1.在网络或 internet 上，和用户认证关联的三个威胁

1.用户可以获得对特定工作站的访问，并假装是从该工作站操作的另一用户。2.用户可以改变工作站的网络地址，使得从改变的工作站发送的请求看起来来自模拟的工作站。3.用户可能会窃听交易所并使用重放攻击来进入服务器或扰乱操作。

2.消息认证和用户认证的区别和联系

区别：

1、性质不同

身份认证指通过一定的手段，完成对用户身份的确认。

消息认证（message authentication）指验证消息的完整性，当接收方收到发送方的报文时，接收方能够验证收到的报文是真实的和未被篡改的。它包含两层含义：验证信息的发送者是真正的而不是冒充的，即数据起源认证；验证信息在传送过程中未被篡改、重放或延迟等。

2、目的不同

身份验证的目的为确认当前所声称为某种身份的用户，确实是所声称的用户。在日常生活中，身份验证并不罕见；比如，通过检查对方的证件，我们一般可以确信对方的身份。虽然日常生活中的这种确认对方身份的做法也属于广义的“身份验证”，但“身份验证”一词更多地被用在计算机、通信等领域。

消息认证目的为了防止传输和存储的消息被有意无意的篡改。

3.

15.10 In Kerberos, when Bob receives a Ticket from Alice, how does he know it is genuine?
15.11 In Kerberos, when Bob receives a Ticket from Alice, how does he know it came from Alice?

如何知道受到的票据是真实的？

如何知道票据来自 alice？

15.10 It contains the Alice's ID, Bob's name, and timestamp encrypted by the KDC-Bob secret key.

15.11 It contains Alice's name encrypted by the KDC-Bob secret key.

- 包括 alice 的 id，bob 的名字和由 KDC Bob 密钥加密的时间戳
- 它包含由 KDC Bob 密钥加密的 Alice 的名字。

4.消息认证码和数字签名的区别

Mac 跟数字签名也有很多区别和联系的。

Mac 跟数字签名也有类似的地方，因为都可以确认发出人身份，同时判断文件有无被篡改。

但是区别也是明显的，因为生成 Mac 和验证 Mac 需要的密钥是同一个，属于对称加密的范畴。而数字签名属于非对称加密，生成签名用私钥，而验证签名是否有效要用公钥。Mac 的工作方式决定了，发送方和接收方要事先共享同一个密钥，这也是对称加密算法的共性。数字签名的接收方是不能再生成签名的，也就是说不可伪造。但是 Mac 的接收方因为手里也有密钥，所以可以对其他信息生成 Mac 。