Student CTF
Summer Term 2013

Raphael Ernst

Assignment Sheet 3

Information about this sheet:

- Release date: Thursday, June 6th, 2013
- Discussion in group: Tuesday, June 11th, 2013

Exercise 3: Binary Patching

Consider the following C program.

```
1  #include <stdio.h>
2  #include <stdlib.h>
3  #include <string.h>
4
5  #define BLOCK_SIZE 4
6
7  int retVal;
8  char memoryBlock1[BLOCK_SIZE];
9  int val;
10 char memoryBlock2[BLOCK_SIZE];
11
12 int sampleFn(char* input) {
13    char memoryBlock3[BLOCK_SIZE];
14    int retVal = 42;
15
16    memcpy(memoryBlock3,input,strlen(input));
17
18    return retVal;
19 }
20
21 int main(int argc, char* argv[]) {
22    retVal = 23;
23    val = 21;
24
25    if(argc != 3) {
26       printf("Expecting␣two␣parameters...\n");
27       return retVal;
28    }
29
30    printf("%s␣%d\n",argv[1],strlen(argv[1]));
```

```
31    printf("retVal:␣%d\n",(int)&retVal);
32    printf("memoryBlock1:␣%d\n",(int)memoryBlock1);
33    printf("memoryBlock1[1]:␣%d\n",(int)&memoryBlock1
          [1]);
34    printf("memoryBlock1[2]:␣%d\n",(int)&memoryBlock1
          [2]);
35    printf("val:␣%d\n",(int)&val);
36    printf("memoryBlock2:␣%d\n",(int)memoryBlock2);
37
38    memcpy(memoryBlock1,argv[1],strlen(argv[1]));
39    printf("Result:\n");
40    printf("sampleFn:␣%d\n",sampleFn(argv[2]));
41    printf("retVal:␣%d\n",retVal);
42    printf("val:␣%d\n",val);
43
44    return retVal;
45 }
```

Compile the program and check the output with valid input data. You will see several outputs. Patch your program binary in two steps such that

a) (first step) the function sampleFn return $\neq 42$,

b) (second step) the output produced by line 40 does no longer occur.