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。

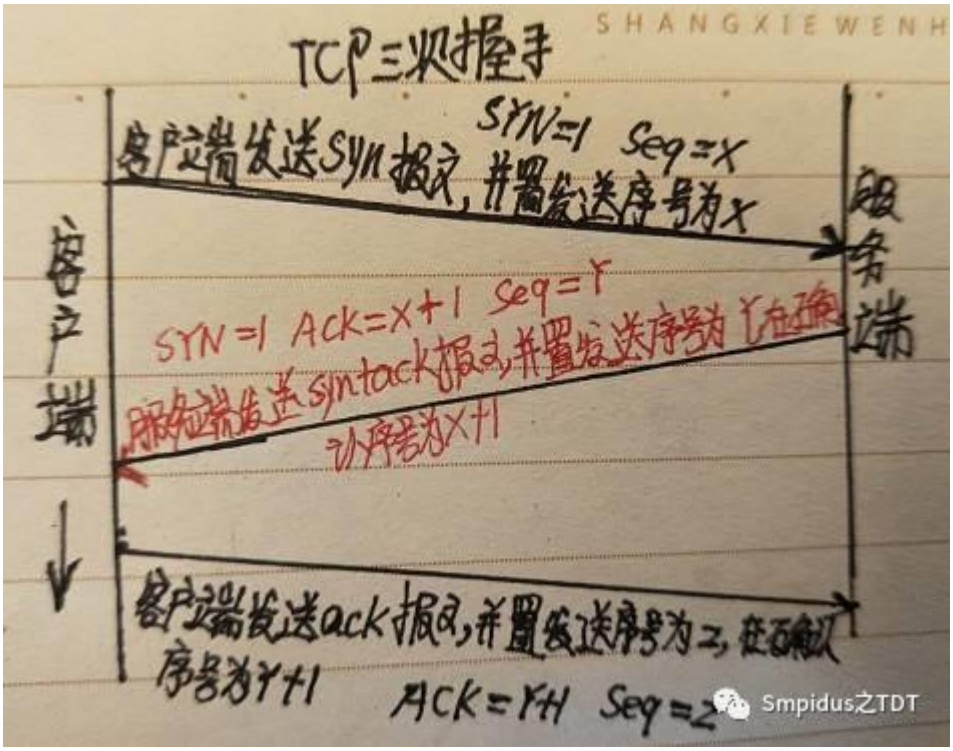
Karma：Amily，我喜欢你。

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

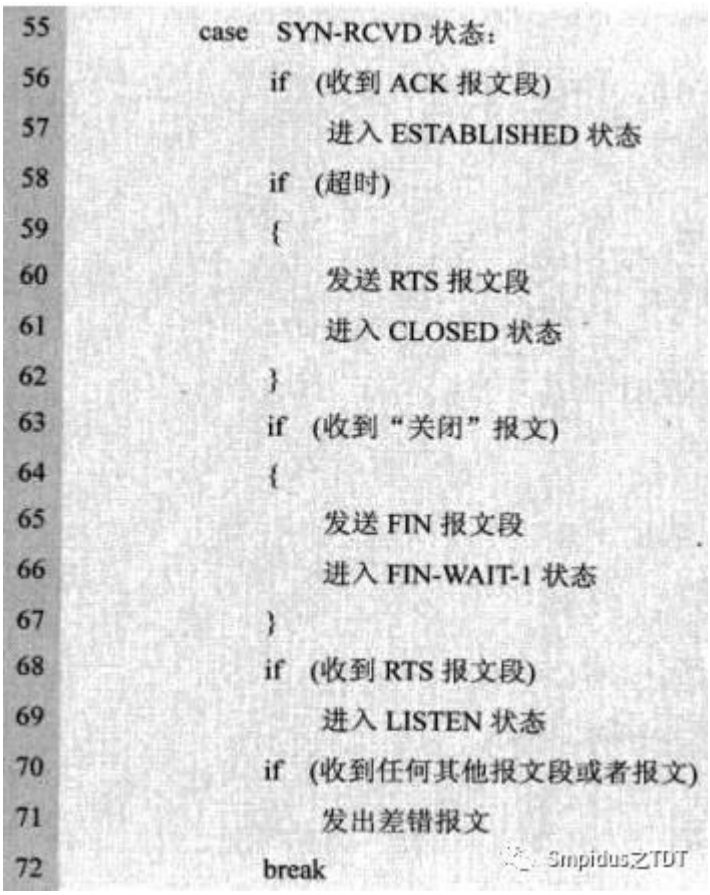
Karma：Amily，我喜欢你。

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。