Lecture 3: Branching and Looping

Table of contents

0.1 Objectives

1 Branching

- By default, the CPU loads and executes programs sequentially.
- A branch, or transfer of control, is a way of altering the order in which statements are executed.
- There are two basic types of transfer:

1. **Unconditional transfer**, in which a transfer is occurred unconditionally.
2. **Conditional transfer**, in which a transfer is occurred based on a certain condition.

1.1 Instruction Pointer

- The EIP, or instruction pointer , register contains the address of the next instruction to be executed. Certain machine instructions manipulate EIP, causing the program to *branch* to a new location.

1.2 JMP Instruction

Syntax

```
        JMP   <destination>
```

- The JMP instruction causes an unconditional transfer to a destination address.
- The destination (target) operand specifies the address of the instruction being jumped to. This operand can be an immediate value, a general-purpose register, or a memory location.

> In this course, we only consider the immediate value for the destination operand.

1.2.1 Relative vs Absolute Offset Address

- The destination address, within the instruction stream, can be relative offset or absolute offset

- A relative offset is a signed displacement to the current value of the EIP.

$$\text{Offset Address} = \text{EIP} + \text{DEST}$$

- An absolute address is an offset from the base of the code segment.

$$\text{Offset Address} = \text{DEST}$$

1.2.2 Types of Jumps:

1. Near Jump:
2. **Short jump**:
3. Far Jump