Assignment 1
CPSC 526 Fall 2017
October 1, 2017

Mason Lieu	Shane Sims
ID: 10110089	ID: 00300601
Tutorial 03	Tutorial 04
mlieu@ucalgary.ca	shane.sims@ucalgary.ca

Task 1 - Exploit the vulnerability

The vulnerability can be found in the readLineFromFd function where this function 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 the instantiated buffer size to overflow the buffer contents into the memory space of the password. This overwrites the server's password with the overflowed bytes, effectively changing the password. The next time the client connects to the server, the client can input the overflowed bytes (i.e. the new password), forcing 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 a number of bytes 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.

How to compile and run our patch

Our patched server is compiled and run the same as the original server.

Sample exploit of the original server

Server side

```
1  Masons-MacBook-Pro:a1 MasonL$ ./secretServer 1234 pass 'My favourite number is 42.'
2  Waiting for a new connection...
3  Talking to someone.
4  Someone used an incorrect password.
5  Waiting for a new connection...
6  Talking to someone.
7  Someone used an incorrect password.
8  Waiting for a new connection...
9  Talking to someone.
10 Someone used the correct password.
```

```
11 Waiting for a new connection...
```

Client side

```
1  Masons-MacBook-Pro:a1 MasonL$ nc localhost 1234
2  Secret Server 1.0
3  NEWPASS
4  I am not talking to you, bye!
5  Masons-MacBook-Pro:a1 MasonL$ nc localhost 1234
6  Secret Server 1.0
7  1111111111222222222233333333344NEWPASS
8  I am not talking to you, bye!
9  Masons-MacBook-Pro:a1 MasonL$ nc localhost 1234
10 Secret Server 1.0
11 NEWPASS
12 The secret is: My favourite number is 42.
```

Line 1 of the server side shows the initialization of the server with the password = 'pass' and the secret.