信息安全 IPsec传输模式下 ESP报文的装包与拆包过程

数据科学与计算机学院 17343094 彭湃

在上次的作业中，我们实现了一个`X.509 Reader`。在最近的课程中，因为老师正好跟我们讲解了在隧道模式下，`ESP`报文的装包与拆包过程，所以我们本次的作业，是需要阐述在另外一种模式——传输模式(`Transfer mode`)下`ESP`报文的拆包与装包过程 ^-^。

话不多说，下面切入正题。

信息安全 IPsec传输模式下 ESP报文的装包与拆包过程
数据科学与计算机学院 17343094 彭湃
一、什么是IPsec
二、ESP分析
三、传输模式装包拆包过程
1. 装包过程
2. 拆包过程

一、什么是IPsec

在开始一切之前，我觉得我们有必要需要回答的一个问题是，什么是`IPsec`？

`IPsec`（Internet Protocol Security)，事实上也就是我们通常所说的网络安全协议，它是一个协议包，通过对透过对`IP`协议的分组进行**加密**和**认证**来保护`IP`协议的网络传输协议族（一些相互关联的协议的集合），或者用老师的说法，它是一个协议组件。它的主要工作区域在网络层。

而作为一个协议组合，它主要由下面几个协议组成：

- `AH`（认证头）：`AH`主要在数据的传送过程中对`IP`数据进行完整性度量和来源认证，还可以防止回放攻击。
- `ESP`(封装安全载荷)：`ESP`是我们本次作业的重点研究对象，它能够在数据的传输过程中对数据进行完整性度量和来源认证，可以选择加密，也可以选择防止回放保护。
- `SA`(安全关联)：`SA`提供算法和数据包，同时提供`AH`、`ESP`操作所需的参数。

二、ESP分析

上面我们提到了`AH`和`ESP`，这两者的作用很相似，事实上`ESP`可以单独使用，也可以直接和`AH`结合使用。它的结构由`IP`协议号50标识，但是他的封装结构和采用的模式相关；同时加密方式也随着采用模式的不同而不同：

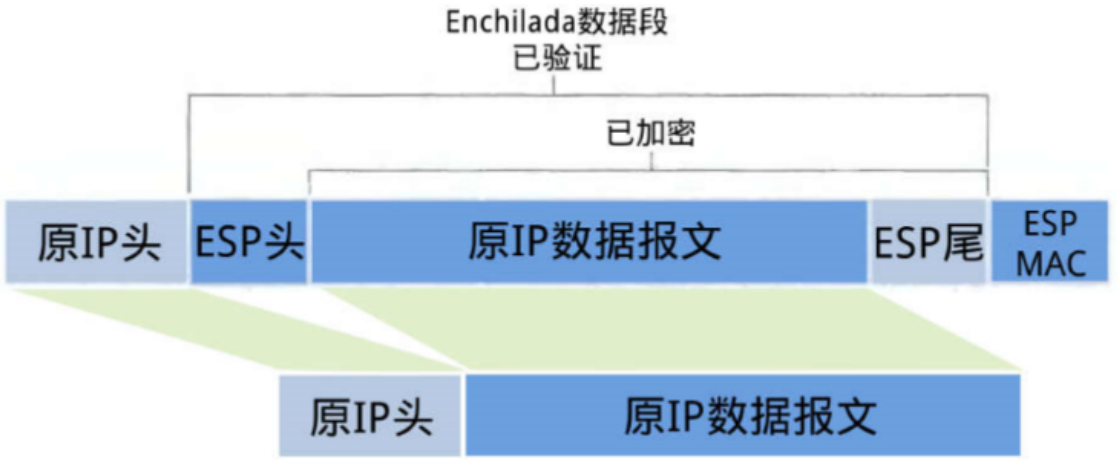
- 传输模式(transport mode)：不对整个`IP`原报文进行保护，而只是对它的有效数据内容部分，也就是我们通常所说的有效载荷进行加密，在这个过程中，原报文的结构会被改变。
- 隧道模式(Tunnel mode)：对整个`IP`原报文进行保护，直接将原报文前面加上`ESP`协议头，再加上新的`IP`头，整个报文的传输过程像是在一个密封的隧道中进行一样，原报文的结构不会改变。

