Assignment 9

1. Briefly describe the concept of "Stack Frame" (1 through 5 points depending on quality of the answer)

**Answer:** The stack frame, also known as the activation record, is a collection of data. This data which falls on the stack is paired with a subprogram call. The frame includes the argument variables passed, the return address, local found variables, and a copy of registers. These registers are modified by the subprogram and need to be restored.

1. Briefly describe the concept of a "Calling Convention" (1 through 5 points depending on quality of the answer)

**Answer:** A calling convention is a way for subroutines to receive parameters from their caller, and how they return results. Depending on the implementation, this will determine where parameters, return values, return addresses, and scope links will be placed. This also determines how the tasks of preparing for a function call and restoring the environment afterward are divided between the caller and called.

1. Why do the book examples always start functions with "push ebp" and "mov ebp, esp" (2 points).

**Answer:** The book starts functions this way because “push ebp” and “mov ebp, esp” identify as prolog assembly functions. These functions store the previous base pointer, then sets it to be the top of the stack. The stack contents are then saved down the stack, causing the function to be able to push and pop in the stack.

1. What is the x64 equivalent to "push ebp" and "mov ebp, esp)" (2 points)

**Answer:** The x64 equivalent for “push ebp” is “push rbp”. The equivalent of “mov ebp, esp” is “mov rbp, rsp”.

1. What are the differences between "Microsoft x64 calling convention" and "System V AMD64 ABI calling convention”? (2 points).

**Answer:** A shadow space is not provided in the System V AMD64 ABI unlike the Microsoft calling convention. The return address is adjacent to the seventh integer argument on the stack upon function entry.

1. Upon entry to myFunction (above), what does the stack look like when using Microsoft x64 calling convention? (3 points)

**Answer:** When using Microsoft x64, a is in rcx, b is in rdx, ci is in R8, d is in R9, and e and f are passed on stack.

1. Upon entry to myFunction (above), what does the stack look like when using stdcall convention (3 points)

**Answer**: When using stdcall convention, registers EAX, ECX, and EDX are designated for use within the function. The return values are stored in the EAX register.