CS6570 : Secure Systems Engineering
Lab 3 : Return Oriented Programming

10th February 2022

In this lab you will utilize Return-oriented programming tools to find and chain gadgets to execute different tasks using the same executable.

Resources:

Before you start, install ROPGagdet : https://github.com/JonathanSalwan/ROPgadget

```
$ pip install ropgadget
$ ROPGadget --binary lab3_rop
```

All the teams are given the same statically linked executable, which you will be exploiting and constructing ROP gadgets.

Problem 1: 30 points

In this problem you will chain gadgets found in *lab3_rop* to compute the 6!. You need not implement loops/jumps to compute 6!. You should chain your gadgets such that step by step multiplication starting from 1 to 6 should be executed by the gadget. The final value (6!) should be printed on the screen. Following is a sample output:

```
Input 10 words:
Here are the first characters from the 10 words concatenated:
SaiGanesha
Value in glb is 720
Segmentation fault (core dumped)
```

Problem 2 : 70 points

In this problem you will chain gadgets found in *lab3_rop* to compute the n^{th} Fibonacci number. You need to implement loops as part of the ROP logic. The n value can be hardcoded as part of the exploit string, but the gadgets as such should remain the same for different n values. On changing the n value, the corresponding Fibonacci number should be calculated without any change in the gadgets. The final n^{th} Fibonacci number should be printed on the screen.
Following is the Fibonacci program logic that you are expected to encode via gadgets:

```
n = 4; // input
a = 0;
b = 1;
do{
    c = a + b;
    a = b;
```

```
    b = c;
}while(n>=1)
printf("%d", c);
```

In the above logic, following would be the Fibonacci sequence: 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, ... The initial numbers 0 and 1 are neglected. Following is a sample output for 15^{th} Fibonacci number:

```
Input 10 words:
Here are the first characters from the 10 words concatenated:
SaiGanesha
Value in glb is 987
Segmentation fault (core dumped)
```

Submission:

1. This is a team-based assignment.
2. The exploit strings for the above 2 problems need to be submitted.
3. No report/document explaining your gadget construction or technique needs to be submitted. Only the exploit strings needs to be submitted.