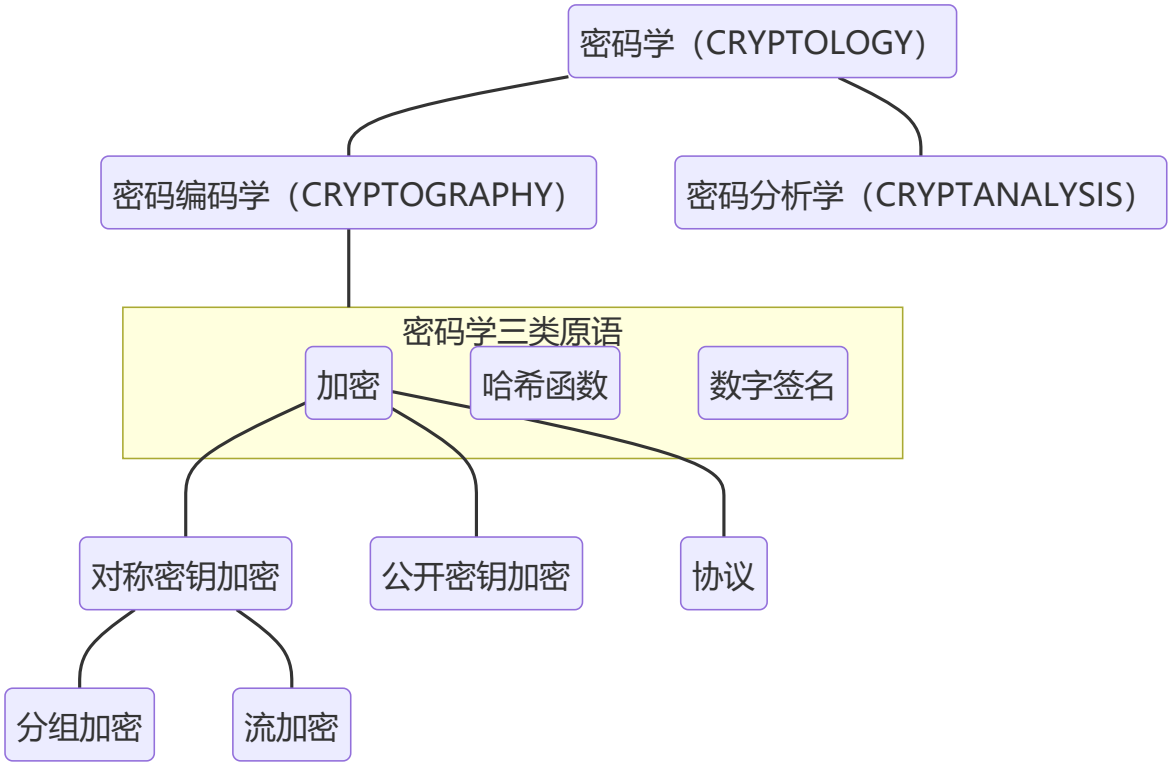


> 教材第一章

OSI 安全架构主要关注安全攻击、安全服务、安全机制。

安全攻击

被动攻击

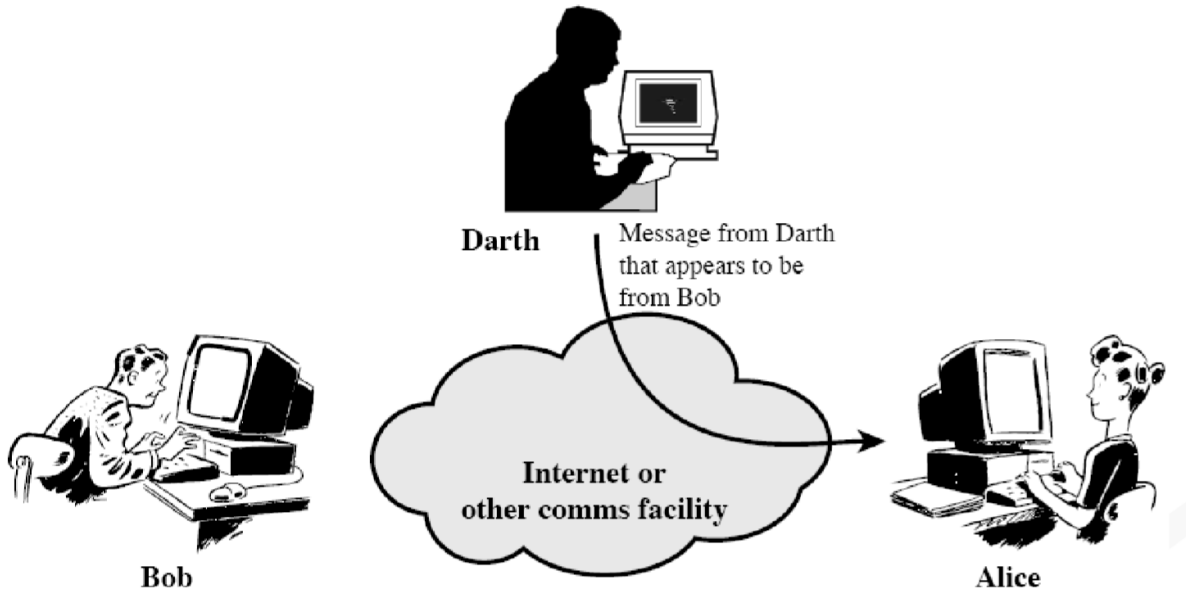
