Assignment 9

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

The set of information for a specific procedure/subroutine that is either currently being, or has yet to be, executed to the point of a return statement. Multiple stack frames can exist at the same time as part of the Call Stack.

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

A Calling Convention is a means for a section of code that has been called into the main area of the code in order for it to receive passed parameters, how memory is allocated for those passed parameters, which registers must have their information preserved for the calling code, and how to prepare and restore information between the caller and callee.

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

To save the previous stack frame.

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

"push rpb" and "mov rpb,rsp"

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

x64 uses the RCX, RDX, R8, R9 registers for the first 4 integer or pointer arguments and XMM0, XMM1, XMM2, XMM3 for floating point arguments. System V holds the first 6 arguments and so it also uses the RDI and RSI registers for integer and floating point arguments, and the XMM4, XMM5, XMM6 and XMM7 for floating point arguments.

> void myFunction(int a, int b, int c, int d, int e, int f) {

> //some code here

> }

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

Parameters “e” and “f” are passed onto the stack.

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

Parameters “a” and “b” are passes onto the stack.