 在网络环境中，特别是在分布式网络环境中，时钟同步并不容易做到
- 一旦时钟同步失败
  - 要么协议不能正常服务，影响可用性(availability)，造成拒绝服务(DOS)
  - 要么放大时钟窗口，造成攻击的机会
- 时间窗大小的选择应根据消息的时效性来确定

询问/应答方式 (Challenge/Response)

- A期望从B获得一个消息
  - 首先发给B一个随机值(challenge)
  - B收到这个值之后，对它作某种变换，并送回去
  - A收到B的response，希望包含这个随机值
- 在有的协议中，这个challenge也称为nonce
  - 可能明文传输，也可能密文传输
  - 这个条件可以是知道某个口令，也可能是其他的事情
  - 变换例子：用密钥加密，说明B知道这个密钥；简单运算，比如增一，说明B知道这个随机值
- 询问/应答方法不适应非连接性的应用，因为它要求在传输开始之前先有握手的额外开销，这就抵消了无连接通信的主要特点。

C、相互鉴别协议

- 在理论上，相互鉴别可通过组合两个单向鉴别交换协议来实现。然而，这种组合需要被仔细地考察，因为有可能这样的组合易受窃听重放攻击。
- 另外，设计协议消息数比相应的单向交换协议的消息数的两倍少得多的相互鉴别交换协议是可能的。
- 因此，由于安全性和性能的原因，相互鉴别交换协议必须为此目的而特别地进行设计。

采用对称密码的鉴别机制

- 无可信第三方参与的鉴别
  - 单向鉴别：使用该机制时，两实体中只有一方被鉴别。
  - 双向鉴别：两通信实体使用此机制进行相互鉴别。
- 有可信第三方参与的鉴别

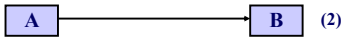
本部分使用以下记法

- A:实体A的可区分标识符
- B:实体B的可区分标识符
- TP:可信第三方的可区分标识符
- K_{XY}:实体X和实体Y之间共享的秘密密钥只用于对称密码技术
- S_X:与实体X有关的私有签名密钥只用于非对称加密技术
- N_X:由实体X给出的顺序号
- R_X:由实体X给出的随机数
- T_X:由实体X原发的时变参数,它或者是时间标记T_X或者是顺序号R_X N_X:
- Y||Z:数据项Y和Z以Y在前Z在后顺序拼接的结果
- eK(Z):用密钥K的对称加密算法对数据Z加密的结果
- fK(Z):使用以密钥K和任意数据串Z作为输入的密码校验函数所产生的密码校验值
- CertX:由可信第三方签发给实体X的证书
- TokenXY:实体X发给Y的权标,包含使用密码技术变换的信息
- TVP:时变参数
- $_SS_X(Z)$:用私有签名密钥S_X对数据Z进行私有签名变换所产生的签名

无可信第三方参与的机制 单向鉴别

- 一次传送鉴别

（1）TokenAB



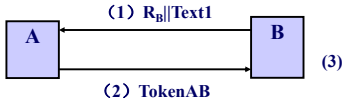
（1）TokenAB=Text2||eK_{AB}(T_A||B||Text1)

N_A

（2）B解密，验证B、时间标记或顺序号的正确性

无可信第三方参与的机制 单向鉴别

- 两次传送鉴别

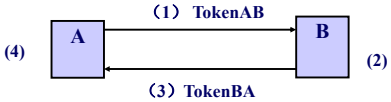


（2）TokenAB=Text3||eK_{AB}(R_B||B||Text2)

（3）B解密，验证B、 R_B的正确性

无可信第三方参与的机制 双向鉴别

- 两次传送鉴别



（1）TokenAB=Text2||eK_{AB}(T_A||B||Text1)

N_A

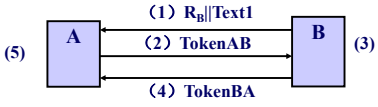
（3）TokenBA=Text4||eK_{AB}(T_B||A||Text3)