`ESP`的加密服务是可选的，但如果启用加密，则也就同时选择了完整性检查和认证。因为如果仅使用加密，入侵者可能发动密码分析攻击。

三、传输模式装包拆包过程

Tips:以下图片均出自蔡老师课件

在传输模式下的`ESP`报文结构图为：



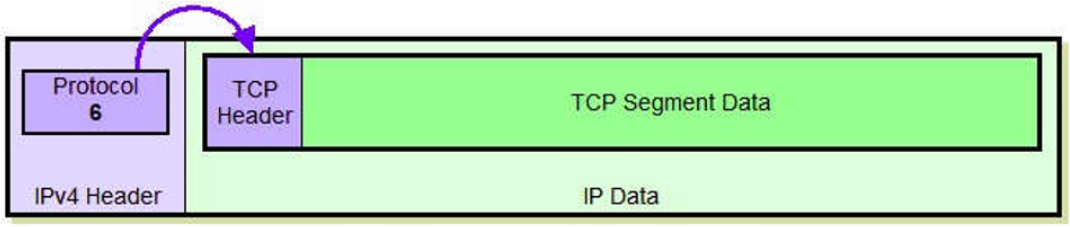
1. 装包过程

- 在原`IP`报文的末尾添加尾部(`ESP Trailer`)。尾部包含三个部分，分别是：`Padding`、`Pad Length`、和`Next header`.

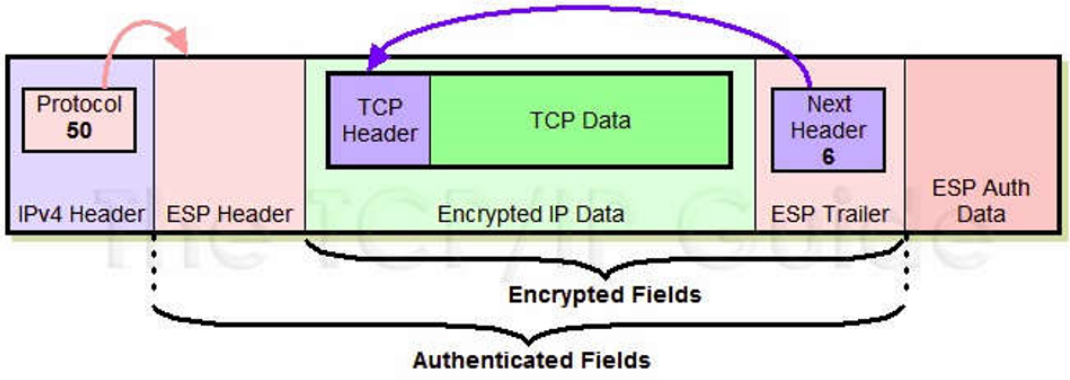
  > *tips :*
  >
  > 三个部分数据的含义：
  >
  > 由于我们选择的加密算法可能是块加密，所以当最后一块长度不够的时候，我们就需要进行填充(这个在之前写`MD5`时我们都有接触)，也就是上面所说的`Padding`，同时需要附上填充长度(`Pad Length`)，这个数据主要是为了方便解包时的查找，而`Next header`则表明了加密报文的类型。

- 将`IP Datagram`部分以及我们上一步得到的`ESP Trailer`作为一个整体进行加密，具体的加密算法与密钥需要由我们第一部分介绍的`SA`给出。
- 在上一步得到的加密数据前面添加`ESP Header`，它主要由两个部分组成，一个是`SPI`，一个是`序号`，`ESP Header`在`IP`的后面。
- 将我们第三步得到的`ESP Header`和第二步得到的加密整体做一个摘要，并且得到一个完整性量值(`ESP Auth Data`)，并且将其添加到`ESP`报文的尾部，这样就是一个完整的`ESP`数据报文。

具体的加密结果可以看下面蔡老师课件的图片，展示的是`IPV4`的数据包在传输模式下的装包加密传输过程，还是比较详细的。



Original IPv4 Datagram Format



IPv4 ESP Datagram Format - IPSec Transport Mode

2. 拆包过程

- 接收到一个数据报文后，首先会判断协议类型，如果是**50**，那么很明显这就是一个`IPsec`包。
- 计算上面最后一部分加密整体的摘要，同时与报文末尾的`ESP Auth Data`进行对比，如果是一样的话，就保证了数据没有被篡改，否则接收的报文就不是之前的报文了。
- 查看`ESP Header`，里面所包含的`SPI`会对应数据报文的`SA`；同时检查序号，确保数据不是回放攻击。
- 上一步我们可以直线`SA`所提供的算法与密钥，我们可以根据这些来解密被加密的部分，主要是`IP Datagram`和`ESP Trailer`。
- 根据解密出来的`ESP Trailer`里面的`Pad Length`，可以直接找出填充字符的字段，直接将其删去后就是最开始的`IP Datagram`。
- 根据获取的原`IP`包地址进行转发。

至此我们的装包与拆包过程解析全部结束。