Jose Herrera

CSE 160 Project 3

1) The value should be random because it lessens the chance that two connections, who are trying to connect to the same server, start with the same initial sequence numbers and thus each connection has a different random starting initial sequence number. This random initial sequence number helps the server know which number it should expect back and when the receiver receives this random number + 1 (the expected number from client) it can officialy establish the connection with this sender.

2) Transport protocol needs to make sure not to overrun the buffer and send more data than the buffer can handle. So the receiver has to let the sender know, by using the ADWindow, how many bytes it can send at a time. The Receiver knows how much data its buffer can handle by subtracting how much data is being written into the buffer and how much is available in the buffer.

3) If a SYN Flood were to occur, the node being attacked will continue to allocate port or socket space for each SYN packet received until all sockets are used up. A way to combat this is to create a timer or some way to give each new port being opened a timed window that if the expected packet is received in that time window, the connection will continue to go through the process of establishing the connection. If the timed window closes without receiving the expected packet, the socket will reopen.

4) Connection Termination is done independently between server and client, thus a FIN attack will cause the socket not to close and allow data to be received from anyone in this port or socket. To combat this, since each node terminates independently, once a node receives the last piece of data from the sender, then the receiver could start a timer and tell the sender it will close the connection once the timer expires and the sender can follow suit.