N_B

（4）B解密，验证B、 R_B的正确性

无可信第三方参与的机制 双向鉴别

- 三次传送鉴别



（2）TokenAB=Text3||eK_{AB}(R_A ||R_B||B||Text2)

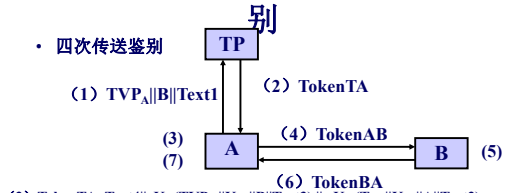
（3）B解密，验证B、 R_B的正确性

（4）TokenBA=Text5||eK_{AB}(R_B ||R_A||Text4)

（5）A解密，验证B、 R_B、 R_A的正确性

涉及可信第三方的机制-双向鉴别

- 四次传送鉴别



（2）TokenTA=Text4||eK_{AT}(TVP_A ||K_{AB}||B||Text3) || eK_{BT}(T_{TP} ||K_{AB}||A||Text2)

N_{TP}

（4）TokenAB=Text6|| eK_{BT}(T_{TP} ||K_{AB}||A||Text2) eK_{AB}(T_A ||B||Text5)

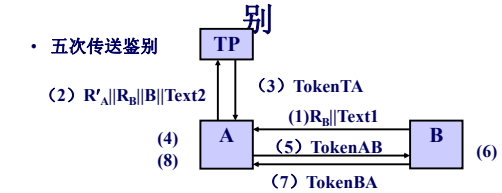
N_{TP} N_A

（6）TokenBA=Text8|| eK_{AB}(T_B ||A||Text7)

N_B

涉及可信第三方的机制-双向鉴别

- 五次传送鉴别



（3）TokenTA=Text5||eK_{AT}(R′$_A$ ||K_{AB}||B||Text4) || eK_{BT}(R_B || K_{AB}|| A||Text3)

（5）TokenAB=Text7|| eK_{BT}(R_B || K_{AB}|| A||Text3) ||eK_{AB}(R_A ||R_B||Text6)

（7）TokenBA=Text9|| eK_{AB}(R_B ||R_A||Text8)

采用公开密码算法的机制

- 在该机制中，声称者要通过证明他知道某秘密签名密钥来证实身份。由使用他的秘密签名密钥签署某一消息来完成。消息可包含一个非重复值以抵抗重放攻击。
- 要求验证者有声称者的有效公钥
  声称者有仅由自己知道和使用的秘密签名私钥。
- 单向鉴别：仅对实体中的一个进行鉴别。
  双向鉴别：两个通信实体相互进行鉴别。

采用公开密码算法的机制—单向鉴别

- 一次传递机制

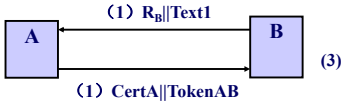
（1）$Token_{AB}=T_A||B||Text2||_{\&}S_A(T_A||B||Text1)$

N_A N_A

(2)B验证A的公开密钥，验证B的标识符号

采用公开密码算法的机制—单向鉴别

- 两次传递机制

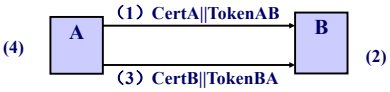


（2）$Token_{AB}=R_A||R_B||B||Text3||_{\&}S_A(R_A||R_B||B||Text2)$

（3）B验证A的公开密钥，验证B的标识符号

采用公开密码算法的机制—双向鉴别（1）

- 两次传递机制



（1）$Token_{AB}=T_A||B||Text2||_{\&}S_A(T_A||B||Text1)$

N_A N_A

（2）B验证A的公开密钥，验证B的标识符号

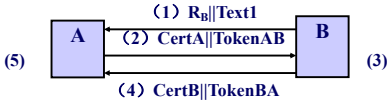
（3）$Token_{BA}=T_B||A||Text4||_{\&}S_B(T_B||A||Text3)$

