Assignment 4B: ARM ROP

Objectives for this assignment:

- Mount a Return-Oriented-Programming attack on an ARM device

Bill of Materials

To complete this lab you will need:

- STM32 NUCLEOL152RE evaluation board
- 1x USB cable Type-A to type-B mini
- hwsec.elf (on canvas)

ROP exploit (4pts)

For this last assignment, you will mount a ROP exploit against the firmware on your Nucleo board! The goal is to print the content of `flag_rop` located at `0x20001b48`.
(Double-check the flag address via `nm firmware.elf | grep flag_rop`)

Connect to the UART interface of the board and type 3 to select “Assignment 4B: ARM ROP”.

You will be prompted with the following message:

```
Welcome to assignment ROP!
Please, smash the stack:
```

From here, an `unsafe_read` function will read your input until `'\n'` is detected.
Use this stack-smashing primitive to create a ROP chain that prints flag_rop.

Deliverable:

- A text file containing the flag.
- A text file listing the targeted gadgets, alongside with a description of how you found them.
- The script or command to exploit the firmware.

Hints:

- For this assignment, you can use a debugger to debug your ROP script, however, the correct flag will only be printed if the debugger is detached!
- Do not try to shellcode! The SRAM region is set as Execute Never (XN).
- Remember you are running Thumb code.
- For finding ROP gadgets, you can either manually disassemble the firmware file, or use automated tools, such as `ropper` or `ROPgadget`.

Bonus: Defeat Anti-Debug (1pts)

As mentioned before, we inserted anti-debug tricks for this challenge. If you find a way to bypass them and extract the flag *even in the presence* of a debugger, you obtain one bonus point!

Important: Unless prior bonus challenge, this one is purely optional, gives you one additional point, and will not be discussed in the graded discussion session!

Deliverable:

- A writeup pinpointing our anti-debug measures, and how you bypassed them.

Hints:

- As this is a bonus challenge, the TAs will not give any help or advise.