信息安全作业 4：描述 IPSec 传输模式下 ESP 报文的装包与拆包过程

IPSec

- IP 协议的安全性

传统的 IP 协议诞生于军用计划，设计之初未考虑太多安全问题，存在很多安全隐患。比如数据明文传输，同在一个集线器的通信可以被互相监听，如果获得交换机权限，所有流经交换机的通信也可以被监听。攻击者即便没有交换机权限，也可以通过中间人攻击窃取用户的通信。

- IPsec（互联网安全协定）提供了网络层加密方案

对 IP 协议进行安全加强的迫切需要催生了 IPsec。IPsec 在网络层将每个 IP 分组的内容先加密再传输，即便中途被截获，攻击者由于缺乏解密数据包所必要的密钥而无法获取其中内容。IPsec 对数据进行加密的方式有两种：传输模式和隧道模式。

- 传输模式只是对 IP 协议报文的有效数据载荷 (payload) 进行了加密，因此需要对原始 IP 报文进行拆装。
- 隧道模式则是对整个 IP 报文进行加密，就好像整个 IP 报文封装在一个安全的隧道里传输一样，保持了原始 IP 报文的完整性。

ESP 协议

ESP（Encapsulating Security Payloads），封装安全载荷协议，IPsec 所支持的两类协议中的一种。该协议能够在数据的传输过程中对数据进行完整性度量，来源认证以及加密，也可防止回放攻击。传输模式，与隧道模式同为 IPsec 工作的两种方式。与隧道模式不同，当 IPsec 工作在传输模式时，新的 IP 头并不会被生成，而是采用原来的 IP 头，保护的也仅仅是真正传输的数据，而不是整个 IP 报文。在处理方法上，原来的 IP 报文会先被解开，再在数据前面加上新的 ESP 或 AH 协议头，最后再装回原来的 IP 头，即原来的 IP 包被修改过再传输。

装包过程

在传输模式下，当要发出一个数据包时：

1. 在原 IP 报文末尾添加尾部信息。

尾部包含三部分：

- 填充数据：由所选加密算法可能是块加密，那么当最后一块长度不够时就需要进行填充；

- 填充长度：并且附上填充长度方便解包时找到填充的数据；
- Next header：则用来标明被加密的数据报文的类型，例如 TCP。

2. 将原 IP 报文以及第 1 步得到的 ESP 尾部作为一个整体进行加密，具体的加密算法与密钥由 SA 给出。
3. 为第 2 步得到的加密数据添加 ESP 头部。ESP 头由两部分组成，SPI 和序号。
4. 对加密区域和 ESP 头部做验证，得到一个完整性度量值 ICV，并附在 ESP 报文的尾部；
5. 将 IP 头部附在 ESP 报文前，得到新的 IP 报文，发送报文。

拆包过程

1. 首先，检查协议类型是 50，确定为 IPSec 包；
2. 通过 ESP 头部 SPI 确认 SA 内容，以及通过序列号确认不是重放攻击；
3. 计算验证区域的摘要，与附在末尾的 ICV 做比较，若相同则说明数据完整；
4. 根据 SA 提供的算法和密钥，解密加密区域，得原 IP 包和 ESP 尾部；
5. 根据 ESP 尾部的填充长度信息删除填充字段得到原 IP 包；
6. 根据得到的原 IP 包的目的地址进行转发。