> 对于被动攻击，重点是预防而非检测

- 信息内容泄露
- 流量分析

主动攻击

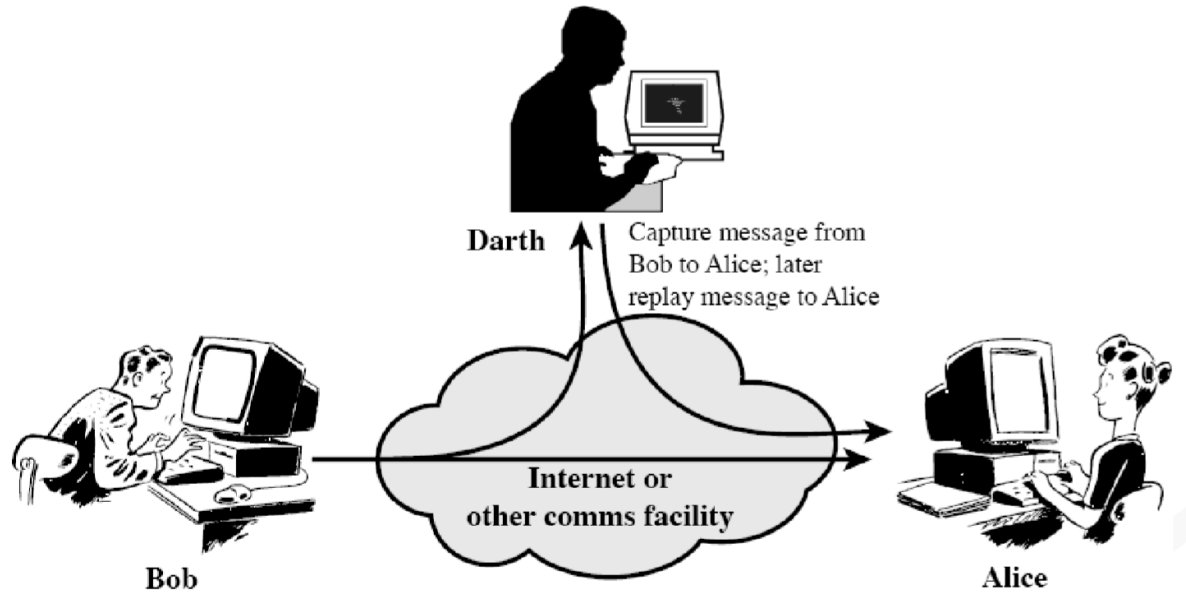
> 主动攻击难以预防，重点在于检测并从攻击造成的破坏或延迟中恢复过来

伪装



