Question 1 ***61C Rev*** [illegible] ()

Comfort with mani[illegible] umber representations covered in 61C will help you succeed in the memory safe[illegible]

Q1.1 What is the he[illegible] decimal number 18?

Q1.2 What is the value of `0x8339e833 + 0x20` in hexadecimal form?

Q1.3 What is the value of `0x550ecdf2 + decimal 16` in hexadecimal form?

Q1.4 What is the largest unsigned 32-bit integer? What is the result of adding 1 to that number?

Q1.5 What is the largest signed 32-bit integer? What is the result of adding 1 to that number?

Q1.6 If you interpret an n-bit two's complement number as an unsigned number, would the negative numbers be smaller or larger than positive numbers?

Q1.7 How many bytes are needed to represent char[16]?

Q1.8 How many bytes are needed to represent int[8]?

Q1.9 **For the follo**[...]**me each block is 1 byte, and addresses increase from left-to-right** [...]

In a little-endi[...]would you represent the pointer `0xDEADBEEF`?

Q1.10 In a little-endian 64-bit system, how would you represent the pointer `0xDEADBEEF`?

Q1.11 In a little-endian 32-bit system, how would you represent the char array "ABCDEFGH"?

Question 2 ***Stack Diagram Practice*** ()

Here are the 11 steps for x86 calling convention for reference:

1. Push arguments onto the stack.
2. Push the old [illegible] onto the stack.
3. Move eip.

   Execution cha[illegible]
4. Push the old [illegible] (push %ebp)
5. Move ebp do[illegible]
6. Move esp down.
7. Execute the function.
8. Move esp up. (mov %ebp, %esp)
9. Restore the old ebp (sfp). (pop %ebp)
10. Restore the old eip (rip). (pop %eip)
11. Remove arguments from the stack.

Consider the following function.

```c
int swap(int* num1, int* num2, int arr_local[]) {
    int temp = *num1;
    *num1 = *num2;
    arr_local[0] = *num1;
    *num2 = temp;
    arr_local[1] = *num2;
    return 0;
}

int main(void) {
    int x = 61;
    int y = 1;
    int arr[2];
    swap(&x, &y, arr);
    return 0;
}
```

Q2.1 Draw the stack diagram if the code were executed until a breakpoint set on line 4. Assume normal (non-malicious) program execution. You do not need to write the values on the stack, only the names. When drawing the stack diagram, assume that each row in your diagram doesn't have to represent 4 bytes in memory. The bottom of the page represents the lower addresses.

Stack

Q2.2 Now, draw arrows on the stack diagram denoting where the ESP and EBP would point if the code were executed until a breakpoint set on line 4.

Q2.3 The return instruction executes steps 8-10 of the calling convention. Draw arrows on the stack diagram denoting where the ESP and EBP would point for each of these steps.

Question 3 ***Security Principles*** ()

We discussed the following security principles in lecture (*or in the textbook*):

A. *Know your threat model:* Know your attacker and their resources; the security assumptions originally made may become invalid

B. *Consider human factors:* Security systems must be usable by ordinary people

C. *Security is economics:* Perform a cost-benefit analysis, since adding security usually costs more money

D. *Detect if you can't prevent:* If one cannot prevent an attack, one should be able to at least detect when an attack happens

E. *Defense in depth:* Layer multiple defenses together

F. *Least privilege:* Minimize how much privilege you give each program and system component

G. *Separation of responsibility:* Split up privilege, so no one person or program has complete power

H. *Ensure complete mediation:* Make sure to check *every* access to *every* object

I. *Consider Shannon's Maxim:* Do not rely on security through obscurity

J. *Use fail-safe defaults:* If security mechanisms fail or crash, they should default to secure behavior

K. *Design in security from the start:* Retrofitting security to an existing application after it has been developed is a difficult proposition

Identify the principle(s) relevant to each of the following scenarios:

Note that there may be more than one principle that applies in some of these scenarios.

Q3.1 New cars often come with a valet key. This key is intended to be used by valet drivers who park your car for you. The key opens the door and turns on the ignition, but it does not open the trunk or the glove compartment.

Q3.2 Many homeowners leave a house key under the floor mat in front of their door.

Q3.3 It is not worth it to use a $400,000 bike lock to protect a $100 bike.

Q3.4 Warranties on cell phones do not cover accidental damage, which includes liquid damage. Unfortunately for cell phone companies, many consumers who accidentally damage their phones with liquid will wait for it to dry, then take it in to the store, claiming that "it broke by itself". To combat this threat, many companies have begun to include on the product a small sticker that turns red (and stays red) [illegible]

Q3.5 Social security [illegible] iginally designed as a secret identifier. Nowadays, they are often easily ob[illegible]

Q3.6 Even if you use a password on your laptop lock screen, there is software that lets a skilled attacker with specialized equipment bypass it.

Q3.7 Shamir's secret sharing scheme allows us to split a "secret" between multiple people so that all of them have to collaborate in order to recover the secret.

Q3.8 DRM encryption is often effective until someone can reverse-engineer the decryption algorithm.

Q3.9 Banks often make you answer your security questions over the phone. Answers to these questions are "low entropy", meaning that they are easy to guess. Some security-conscious people instead use a random password as the answer to the security question. [a] However attackers can sometimes convince the phone representative by claiming "I just put in some nonsense for that question".

[a] Q: "What is your dog's maiden name?". A: "60ba6b1c881c6b87"

Q3.10 Often times at bars, an employee will wait outside the only entrance to the bar, enforcing that people who want to enter the bar form a single-file line. Then, the employee checks each individual's ID to verify if they are 21 before allowing them entry into the bar.

Q3.11 Tesla vehicles come equipped with "Sentry Mode" which records footage of any break-ins to the vehicle and alerts the vehicle owner of the incident.

Q3.12 When a traffic [illegible]y be giving conflicting signals, it enters a state of error and displays a flash[illegible]ections.