James Watterson

CS422 - Lab5

The main security vulnerability of the mytalk application is the inability to verify that messages came from the peer from which the requests purport to come from. There are two facets to this problem, initiating a session and maintaining a session. The more crucial component is the maintenance of a session.

Session Maintenance

To verify the provenance of a message during a session is fairly simple. Upon initial contact the two peers exchange keys and any further communication should have these unique keys prepended to the message. This way every message that is received can be verified to be sent from the machine the packets purport to have been sent from.

Session Initiation

Initiating a session is a less important problem because the question of the validity of a message is more important than actually beginning to accept them. To filter bogus request in this domain, peers should perform a handshake sequence. Of course part of this handshake should be to exchange the keys mentioned above.