TCP 数据加密实现方案简述

湖南新实网络科技有限公司

2019 年 8 月 15 日

文档基本信息

主题	TCP 数据加密实现方案简述
文档号	
创建时间	2019-8-15
发布日期	2019-8-15
版本号	1.0
文件名	TCP 数据加密实现方案简述.pdf
文件格式	Portable Document Format

版本记录信息

版本号	修改人	日期	备注
1.0	张彦龙	2019-8-15	初始版本

地址：湖南长沙岳麓区中电软件园 6 栋 302 室

目录

TCP 数据加密实现方案简述

应用场景：

如图 1 所示，对主机 A 与主机 B 间的 TCP 的通信进行加解密处理。即主机 A 的 TCP 数据通过网络加密结点对其 TCP 数据加密后传送给网络，数据包经互联网传送给主机 B 端的网络加解密结点进行解密处理，处理后的数据送给主机 B 。反向同理。

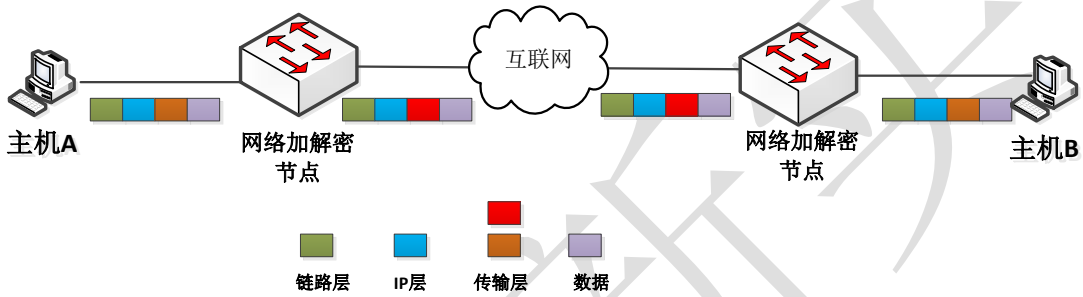

图 1 应用场景图

方案 1 固定密钥的实现：

在网络加解密的结点将 TCP 报文的序号按某一算法进行加密处理，另外将 TCP 数据报文的 DATA 域的数据进行乱序处理，从而实现在对 TCP 数据流报文进行发送序号乱序的同时实现了对报文内容的乱序加密处理。

具体硬件加密方式：

网络加解密结点解析所有经过它的数据流的报文，识别报文是否为 TCP/IPv4 的类型报文，若是则根据图 2 所示的 TCP 头部格式，在传送 TCP 数据时，将序号字段（Sequence Number）作为密钥进行加密处理。否则数据会直接转发输出。

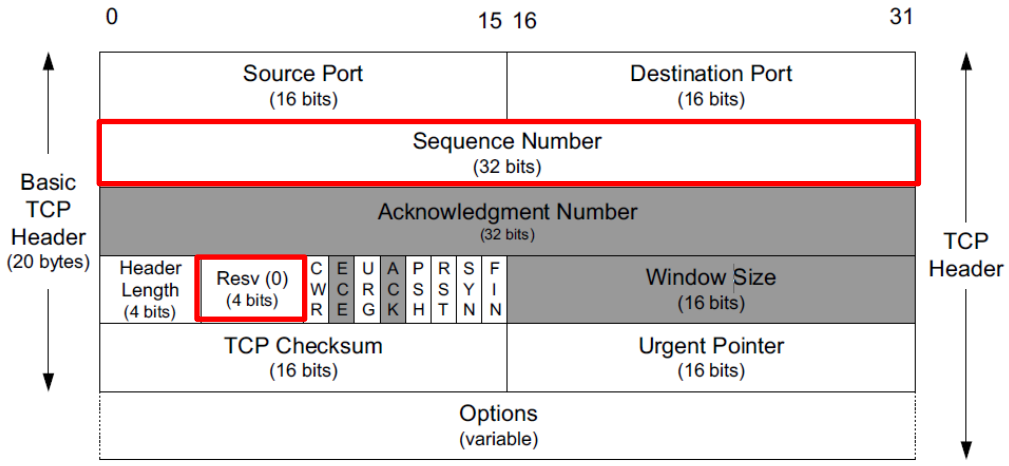

图 2 TCP 头部格式

另外，网络加解密结点会针对其 TCP 类型报文的数据部分根据硬件处理格式进行乱序处理，从而实现数据加密的功能。如图 3 所示，硬件是将数据帧以 128b(16B)的形式进行组织。