N_B N_B

（4）A验证B的公开密钥，验证A的标识符号

采用公开密码算法的机制—双向鉴别（2）

- 三次传递机制



（2）$Token_{AB}=R_A||R_B||B||Text3||_{\&}S_A(R_A||R_B||B||Text2)$

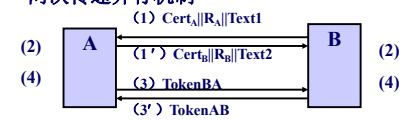
（3）B验证A的公开密钥，验证B的标识符号

（4）$Token_{BA}=R_B||R_A||A||Text5||_{\&}S_B(R_B||R_A||A||Text4)$

（5）A验证B的公开密钥，验证A的标识符号

采用公开密码算法的机制—双向鉴别（3）

- 两次传递并行机制



（1）$Token_{AB}=R_A||R_B||B||Text4||_{\&}S_A(R_A||R_B||B||Text3)$

（1′）$Token_{BA}=R_B||R_A||A||Text6||_{\&}S_B(R_B||R_A||A||Text5)$

（2）A和B确保他们拥有另一实体的公开密钥

（4）A和B验证各自的随机数

采用密码校验函数的机制

- 在该机制中，待鉴别的实体通过表明它拥有某个秘密鉴别密钥来证实其身份。可由该实体以其秘密密钥和特定数据作输入，使用密码校验函数获得密码校验值来达到。
- 声称者和验证者共享秘密鉴别密钥，应仅为该两个实体所知，以及他们的信任方。

采用密码校验函数的机制 单向鉴别

- 一次传递鉴别

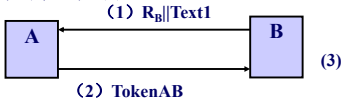
（1）TokenAB=T_A||Text2||fK_{AB}(T_A||B||Text1)

N_A N_A

(2)B验证A的标识符号和时间标记

采用密码校验函数的机制 单向鉴别

- 两次传递机制

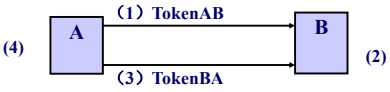


（2）TokenAB=Text3||fK_{AB}(R_B||B||Text2)

（3）B验证B的标识符号和随机数

采用密码校验函数的机制 双向鉴别（1）

- 两次传递机制



（1）TokenAB=T_A||B||Text2||fK_{AB}(T_A||B||Text1)

N_A N_A

（2）B验证A的标识符号和时间标记

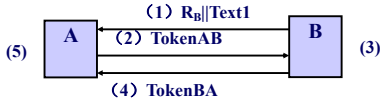
（3）TokenBA=T_B||A||Text4||$_KS_B$(T_B||A||Text3)

N_B N_B

（4）A验证B的标识符号和时间标记

采用密码校验函数的机制 双向鉴别（2）

- 三次传递机制



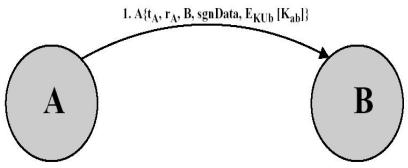
（2）TokenAB=R_A||Text3||fK_{AB}(R_A||R_B||B||Text2)

（3）B验证B的标识符号和随机数

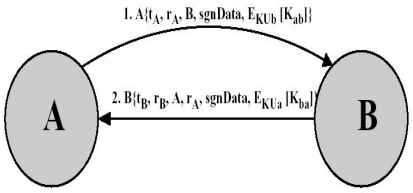
（4）TokenBA=Text5|| fK_{AB}(R_B||R_A||Text2)

（5）A验证A的标识符号和随机数

鉴别过程:单向鉴别



鉴别过程:双向鉴别



鉴别过程:三向鉴别