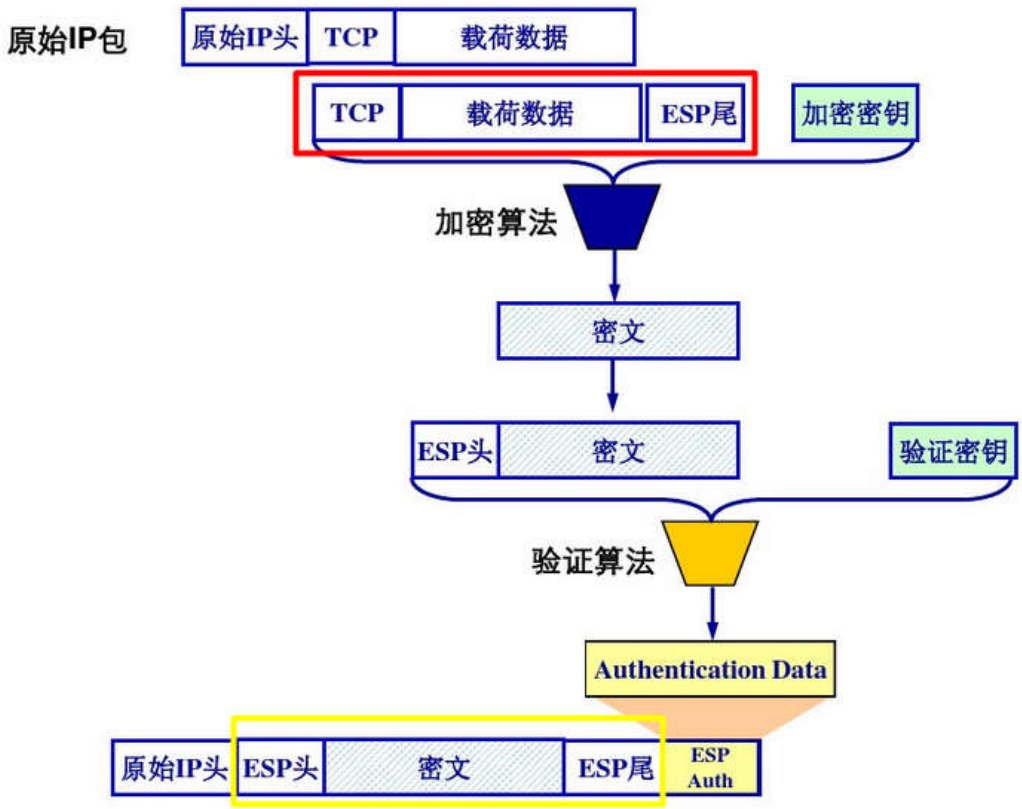
IPSec 传输模式下 ESP 报文的装包与拆包过程

课程名称	信息安全概论	任课老师	蔡国扬
年级	2018级	专业（方向）	软件工程专业
学号	18342069	姓名	罗炜乐
电话	18027303477	Email	luowle@foxmail.com
开始日期	2020.12.20	完成日期	2020.12.20

装包过程

流程图



过程描述

1. 在原IP报文中的TCP报文后添加相应的`ESP trailer`信息。
2. `ESP trailer`包含三部分：`Padding`，`Pad length`和`Next header`。`Padding`是块加密中最后一个数据块长度不足时所做的填充。`Pad length`指刚刚`Padding`填充的长度，方便拆包时找到用来填充的数据段。`Next header`标明被封装的原报文的协议类型(例如 6 = TCP)。
3. 为第2步得到的密文添加`ESP`头。`ESP`头由`SPI (Security Parameter Index)`和`Seq`两部分组成。`SPI`用来查找对应`SA(Security Association)`，`Seq`是对包进行编号，防止多次接收。密文和 ESP头合起来称为`Enchilada`，构成认证部分。
4. 对第3步生成的`Enchilada`认证部分做摘要（`ESP Authentication Data`），得到一个32位整数倍的`ICV(integrity check value)`，附在`Enchilada`之后。`ICV`生成算法和验证密钥由`SA`给出。
5. 将原始的 IP 报文头中的协议号改为50（代表`ESP`），然后将 IP 报文头加到第4步的结果之前构成`IPsec`报文。

拆包过程

过程描述

1. 接收方收到 IP 报文后，发现协议类型是50，标明这是一个`ESP`包。然后查看`ESP`头，找到`SPI`并通过`SPI`决定数据报文所对应的`SA`，获得对应的模式（隧道或传输模式）以及安全规范。
2. 根据`SA`指定的摘要算法和验证密钥计算`Enchilada`的摘要值，与附在 IP 报文最后的`ESP Authentication Data`进行对比，二者相同则数据完整性未被破坏。
3. 查看`ESP header`中的`Seq`，确定该包是第一次收到，防止数据回放攻击。
4. 根据`SA`得到的加密信息，解密被加密的信息，得到原数据段以及`ESP trailer`。
5. 根据`ESP trailer`的填充信息，删去填充的数据和`ESP`字段得到原来的`TCP`数据段。
6. 根据 TCP 报文头信息将报文交付给传输层。