§5.5 身份认证

身份认证又称作识别(Identification)、实体认证(Entity Authentication)、身份证实(Identity Verification)等。它与消息认证的区别：身份认证一般都是实时的，而消息认证本身不提供时间性；另一方面，身份认证通常证实身份本身，而消息认证除了认证消息的合法性和完整性外，还要知道消息的含义。

在一个竞争和斗争的现实社会，身份欺诈是不可避免的。因此常常需要证明个人的身份。传统的身份认证一般是通过检验“物”的有效性来确认持该物者的身份。“物”可以为徽章、工作证、信用卡、身份证、护照等，卡上含有个人照片，并有权威机构签章。

§5.5 身份认证

随着信息化和网络化业务的发展，这类依靠人工的识别工作已逐步由机器通过数字化方式来实现。在信息化社会中，随着信息业务的扩大，要求验证的对象集合也迅速加大，大大增加了身份认证的复杂性和实现的困难性。

通常，身份认证是通过三种基本方式或其组合方式来完成：

（1）用户所知道的某个秘密信息，如用户口令。

（2）用户所持有的某个秘密信息（硬件），即用户必须持有合法的随身携带的物理介质，如磁卡、智能卡或用户所申请领取的公钥证书。

（3）用户所具有的某些生物特征，如指纹，声音，DNA图案，视网膜扫描等。

§5.5 身份认证

口令认证：

最简单、最普遍的身份识别技术，如各类系统的登录等。口令具有共享秘密的属性，口令有时由用户选择，有时由系统分配。通常情况下，用户先输入某种标志信息，比如用户名和ID号，然后系统询问用户口令，若口令与用户文件中的相匹配，用户即可进入访问。口令有多种，如一次性口令；还有基于时间的口令。

§5.5 身份认证

这种方法的缺点是：

（1）其安全性仅仅基于用户口令的保密性，而用户口令一般较短且容易猜测，因此这种方案不能抵御口令猜测攻击。

（2）大多数系统的口令是明文传送到验证服务器的，容易被截获。

（3）口令维护的成本较高。为保证安全性，口令应当经常更换。另外为避免对口令的字典攻击，口令应当保证一定的长度，并且尽量采用随机的字符。但缺点是难于记忆。

（4）口令容易在输入的时候被攻击者偷窥，而且用户无法及时发现。

§5.5 身份认证

数字证书：

这是一种检验用户身份的电子文件，也是企业现在可以使用的一种工具。这种证书可以授权购买，提供更强的访问控制，并具有很高的安全性和可靠性。

非对称体制身份识别的关键是将用户身份与密钥绑定。CA(Certificate Authority)通过为用户发放数字证书来证明用户公钥与用户身份的对应关系。验证者向用户提供一随机数；用户以其私钥SK对随机数进行签名，将签名和自己的证书提交给验证方；验证者验证证书的有效性，从证书中获得用户公钥PK，以PK验证用户签名的随机数。

§5.5 身份认证

智能卡：

网络通过用户拥有什么东西来识别的方法，一般是用智能卡或其它特殊形式的标志，这类标志可以从连接到计算机上的读取器读出来。访问不但需要口令，也需要使用物理智能卡。

智能卡技术将成为用户接入和用户身份认证等安全要求的首选技术。用户将从持有认证执照的可信发行者手里取得智能卡安全设备，也可从其他公共密钥密码安全方案发行者那里获得。这样智能卡的读取器必将成为用户接入和认证安全解决方案的一个关键部分。

§5.5 身份认证

主体特征认证：

目前已有的设备包括：视网膜扫描仪、声音验证设备、手型识别器等。安全性高。

例如：系统中存储了他的指纹，他接入网络时，就必须在连接到网络的电子指纹机上提供他的指纹（这就防止他以假的指纹或其它电子信息欺骗系统），只有指纹相符才允许他访问系统。

更普通的是通过视网膜膜血管分布图来识别，原理与指纹识别相同，声波纹识别也是商业系统采用的一种识别方式。

§5.5 身份认证

身份欺诈事例：

1、象棋大师问题

2、黑手党骗局

3、恐怖分子问题

§5.5 身份认证

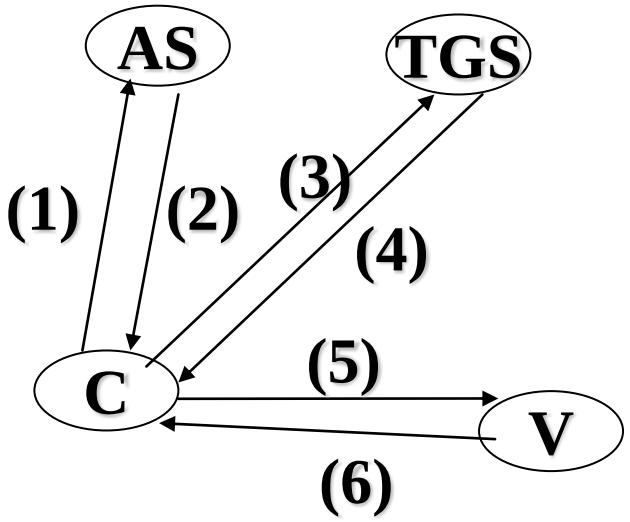
身份认证—Kerberos认证系统

Kerberos：希腊神话“三个头的狗——地狱之门守护者”希望有三个功能：身份认证、记账、审核。

Kerberos针对分布式环境，一些工作站可能安装于不安全场所，而且用户也并非是完全可信的。

Kerberos是网络通信提供可信第三方服务的面向开放系统的认证机制。

§5.5 身份认证



C(客户机)/AS(认证服务器)/V(服务器)

