**CSCI 530 Lab**

**Application Security**

1. The new separation is 6 from the ebp
2. A) The value is 24 .24 characters can be passed as the arguments until the segmentation fault occurs.

B) The reason that it is ok to get more than 10 characters up to a point is that, maybe the stack has some buffer bytes around itself, to prevent overflows generally.

C)

1. Contents of fixmyname.txt :

#include "stdio.h"

unsigned char key[4] = { 0x47, 0x4f, 0x57, 0x88 };

main()

{

int j;

unsigned long data;

printf("\nEvolution of 'data' as bytes from 'key' are in-shifted from right\n");

printf("letters should be progressively replaced by numbers, one byte at a time\n\n");

data=0xaabbccdd;

printf("Initial value of 'data': %08x\n\n", data );

printf("4 rounds: slide existing bits one byte left, then OR incoming byte into rightmost\n");

for (j=0;j<4;j++)

{

data=(data<<8)|(unsigned long)key[j];

printf("------> %08x\n", data );

sleep(3);

}

}

Evolution of 'data' as bytes from 'key' are in-shifted from right

letters should be progressively replaced by numbers, one byte at a time

Initial value of 'data': aabbccdd

4 rounds: slide existing bits one byte left, then OR incoming byte into rightmost

------> bbccdd47

------> ccdd474f

------> dd474f57

------> 474f5788