

1. 什么是网络安全

1.1 什么是网络安全

私密性/机密性:

只有发送方和预订的接收方能理解传输的报文内容

发送方加密报文

接收方解密报文

可认证性:

发送方和接收方需要确认对方身份

报文完整性:

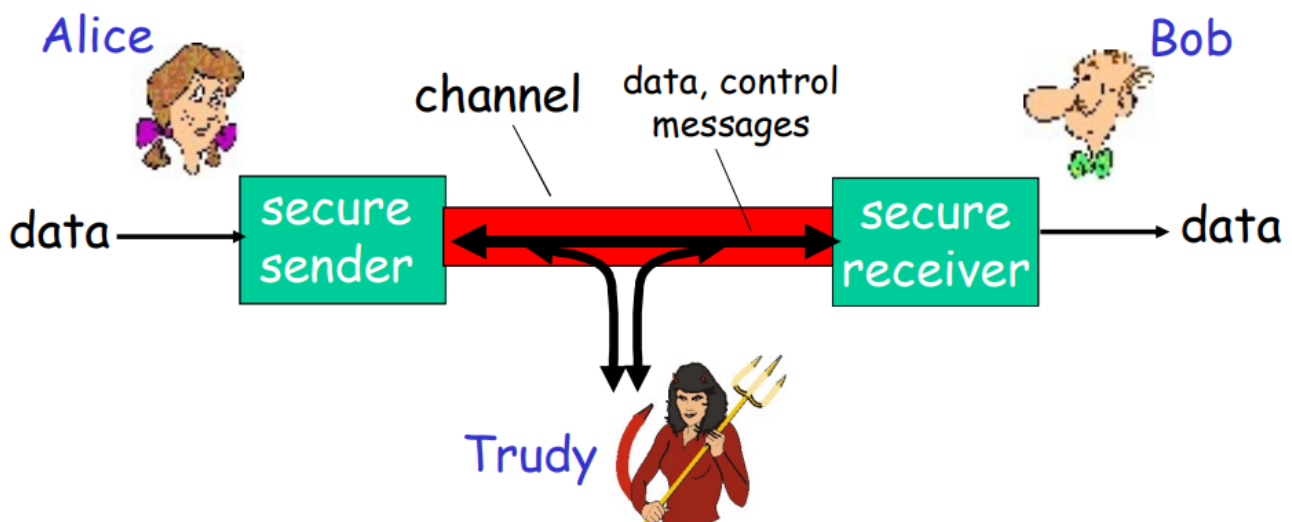
发送方、接收方需要确认报文在传输的过程中或事后没有被改变

访问控制和服务的可用性:

服务可以接入以及对用户而言是有用的

朋友和敌人: Alice, Bob, Trudy

- 网络安全世界比较著名的模型
- Bob, Alice (lovers!) 需要安全的通信
- Trudy (intruder) 可以截获, 删除和增加报文



网络中的坏蛋:

窃听: 截获报文

插入: 在连接上插入报文

伪装: 可以在分组的源地址写出伪装的地址

劫持: 将发送方或者接收方踢出, 接管连接

拒绝资源: 阻止服务被其他正常用户使用 (e.g., 通过对资源的过载使用)

.....