Assignment 1
CPSC 526 Fall 2017
October 1, 2017

Mason Lieu
ID: 10110089
mlieu@ucalgary.ca

Shane Sims
ID: 00300601
shane.sims@ucalgary.ca

Task 1 - Exploit the vulnerability

The vulnerability can be found in the readLineFromFd function where it reads from the socket into the provided buffer. Since this function does not check the size of the input, the vulnerability can be exploited by a client by providing an input greater than 32 bytes to overflow the buffer into the memory space of the password. This effectively overwrites the server's password with the overflowed bytes. The next time the client connects to the server, the client can input the overflowed bytes for the password to force the server to reveal its secret.

Task 2 - Fix the vulnerability

The vulnerability can be removed from the readLineFromFd function by reading from the socket an amount equal to the size of the buffer. This ensures that a buffer overflow does not take place and the server's data is protected from this exploit.