$ID_c/ID_v/ID_{tgs}$分别为C/V/TGS的身份

AD_c： 用户的网络地址

TS_i：第i个时戳

$Lifetime_i$： 第i个有效期限

P_c：C上的用户口令

K_c：C和AS的共享密钥

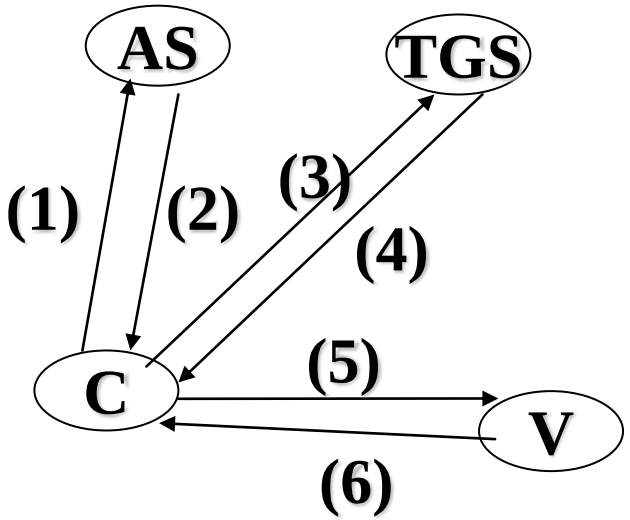
K_v：V和TGS的共享密钥

K_{tgs}： TGS 和AS的共享密钥

$K_{c,tgs}$：C与TGS的共享密钥

$K_{c,v}$：C与V的共享密钥

§5.5 身份认证

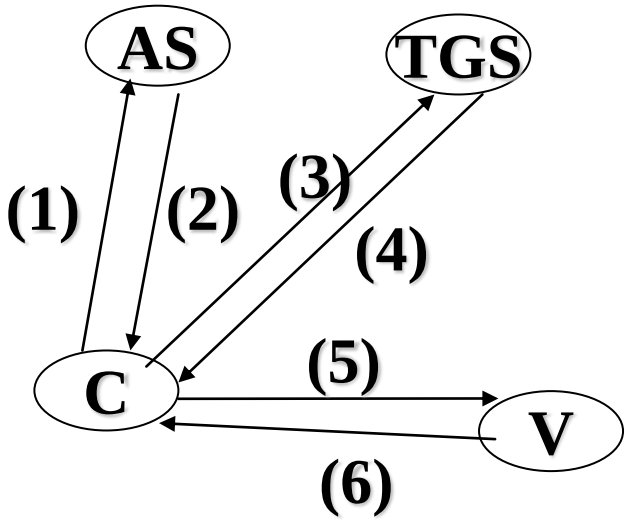


(1) C→AS： $ID_C||ID_{tgs}||TS_1$

(2) AS→C： $E_{Kc}[K_{c,\ tgs}||ID_{tgs}||TS_2||Lifetime_2||Ticket_{tgs}]$

$Ticket_{tgs} = E_{Ktgs}[K_{c,tgs}||ID_c||AD_c||\ ID_{tgs}\ ||TS_2||Lifetime_2]$

§5.5 身份认证



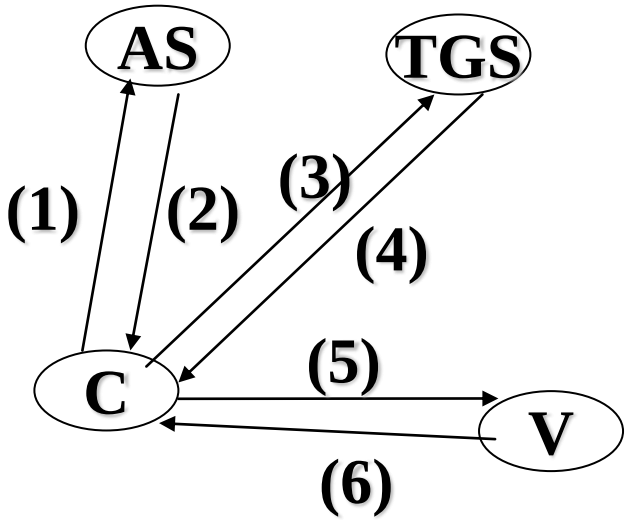
(3) C→TGS： $ID_v||Ticket_{tgs}||Authenticator_c$

