IPSec传输模式下ESP报文的装包与拆包过程

13331233 孙中阳

IPSec

`Internet 协议安全性` (IPSec)是一种开放标准的框架结构，通过使用加密的安全服务以确保在 Internet 协议 (IP) 网络上进行保密而安全的通讯。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等。

ESP

`封装安全载荷` （ESP）定义在RFC2406中，用于为IP提供保密性和抗重播服务，包括数据包内容的保密性和有限的流量保密性。作为可选的功能，ESP也提供和AH鉴别头部同样的数据完整性和兼备服务。由于ESP要对数据进行加密处理，因而它比AH需要更多的处理时间。

报文构成

`安全参数索引（32 bit）` `序列号（32 bit）` `载荷数据（变长）`
`填充填充长度（8 bit）` `下一头部（8 bit）` `鉴别数据（可变长）`

IPsec ESP

报文构成

`IP 头` `ESP 头` `IP 数据报文` `ESP 尾` `ESP MAC`

装包过程

1）在 IP 报文的末尾添加 ESP 尾信息。ESP 尾部包含三部分,按顺序分别是

`padding`、`pad length`、`next header`。由于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(padding)，附上填充长度(pad length)方便解包时顺利找出用来填充 的那一段数据。而`next header` 则用来标明被加密的数据报文的类型，例如 TCP。

2) 将 IP 报文以及第 1)步得到的 ESP 尾作为一个整体进行加密，得到加密数据。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，ESP 头由两部分组成，`SPI` 和`sequence number`。 加密数据与 ESP 头组合的部分称为 `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，作为 ESP MAC。

5) 拿到 IP 头，IP 头与第 4)步得到的结果组合就是可以发送的完整的包了。

拆包过程

1) 检查收到报文的协议类型，若不是 IPSec 则退出过程，若是则进入第 2)步。

2) 如果收到的 IPSec 包是一个分段，则必须保留并等到其他部分接收完才能进入第 2)步。

3) 查看 ESP 头，检查 SA 是否存在，若不存在则丢弃包，退出过程。若存在则通过 ESP 头 中的 SPI 判断 SA，然后进入第 3)步。

4) 计算 `enchilada` 部分的摘要，与附在末尾的 ICV 做对比，若相同，说明数据是完整的， 可以继续执行;若不同，则可以断定所收到的报文已经不是原来的报文，从而退出过程。

5) 检查 Seq 里的顺序号，保证数据是“新鲜”的。

6) 根据 SA 所提供的加密算法和密钥，解密 `enchilada` ，得到原 IP 报文与 ESP 尾。

7) 根据 ESP 尾的填充长度信息，找出填充字段并删去，从而得到原来 的 IP 报文。

8) 转让到更高一级的协议层(如 TCP 或 UDP)，由它们对这个包进行处理。