**Homework - Buffer Overflow**

**Total = 50 points**

**Instructions:**

* Each new question should start from a new page. Pls copy-paste the question before your response.
* Although you can work in a group, the final submission is an individual assignment.
* Simple and clear arguments or comments in Bullet points about the solution Well-labeled block diagram as and when required
* Keywords are highlighted/underlined
* Please, submit a typed response. Handwritten response is unacceptable.

Pls follow above policies, otherwise you will lose 10% for each violation.

For questions 1 and 2, assume that the size of char, int and float are 1 byte, 2 bytes and 4 bytes respectively:

1. Draw TWO separate stack diagrams for the stack contents for the following sample C Code: (10 points)

void func (int a, int b){ <------------ Instruction Pointer position # 1

char buffer[5];

int c;

c = a + b; <------------ Instruction Pointer position # 2

}

void main(){

func(1, 2);

}

func

main

return

b

a

prologue

func(1,2)

start



func

main

func(1, 2)

a

b

return

sfp

Buffer

(5 bytes)

c

start

1. Draw the stack diagram for the stack contents for the following sample C Code: (5 points)

void func (char a, int b, float c){

char buffer[8];

int x;

int y;

x = a\*2 ; <------------ Instruction Pointer position

}

void main(){

func(1, 2);

}

**It wouldn’t send to the function without proper arguments.**

func

main

func(1,2)

start

1. Given the following C-code: (5 points)

char destination[4]; char \*source = “CY201”

* 1. What is the anticipated output for the C language string functions – strcpy, strncpy and strlcpy? (3 points)

strcpy(destination, source) will copy everything “CY201\0”.

However, this will cause a buffer overflow due to destination’s size of 4.

strncpy(destination, source, n) will copy up to n characters from the source.

E.g: strncpy(destination, source, 3) will copy “CY2” without the null terminator.

strlcpy(destination, source, n) will copy n – 1 characters and add null terminator.

E.g: strlcpy(destination, source, 3) will copy “CY\0”

* 1. Which is the safest function to use from the above options? Explain. (2 points)

**strlcpy will be the safest. It will add the null terminator that creates the most safety in any situation. Without this, the string can overflow because it doesn’t know when to terminate.**

1. Explain the purpose of four different parts of stack during dynamic memory allocation. (5 points)
2. Draw the sequence of events when main function calls ‘multiply (a, b)’ and then multiply function calls ‘add (x, y, z)’. Your diagram should show the different parts of function call and local variables in the stack. (5 points)
3. For the given C-code: (10 points)

void function(char \*str) {

char buffer[8];

strcpy(buffer,str);

}

void main(){

char large str[256];

int i;

for(i = 0; i<255; i++){

large str[i] = ‘A’;

}

function(large str);

}

* 1. What is the anticipated output when large string buffer size in the main function is the same as the local variable buffer size in the function func\_sample()? (3 points)
  2. What is the anticipated output when large string buffer size in the main function is much greater than the local variable buffer size in the function func\_sample()? (3 points)
  3. The SP address can be higher or lower as compared to the IP address. Under which of these circumstances can we avoid the above problem? (2 points)
  4. With a diagram, show the location of an embedded canary to avoid problem in (b) above. (2 points)

1. Truths and misconceptions about virus: Mark as true or false AND justify the following statements with appropriate explanation (1-2 sentences): (10 points)
   1. Viruses can modify “hidden” or “read-only” files
   2. Files only appear in executable files
   3. Viruses cannot remain in memory when power is off
   4. Viruses cannot infect hardware
   5. Viruses can be malevolent, benign or benevolent