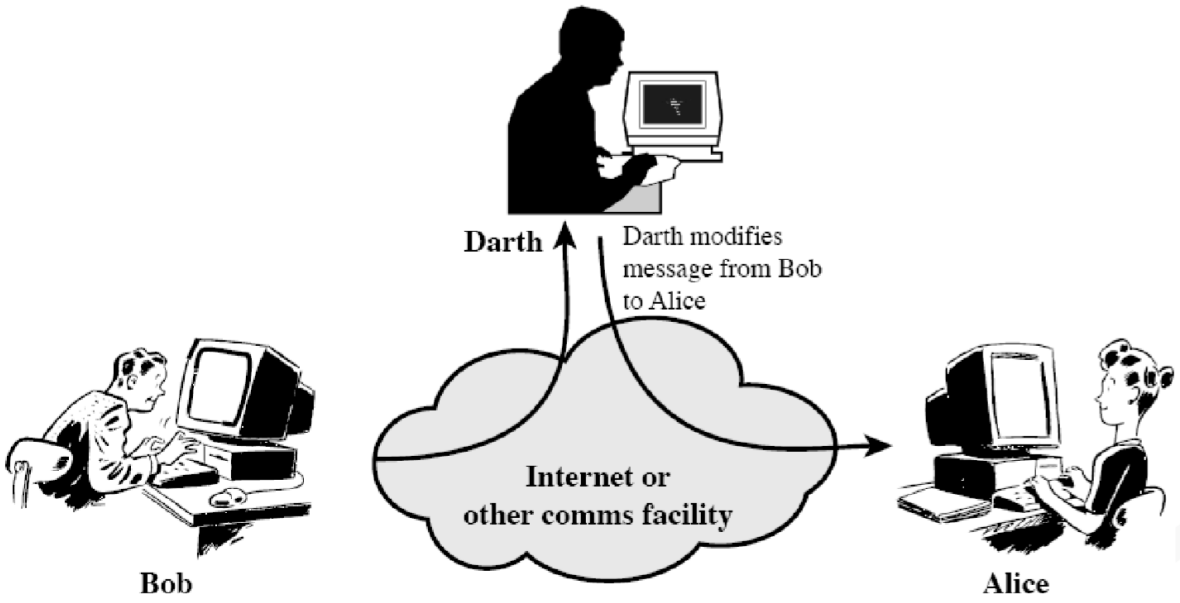
(a) Masquerade (伪装)

重放



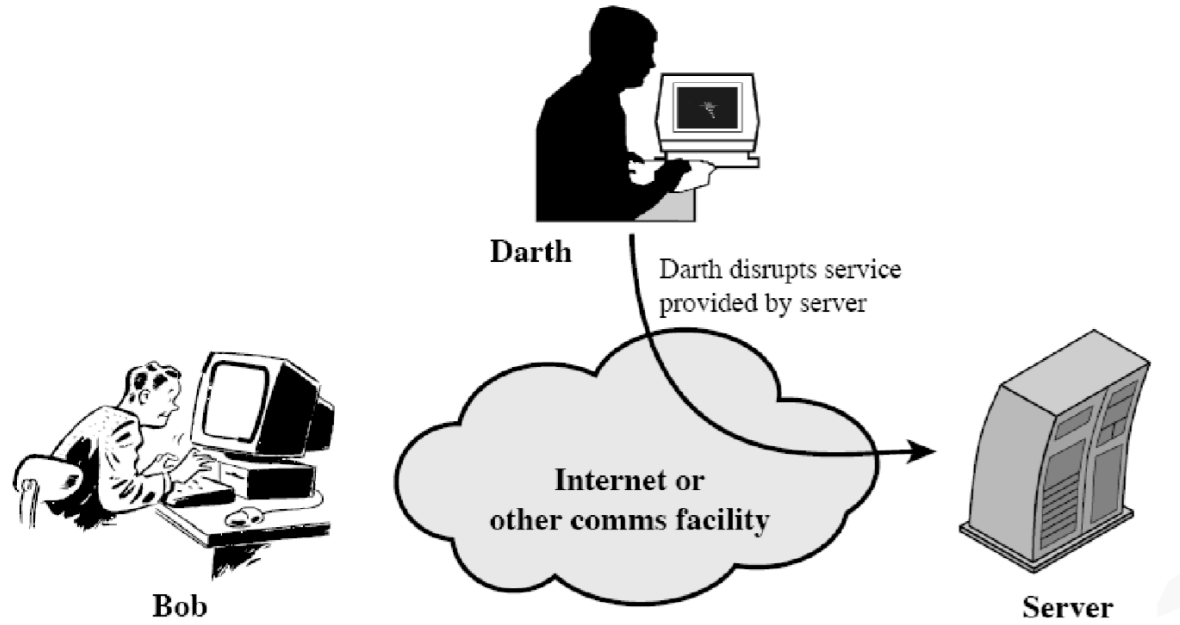
(b) Replay (重放)

