**恋爱式的三次握手和四次挥手**

TCP（Transmission Control Protocol 传输控制协议）是一种面向连接的、可靠的、基于字节流的传输层通信协议，由IETF（Internet Engineering Task Force，是Internet工程任务组，又叫互联网工程任务组，成立于1985年底，是全球互联网最具权威的技术标准化组织，主要任务是负责互联网相关技术规范的研发和制定）的RFC（Request For Comments，是一系列以编号排定的文件。文件收集了有关互联网相关信息，以及UNIX和互联网社区的软件文件） 793定义。

三次握手（three-way handshake）是指建立一个TCP连接时，需要Client和Server总共发送3个包。

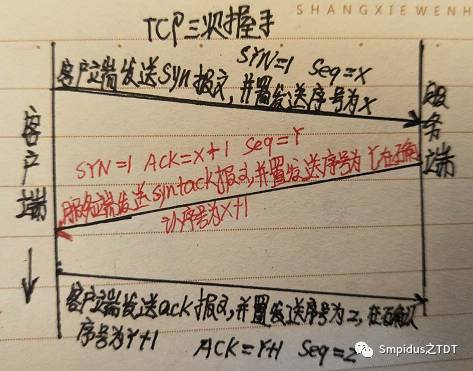
Karma：Amily，我喜欢你。

Amily：Karma，我也喜欢你。

Karma：你喜欢我，我也喜欢你，那我们在一起吧。

TCP连接OK。

把第一句当作是发出的SYN报文，表示请求连接，Amily回答Karma的话视为SYN+ACk报文，即用ACK报文对Karma发出的SYN报文表达确认，又向Karma发出了新的报文，再Karma发出ACK报文确认后，连接建立，Karma and Amily together。





四次挥手（four-way handshake）拆除需要发送四个包。Client或Server均可主动发起挥手动作，任何一方执行close（）操作即可产生挥手操作。

Amily：Karma，我们结婚吧。

Karma：Amily，让我准备一下。

Karma：Amily，我们结婚吧。

Amily：OK，那我们去登记。

TCP连接interrupt。

第一句是Amily发出的FIN报文，表示自己已经传输结束，Karma回答Amily第一句为ACK报文，表示我已经知道了，但是我还没有确定是否收到所有的，还需要稍等一会。Karma第二句回答为FIN报文，表示自己已经收集完成，可以interrupt。Amily第二句回答为ACK报文，表示收到会interrupt。

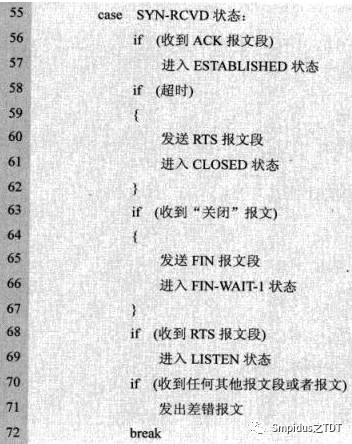
若采用两次握手建立连接

Karma：Amily，我喜欢你。

Amily：Karma，我也喜欢你。

那就没有together或者marry哦。

SYN:(Synchronize sequence numbers)用来建立连接，在连接请求中，SYN=1，ACK=0，连接响应时，SYN=1，ACK=1。  
即，SYN和ACK来区分Connection Request和Connection Accepted。  
RST:(Reset the connection)用于复位因某种原因引起出现的错误连接，也用来拒绝非法数据和请求。如果接收到RST位时候，通常发生了某些错误。  
ACK:(Acknowledgment field significant)置1时表示确认号(Acknowledgment Number)为合法，为0的时候表示数据段不包含确认信息，确认号被忽略。  
  
《TCP/IP协议族》中每一个状态的转换为代码整理下：



第58行指明了当第三次握手失败时的处理操作，可以看出当失败时Server并不会重传ACK报文，而是直接发送RTS报文段，进入Closed状态。这样做的目的是为了防止SYN Flood攻击。  
  
三次握手的漏洞  
DoS攻击、DDoS攻击和DRDoS攻击相信大家已经早有耳闻了吧!  
  
