Arun Agarwal

Professor Salvatore

Computer Systems and Low-Level Programming (CIS 2107)

March 26th, 2021

Assignment 5

1. What is the command to compile the files with extra symbols that are useful for GDB?

gcc -g GDBassign.c blowfish.c

2. What's the address of stuff?

gdb a.out

break main

run

x stuff

0x7fffffffc2a0: 0x00000000

3. What's the address of stuff[0]?

x &stuff[0]

0x7fffffffc2a0: 0x00000000

4. Do we expect these to be the same? Why? Explain what the [ ] operator does in C.

Yes, we do expect these results to be the same because the pointer to the entire array will refer to the first element of that array. The [] operator in C is short for *(ptr + i), where i would be the index.

5. In Blowfish_Init( ), what is the value of key?

0x400ce0 “LAME_KEY”

6. What command(s) did you type in order to learn this?

break Blowfish_Init

d key

c

7. In Blowfish_Init( ), what are the values of i and j after the nested for loops have finished? i.e., after:

```
for (i = 0; i < 4; i++)
{
    for (j = 0; j < 256; j++)
      ctx->S[i][j] = ORIG_S[i][j];
}
```

i = 4

j = 256

8. What command(s) did you type in order to learn this?

break Blowfish_Init

s //until I reached the blowfish function

s //until I am in the for loop

u //to finish the for loop

print i

print j

9. Before the Blowfish_Encrypt function is called, what is the value of stuff[3] (for each, print the value, and the command used to obtain the value):
    a. in hex?
    b. in binary?
    c. as a float?
    d. as 4 chars?

break main

n //Keep pressing this until we reach the line: printf("Encrypting buffer ..\n"); (This is code just before Blowfish_Encrypt is called)

a. In hex:

print /x stuff[3]

0x20656874

b. in Binary:

print /t stuff[3]

10000001100101011010000111010 0

c. as a float:

print /f stuff[3]

1.94316151e-19

d. as 4 chars:

x /4c &stuff[3]

116 't' 104 'h' 101 'e' 32 ' '

10. Before the Blowfish_Encrypt function is called, what is the value of stuff if we treat it as a string? (You don't have to write the whole string. Just describe what's there.) What was the command typed in order to obtain this value?

The value of stuff if we treat it as a string seems to be a string from a Muppet song:

"Oh, who are the people in your neighborhood?\nIn your neighborhood? \n In your neighborhood? \n Say, who are the people in your neighborhood? \n The people that you meet each day \n \n [Anything Muppet #1: "...

The command types in order to obtain this value was x /s stuff.

11. What is the value of x the first time that the function F() in Blowfish.c is called?

break F

run

Breakpoint 1, F (ctx=0x7fffffffd910, x=1753098189) at blowfish.c:550

d = x & 0x00FF;

```
(gdb) p x
$1 = 1753098189
```

The value of x the first time that the function F() in Blowfish.c is called is 1753098189.

12. What is the output if we run GDB's backtrace (abbreviated "bt") command inside the function F() in Blowfish.c the first time F() is called? Briefly explain the output of the command in your own words.

This is the output when we run GDB's backtrace command, bt, inside the function F() in Blowfish,c the first time F() is called:

```
(gdb) bt
#0  F (ctx=0x7fffffffd910, x=1753098189)
    at blowfish.c:550
#1  0x0000000000400860 in Blowfish_Encrypt (
    ctx=0x7fffffffd910, xl=0x7fffffffc240,
    xr=0x7fffffffc244) at blowfish.c:602
#2  0x0000000000400aa9 in Blowfish_Init (
    ctx=0x7fffffffd910,
    key=0x400ce0 "LAME_KEY", keyLen=8)
    at blowfish.c:754
#3  0x000000000040066d in main () at GDBassign.c:383
```

Here, Backtrace (or 'bt') was run inside the function F() in Blowfish.c the first time F() is called. The arguments of the function call F() are listed along with the value of each variable. Next, the Blowfish_Encrypt method, which contains the F() method and the arguments for the Blowfish_Encrypt call that has F() in its scope, are listed. After that, the Blowfish_Init function is listed with its arguments and their values, and it has Blowfish_Encrypt in its scope. Thus, the backtrace command is showing the functions that were called to allow one to arrive at the current frame the first time F() was called. Furthermore, it indicates the line number and the source file of the related/relevant methods.