图 3 硬件处理帧形式

根据网络加解密结点对数据处理的特点，加密可以将每拍 TCP 报文数据部分的字节数据高低 4 位对调来实现，如图 4 所示。

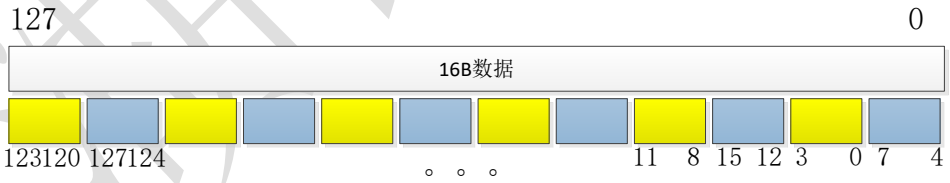

图 4 数据位对调乱序示意图

硬件实现的难点：

1） TCP 报文解析（IPV 4 ）；

2） TCP 的校验和重计算；

3） 线速实现加密处理及恢复。

优点：

1） 可实现加解密处理；

2） 可以保证处理延时。

方案 2 动态密钥的实现：

动态密钥是基于 TCP 类型的数据在握手的过程中传递，即在建立 TCP 的握手时协商此对应 TCP 流对应的密钥；在连接结束时，删除其密钥信息，在下次建立时随机获取密钥池中的新的密钥来进行加密通信。处理过程如图 5、6 所示。