信息修改



(c) Modification of messages

拒绝服务



(d) Denial of service(拒绝服务)

安全服务

安全服务通过安全机制来实现其安全策略。X.800 将这些服务分为 5 类共 14 个特定服务（本课对**访问控制**不做要求）：

表 1.2　安全服务

认　证	**数据完整性**
保证通信的实体是它所声称的实体	保证收到的数据的确是授权实体发出的数据（即未修改、插入、删除或重播）
同等实体认证	**具有恢复功能的连接完整性**
用于逻辑连接时为连接的实体的身份提供可信性	提供一次连接中所有用户数据的完整性。检测整个数据序列内存在的修改、插入、删除或重播，且试图恢复之
数据源认证	**无恢复的连接完整性**
在无连接传输时保证收到的信息来源是声称的来源	同上，但仅提供检测，无恢复
访问控制	**选择域连接完整性**
阻止对资源的非授权使用（即这项服务控制谁能访问资源，在什么条件下可以访问，这些访问的资源可用于做什么）	提供一次连接中传输的单个数据块内用户数据的指定部分的完整性，并判断指定部分是否有修改、插入、删除或重播
数据保密性	**无连接完整性**
保护数据免于非授权泄露	为单个无连接数据块提供完整性保护，并检测是否有数据修改。另外，提供有限的重播检测
连接保密性	**选择域无连接完整性**
保护一次连接中所有的用户数据	为单个无连接数据块内指定域提供完整性保护；判断指定域是否被修改
无连接保密性	**不可否认性**
保护单个数据块中的所有用户数据	防止整个或部分通信过程中，任一通信实体进行否认的行为
选择域保密性	**源不可否认性**
对一次连接或单个数据块中指定的数据部分提供保密性	证明消息是由特定方发出的
流量保密性	**宿不可否认性**
保护那些可以通过观察流量而获得的信息	证明消息被特定方收到

安全机制

课程主要关注以下三种安全机制：

- 加密
- 数字签名：附加于数据单元之后的一种数据，它是对数据单元的密码变换，以使得（如接收方）可证明数据源和完整性，并防止伪造
- 数据完整性

表 1.4　安全服务与机制间的联系

	机　制							
服　务	加　密	数字签名	访问控制	数据完整性	认证交换	流量填充	路由控制	公　证
同等实体认证	Y	Y			Y			
数据源认证	Y	Y						
访问控制			Y					
保密性	Y						Y	
流量保密性	Y					Y	Y	
数据完整性	Y	Y		Y				
不可否认性		Y		Y				Y
可用性				Y	Y			

思考题

1.1

> 什么是 OSI 安全架构?

OSI 安全框架是提供安全的一种组织方法，主要关注：安全攻击、安全机制和安全服务。

1.4

> 列出并简要定义安全服务的种类。

认证，访问控制，数据保密性，数据完整性，不可否认性。

1.5

> 列出并简要定义安全机制的种类。

课程主要关注加密，数字签名以及数据完整性三种特定的安全机制。