IPSec 传输模式下 ESP 报文的装包与拆包过程

2015 级计应　　15331151　　李佳

一、IPsec 简介

IPSec (IP Security)是 IETF（Internet Engineering Task Force，Internet 工程任务组）的 IPSec 小组建立的一组 IP 安全协议集。IPSec 定义了在网络层使用的安全服务，其功能包括数据加密、对网络单元的访问控制、数据源地址验证、数据完整性检查和防止重放攻击。

IPSec 是安全联网的长期方向。它通过端对端的安全性来提供主动的保护以防止专用网络与 Internet 的攻击。在通信中，只有发送方和接收方才是唯一必须了解 IPSec 保护的计算机。在 Windows XP 和 Windows Server 2003 家族中，IPSec 提供了一种能力，以保护工作组、局域网计算机、域客户端和服务器、分支机构（物理上为远程机构）、Extranet 以及漫游客户端之间的通信。

二、ESP 简介

IPsec 封装安全负载(IPsec ESP)是 IPsec 体系结构中的一种主要协议，其主要设计来在 IPv4 和 IPv6 中提供安全服务的混合应用。IPsec ESP 通过加密需要保护的数据以及在 IPsec ESP 的数据部分放置这些加密的数据来提供机密性和完整性。且 ESP 加密采用的是对称密钥加密算法，能够提供无连接的数据完整性验证、数据来源验证和抗重放攻击服务。根据用户安全要求，这个机制既可以用于加密一个传输层的段(如:TCP、UDP、ICMP、IGMP)，也可以用于加密一整个的 IP 数据报。封装受保护数据是非常必要的，这样就可以为整个原始数据报提供机密性。ESP 提供机密性、数据起源验证、无连接的完整性、抗重播服务和有限业务流机密性。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，也可以防止回放攻击。

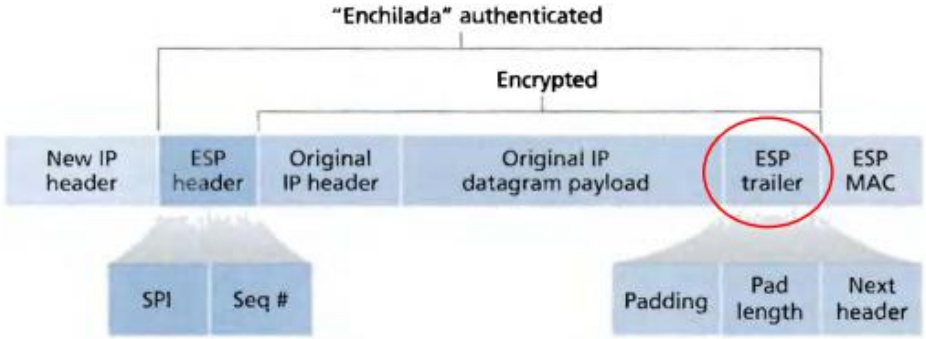
传输模式是 IPSec 工作的两种方式之一。与隧道模式不同的是，保护的仅仅是真正传输的数据，而不是整个 IP 报文。在处理的方法上，原来的 IP 报文会先被解开，再在数据前加上新的 ESP 或 AH 协议头，最后再装回原来的 IP 头中，即原来的 IP 包被修改过再传输了。

三、传输模式下 ESP 报文的装包与拆包过程

在传输模式下的 IPSec ESP 报文的结构图如下：

装包过程：

1.在原 IP 报文末尾添加尾部(ESP trailer)。尾部信息如图所示，包含三部分。由于所选加密算法可能是块加密，当最后一块长度不够时，需要进行补充(padding)。且需要附上填充长度(Pad length)来方便解包时顺利找出用来填充的那一段数据。而 Next header 则用来表明被加密的数据报文的类型。



2.将原数据报文和刚添加的 ESP 尾部信息作为一个整体进行加密，具体的加密算法由密钥和 SA 给出。

3.在第 2 步得到的加密数据前添加 ESP Header。ESP Header 由 SPI 和序号(Sequence number)两部分组成。加密数据与 ESP 头合称为”enchilada”。

4.附加完整性度量结果(ICV, Integrity check value)。对第三步得到的”enchilada”做摘要，得到一个完整性度量值，并附在 ESP 报文的尾部。

5.将原 IP 头放回到第 4 步后形成的报文的头部前，组织成一个新的 IP 报文。

拆包过程：

1.接收方收到数据报文后，发现协议类型是 50，知道这是一个 IPSec 包。首先查看 ESP 头，通过里面的 SPI 决定数据报文所对应的 SA。

2.计算”enchilada”部分的摘要，与附在末尾的 ICV 做对比，如果一样，说明数据完整；否则断定收到的报文已经不是原来的报文了。

3.检查 Seq 里的顺序号，保证数据是”新鲜”的，不是回放攻击。

4.根据 SA 所提供的加密算法和密钥，解密被加密过的数据 ”enchilada”。得到原 IP 报文的数据部分和 ESP 尾部(trailer)。

5.根据 ESP 尾部的填充长度信息，可以找出填充字段的长度，删去后就得到原来的 IP 报文。

6.根据获取的原 IP 包目标地址进行转发。