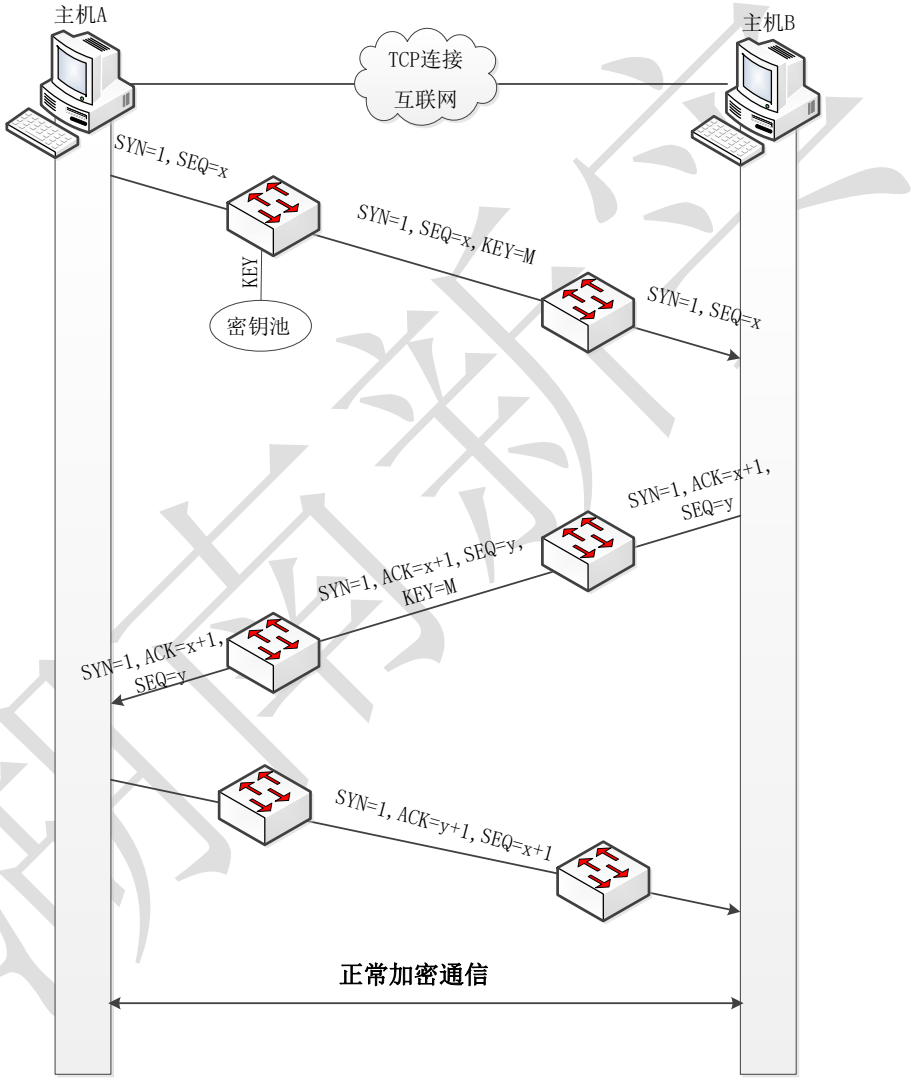

图 5 基于 TCP 建立的密钥协商过程图

在 TCP 建立连接时，网络加解密结点会监测，输入报文是否主 SYN 的报文，若是，则从密钥池中随机申请一个密钥（KEY），将密钥信息随建立连接的报文发送给接收端，接收端接收密钥信息，在接收到连接响应报文时，将确认的密钥信息再返回给发送端，以确认其已经正确协商密钥可以正常通信。

在 TCP 结束连接时，当结束发送端（主机 A）发送 FIN 报文时，网络加密结

点先不立刻注销密钥信息，而是等待主机 B 发送结束时才注销密钥信息，因为主机 A 在申请结束连接时，主机 B 可能还会向主机 A 发送 TCP 的数据，因此，需要等待主机 B 也发送结束报文时才进行密钥的注销。