$Authenticator_c=E_{Kc,\ tgs}[ID_c||AD_c||TS_3]$

(4) TGS →C： $E_{Kc,\ tgs}[K_{c,\ v}||ID_v||TS_4||Ticket_v]$

$Ticket_v=E_{Kv}[K_{c,\ v}||ID_c||AD_c||ID_v||TS_4||Lifetime_4]$

§5.5 身份认证



(5) C→V： $Ticket_v||Authenticator_c$

$Ticket_v = E_{K_v}[K_{c,v}||ID_c||AD_c||ID_v||TS_4||Lifetime_4]$

$Authenticator_c = E_{k_{c,v}}[ID_c||AD_c||TS_5]$

(6) V →C： $E_{k_{c,v}}[TS_5+1]$

§5.5 身份认证

Kerberos的局限性：

1．时间同步问题：

因为整个Kerberos的协议都严重地依赖于时钟，而实际证明，要求在分步式系统环境中实现良好的时钟同步，是一个很难的课题。

2．口令猜测问题：

Kerberos的口令没有进行额外的特殊处理，以至于即使用强力攻击（即穷举法）的时间复杂度仅和口令的长度成比例，这将形成一个两难的局面：或是增加密钥长度换取更高的安全，但这会造成用户的使用困难和增加系统加/解密开销。

§5.5 身份认证

3．认证域之间的信任问题：

认证域之间的多级跳跃过程复杂且不明确，相互信任和协调不方便。若各Kerberos区域形成复杂或不规则的网状结构，则要求方便的域间服务，将付出极大的代价，即系统的可扩充性不强。针对这种无序的状况，应有规划有目的地建立起全球一体化的分层（树状）结构，形成良好的信任链条。

§5.5 身份认证

4．重放攻击的问题：

长票的生存期较长，容易被重放攻击；对短票而言，如果攻击者技术高明，也有机会重放攻击，况且攻击者可以着手破坏系统的时钟同步性。我们建议，在Kerberos引入序列号循环机制，即让传送的消息带上一定的序列号，这些序列号在由系统循环地赋予消息，再结合系统原有的生存期控制，将有效地保证一定的时间段里只能存在唯一的合法消息，从而消除了重放的可能性。当然，这必须付出一定的系统开销代价。

§5.5 身份认证

5．密钥的存储问题：

Kerberos认证中心要求保存大量的共享私钥，无论是管理还是更新都有很大的困难，需要特别细致的安全保护措施（甚至应采用硬件/物理方法），将付出极大的系统代价。

6．系统程序的安全性、完整性问题：

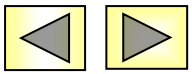
对Kerberos系统程序进行攻击，特别是恶意篡改登录程序，是有效的攻击方法。所以，必须花一定的系统代价去防范对认证系统本身的集中攻击。其中，建立高性能的防火墙和进行日志是必要的。

§5.5 身份认证

身份认证—X.509认证业务

公钥证书（数字证书）：由一个第三方证书授权中心(CA)发行的，经CA数字签名的包含用户的公钥和与用户身份相关的信息，是实体在网上信息交流及商务交易活动中的身份证明，具有唯一性。在基于证书的安全通信中，数字证书是证明用户合法身份和提供用户合法公钥的凭证，是建立保密通信的基础。

通常使用的是符合X.509的数字证书。它包含以下一些内容：证书的版本信息；证书的序列号，每个证书都有一个唯一的证书序列号；证书所使用的签名算法；证书的发行机构名称；证书的有效期；证书所有者的名称；证书所有者的公开密钥；证书发行者对证书的签名。



§5.5 身份认证

X.509认证过程：

假设通信双方都知道对方的公钥，或者双方都从目录服务器获得对方的公钥证书。

认证过程有三种：

（1）单向身份认证

用户A将消息发往B，向B证明：

a) A的身份，消息是由A产生的

b) 消息的意欲接收者是B

c) 消息的完整性和新鲜性

§5.5 身份认证



说明：ID_A、ID_B：A和B的身份标识

E_{SA}：用A的私钥加密　　E_{PB}：用B的公钥加密

T_A：A产生消息的时戳，包括产生时间、截止时间

R_A：A产生的不会重复的随机数，防止重放、伪造，B在收到的消息截止时间内要一直保存R_A

K_{AB}：双方欲建立的会话密钥

B需要验证：A的证书的有效性；A的签名；消息完整性；接收者是否为B；时戳是否是当前时间；R_A有无重复

§5.5 身份认证

（2）双向身份认证



在单向认证基础上，B向A做出应答，以证明：

a) B的身份、应答是B产生的

b) 应答的意欲接收者是A

c) 应答消息是完整的和新鲜的

应答消息包含由A发来的一次性随机数R_A，以使应答消息有效。 T_B 、R_B是B的时戳和随机数，K_{BA}：双方的会话密钥

§5.5 身份认证

（3）三向身份认证



在双向认证基础上，A再向B做出应答，构成三向身份认证。

三向身份认证的目的是将收到的对方发来的一次性随机数又返回给对方，因此双方不需要检查时戳只要检查对方的一次性随机数即可判断出重放攻击。在通信双方无法建立时钟同步时，就要用此方法。