算法，迫使客户选择一种较弱的算法。为了防止这种篡改攻击，在步骤5中客户发送一个级联它已发送和接收的所有握手报文的MAC。服务器能够比较这个MAC与它已接收和发送的握手报文的MAC。如果有不一致，服务器能够终止该连接。类似地，服务器发送一个它已经看到的握手报文的MAC，允许客户检查不一致性。

你可能想知道在步骤1和步骤2中存在不重数的原因。序号不足以防止报文段重放攻击吗？答案是肯定的，但它们并不只是防止“连接重放攻击”。考虑下列连接重放攻击。假设Trudy嗅探了Alice和Bob之间的所有报文。第二天，Trudy冒充Bob并向Alice发送正好是前一天Bob向Alice发送的相同的报文序列。如果Alice没有使用不重数，她将以前一天发送的完全相同的序列报文进行响应。Alice将不怀疑任何不规矩的事，因为她接收到的每个报文将通过完整性检查。如果Alice是一个电子商务服务器，她将认为Bob正在进行第二次订购（正好订购相同的东西）。在另一方面，在协议中包括了一个不重数，Alice将对每个TCP会话发送不同的不重数，使得这两天的加密密钥不同。因此，当Alice接收到来自Trudy重放的SSL记录时，该记录将无法通过完整性检查，并且假冒的电子商务事务将不会成功。总而言之，在SSL中，不重数用于防御“连接重放”，而序号用于防御在一个进行中的会话中重放个别分组。

2. 连接关闭

在某个时刻，Bob或者Alice将要终止SSL会话。一个方法是让Bob通过直接终止底层的TCP连接来结束该SSL会话，这就是说，通过让Bob向Alice发送一个TCP FIN报文段。但是这种幼稚设计为*截断攻击*（truncation attack）创造了条件，Trudy再一次介入一个进行中的SSL会话中，并用TCP FIN过早地结束了该会话。如果Trudy这样做的话，Alice将会认为她收到了Bob的所有数据，而实际上她仅收到了其中的一部分。对这个问题的解决方法是，在类型字段中指出该记录是否是用于终止该SSL会话的。（尽管SSL类型是以明文形式发送的，但在接收方使用了记录的MAC对它进行了鉴别。）通过包括这样一个字段，如果Alice在收到一个关闭SSL记录之前突然收到了一个TCP FIN，她可能知道正在进行着某些耍花招的事情。

到此为止完成了对SSL的介绍。我们已经看到它使用了在8.2节和8.3节讨论的许多密码学原则。希望更深入地探讨SSL的读者可以阅读Rescorla的有关SSL的可读性很强的书籍［Rescorla 2001］。

8.7 网络层安全性：IPsec和虚拟专用网

IP **安全**（IP Security）协议更常被称为**IPsec**，它为网络层提供了安全性。IPsec为任意两个网络层实体（包括主机和路由器）之间的IP数据报提供了安全。如我们很快要描述的那样，许多机构（公司、政府部门、非营利组织等等）使用IPsec创建了运行在公共因特网之上的**虚拟专用网**（virtual private network，VPN）。

在学习IPsec细节之前，我们后退一步来考虑为网络层提供机密性所包含的意义。在网络实体对之间（例如，两台路由器之间，两台主机之间，或者路由器和主机之间）具有网络层机密性，发送实体加密它发送给接收实体的所有数据报的载荷。这种载荷可以是一个TCP报文段、一个UDP报文段、一个ICMP报文等等。如果这样的网络层服务适当的话，从一个实体向其他实体发送的所有数据报将隐形于任何可能嗅探该网络的第三方，发