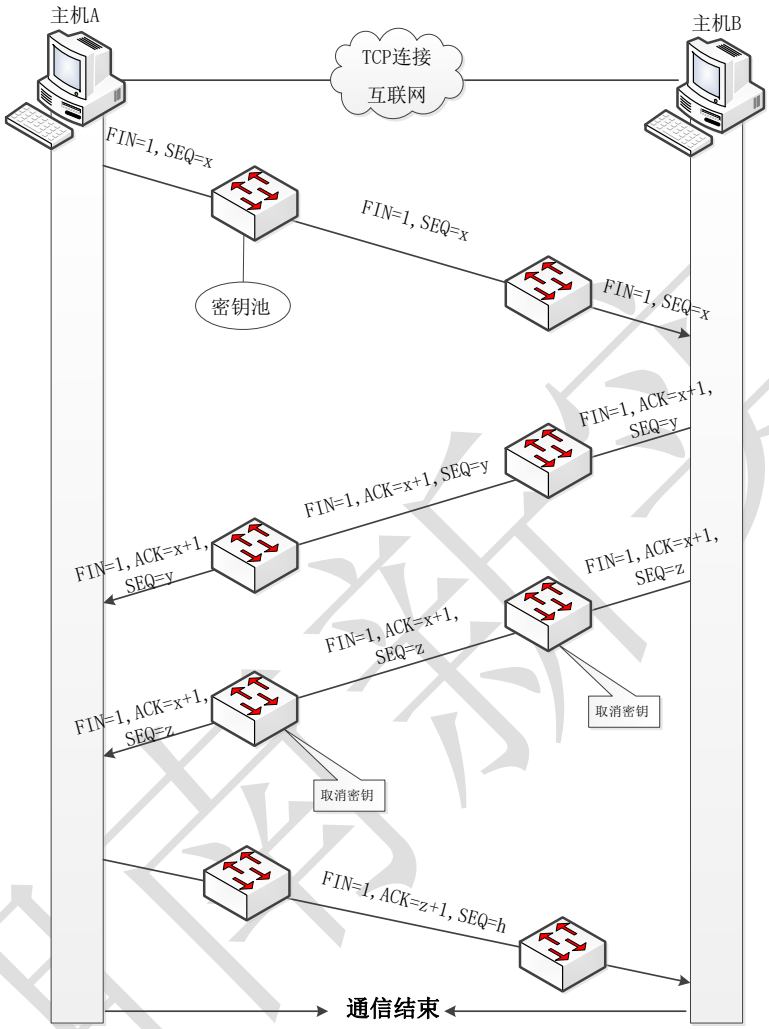

图 6 基于 TCP 结束的密钥取消过程图

密钥池为网络加密结点内部存储的密钥的集合，密钥池内有多种密钥，为了保证通信的安全性，在每条 TCP 流进行通信时，都会选用不同的密钥进行加解密处理。从而可以更细粒度的保证每条 TCP 数据流的安全性。

同方案 1 相同在针对密钥加密的同时还可以实现对报文内容的乱序处理，从而进一步保证其数据的安全性。

方案 2 实现的优化

在实现时，由于每条 TCP 的建立都会随机的在密钥池中选择密钥进行连接且

链路可以存在很长时间无数据交互的情况或链路出现故障无法正常通信的情况，因此在实现时针对每条流设定一个计时器，即若有此流的报文交互则不断更新其时间值到最新的时间点，若某条流长时间无数据通信时，则将此流对应的流表及协商的密钥删除，在恢复通信时重新协商密钥进行通信，如图 7 所示。

当流 A 的数据经过网络加密节点时则更新其流 A 所对应的计时器，流 B 和流 C 则保持不变，若已经达到超时的时间，则更改流状态，将此流表项标记为无效。若此时又有对应流表的数据到来则使用默认密钥进行加密处理，同时通过 TCP 头的状态位的保留位，如图 2 所示，来标记其加密的密钥状态，从而是接收端也可以通过相同密钥解密。

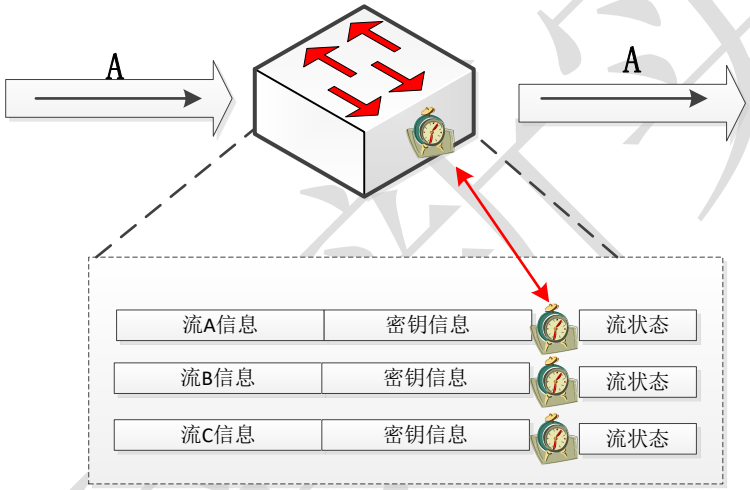

图 7 流表状态管理

以上为 TCP 的两种加密的方案，方案 1 为固定密钥实现方式，其实现比较简单，加密效果则不太安全；方案 2 实现比较复杂，可以针对不同的 TCP 流，选用不同的加密方法，从而可以更细粒度的对通信内容进行加密处理，从而通信内容会更加安全。另外，两种实现方案都需要硬件对报文进行解析、报文乱序移位处理及报文 TCP 头及 IP 头部校验和进行重新计算处理，因此硬件资源开销比较大，但其可以保证加密处理的延时。