

CSC 583 Fall 2024 Lab 1

Dr. Si Chen

September 17, 2024

Introduction

The goals of this lab are:

- Understanding the concepts of registers and stack frames in ARM AArch32 Assembly programming.
- Using GDB to reverse engineer and read the assembly code.

Our course webpage: <https://www.cs.wcupa.edu/schen/advsec24/>

Lab Instructions

Step 1: Connect to the BadgerCTF System and go to lab folder

```
cd advsec24/lab1
```

Step 2: Use GDB to Analyze the Binary Program

```
debug-arm lab1
```

Step 3: Disassemble the add_plus1 Function

```
disas add_plus1
```

Questions:

1. Q1: Identify the assembly instructions for loading the integers a and b into registers.
2. Q2: Identify and explain the instructions responsible for performing the addition and storing the result.
3. Q3: Why are we using the 'add' instruction for calculating $a + b + 1$?

4. Q4: Identify the instructions that create the stack frame in the function 'add_plus1'. Explain their purpose.
5. Q5: Identify the instructions that remove the stack frame in the function 'add_plus1'. Why is this necessary?

Deliverables

Submit a detailed project report in PDF format to answer the above questions. Include pictures, diagrams, and code snippets.

Submission

- Check the lab due date on the course website. Late submissions will not be accepted.
- Submit your assignment to D2L directly.
- **No copy or cheating is tolerated.** If your work is based on others', please give clear attribution. Otherwise, you **WILL FAIL** this course.