DoS是Denial of Service的简写就是拒绝服务。  
它的攻击方法说白了就是单挑，是比谁的机器性能好、速度快。  
  
DDoS就是Distributed Denial of Service的简写就是分布式拒绝服务。  
它的原理说白了就是群殴，用好多的机器对目标机器一起发动 DoS攻击，但这不是很多黑客一起参与的，这种攻击只是由一名黑客来操作的。  
  
DRDoS就是Distributed Reflection Denial of Service的简写,这是分布反射式拒绝服务的意思。  
它的攻击原理和Smurf攻击原理相近，不过DRDoS是可以在广域网上进行的，而Smurf攻击是在局域网进行的。  
  
1.SYN Flood攻击  
  
假如有很多人冒充Karma，就没有人回复Amily，但是Amily一直在等待Karma的消息。并且Amily处理能力是有限的，达到上限怎么办呢？  
  
SYN Flood  
攻击是当前网络上最为常见的DDos攻击，也是最为经典的拒绝服务攻击。通过网络服务所在的端口发送大量伪造原地址的攻击报文，发送到Server，造成Server上的半开连接队列被占满，从而阻止其他用户进行访问。  
它的数据报特征是大量SYN包，并且缺少最后一步的ACK回复。  
这种攻击的特点是它利用了TCP/IP协议的漏洞，除非你不用TCP/IP，才有可能完全抵御住DDoS攻击。  
原理：  
攻击者首先伪造地址，对Server发起SYN请求，Server回应SYN+ACK，而真实的IP会认为我没有发送请求，不作回应，而Server没有收到回应，Server就不知道是否发送成功，默认情况下重试5次SYN\_retries，这样的话，对于Server内存和带宽有很大的消耗。攻击者处于公网下，可以伪造IP的话，对于Server就很难根据IP来判断攻击者，给防护带来很大的困难。  
  
解决方法：  
(1).无效连接监视释放  
不停监视半开连接和不活动连接，当半开连接数和不活动连接数到达一定值时候，就释放系统资源。  
《孙子兵法》的谋攻引申出来的一句话：伤敌一千，自损八百。  
(2).延缓TCB（传输控制模块）分配方法  
SYN Flood的关键是利用了，SYN数据报一到，系统就分配TCB资源。  
那么我们有两种方法资源问题  
SYN cache  
这种技术在收到SYN时不急着分配TCB，而是先回应一个ACK报文，并在一个专用的HASH表中（Cache）保存这种连接，直到收到正确的ACK，才分配TCB。  
(3).SYN Cookie  
用一种特殊的算法生成sequence number，算法考虑到对方的（IP、端口等）信息和己方信息，收到对方的ACK报文后，验证之后才决定是否生成TCB。  
  
防御方法：  
1.确保服务器的系统文件是最新的版本，并及时更新系统补丁。  
2.关闭不必要的服务。  
3.限制同时打开的SYN半连接数目。  
4.缩短SYN半连接的time out 时间。  
5.正确设置防火墙。  
6.禁止对主机的非开放服务的访问。  
7.限制特定IP地址的访问。  
8.启用防火墙的防DDoS的属性。  
9.严格限制对外开放的服务器的向外访问。  
10.运行端口映射程序或端口扫描程序，要认真检查特权端口和非特权端口。  
11.认真检查网络设备和主机/服务器系统的日志。只要日志出现漏洞或是时间变更，那这台机器就可能遭到了攻击。  
12.限制在防火墙外与网络文件共享。这样会给黑客截取系统文件的机会，主机的信息暴露给黑客，无疑是给了对方入侵的机会。  
  
2.IP欺骗DOS攻击  
  
在Amily和Karma去登记时有人冒充Amily发送RST报文，想要终止他们的登记，那么Karma收到该报文后会怎么想呢？  
  
解决方法：  
  
可以进行口令加密，仅当口令正确时才会接收报文。也可以采用鲁棒的交互协议，加上入口包过滤来保护网络。