CS 628A: Background Evaluation Pop Quiz: Solutions

Instructor: Pramod Subramanyan

7 Jan 2019 (16 points/12 minutes)

Due: 11:59 PM on 8 Jan 2019 @ Moodle

Answers are the options shown in **bold.** We've also provided a brief explanation of the answer. Some of these answers contain further exercises. It is recommended that you do those exercises.

---

1. In the following C program, where is the field `data` referred to in `stk->data` stored?

```
struct stack_t {
  int data;
  struct stack_t* prev;
};

struct stack_t* foo() {
  struct stack_t *stk = malloc(sizeof(struct stack_t));
  stk->data = 52;
  stk->prev = NULL;
  return stk;
}

int main() {
   struct stack_t *stk = foo();
   printf("data=%d\n", stk->data);
   return 0;
}
```

   (a) The stack
   (b) The heap
   (c) In the data segment
   (d) In the initialized data segment

   Explanation: malloc always allocates memory on the heap.

   Further Reading: Is there a C standard library function that allocates data from the stack? What is this function called and how does one deallocate the memory returned by it?

2. Suppose the program shown in question 1 is executed. Which of the following statements about its execution is **incorrect**?

   (a) The program could crash due to a segmentation fault.
   (b) The program could print 52 and exit.
   (c) If the call to malloc fails, the program is guaranteed to crash.
   (d) The program does not invoke a system call.

Explanation: (a) is possible (although very unlikely); the program could crash due to the malloc invocation in foo returning NULL. (b) is clearly possible. (c) is actually true, because the page corresponding to address 0 is always unmapped so the program is guaranteed to crash if malloc fails. (d) is the one that is wrong because the program calls printf which will eventually invoke the write system call.

3. What does the abbreviation "so" in libc.so.6 represent?

   Answer: shared object

   Explanation: shared objects are also called dynamically linked libraries.

4. Can I write a (user space) program that prints out the string "hello, world!" without linking to or invoking the C standard library?

   (a) Yes
   (b) No

   Explanation: Yes, of course. You could directly invoke the write system call using (for example) inline assembly. It is a good exercise to write the above program which prints "hello, world" without invoking printf/puts etc. and instead invokes write directly.

5. Can I write a (user space) program that prints out the string "hello, world!" without making a system call?

   (a) Yes
   (b) No

   Explanation: No, the only way a user space program can produce output on the screen is by invoking a system call.

6. Suppose two processes word.exe and excel.exe are executing concurrently. If the stack in excel.exe is continuously growing due to an error in a recursive algorithm, this stack could eventually overwrite the heap of word.exe, and thereby cause a buffer overflow attack.

   (a) True
   (b) False

   Explanation: No, the address spaces of programs are isolated from each other. So memory safety errors in one cannot (usually – there are a few exceptions) affect the other.

   Further reading: Read about how two processes can share memory with each other. Try to write two programs that share memory, and create an error in one that causes the other to crash.

7. What does the following assembly language program do?

```
mov  ebx,0
mov  edx,1
mov  ecx,10
```

```
L1: mov  eax,ebx
    add  eax,edx
    mov  ebx,edx
    mov  edx,eax
    dec  ecx
    jnz  L1
```

(a) Sum the integers from 1 to 10.
(b) Sum the integers from 1 to 9.
(c) Compute the Fibonacci sequence.

Explanation: ebx is initially 0, edx is initially 1 and the loop counter ecx is 10. After each iteration, the new value of ebx is edx and the new value of edx is ebx + edx. This is clearly the Fibonacci sequence.

8. The wireless network iitk is an open network, which means that anyone can eavesdrop on data being sent over this network. Does this mean that I can read the Facebook messages of all the students who open up their FB account during class?

(a) Yes, but others will also be able to see that I am reading the FB messages.
(b) No, because the proxy gateway.iitk.ac.in encrypts all traffic on the network.
(c) Yes, but if I get caught, I could be prosecuted for violating students' right to privacy.
(d) **No, because FB uses transport layer security**.

Explanation: The FB website and app use TLS. A good discussion of why TLS is used is on Piazza.

9. Even if a web server does not use HTTPS, if I access it using the Tor web browser, all data I send to it and receive from it will always be encrypted.

(a) True
(b) False
(c) Depends on the specific web server (e.g., true for nginx and false for apache).

Explanation: No, the data between the exit node and the web server may not be encrypted.

Further reading: If you are unfamiliar with Tor, looking up some basic resources on the Tor protocol might be useful.

10. Which of the following types of servers does not (usually) require authentication?

(a) SMTP server
(b) POP3/IMAP server
(c) DNS

Explanation: an SMTP server is used to send email and you usually have to login before you send email. POP/IMAP are used to receive email. This also requires you to login.

11. What is the course number for this class?
(a) CS 733

(b) CS 628A
(c) CS 698J
(d) CS 634

Explanation: This was to be found at the top of the document.

12. If an attacker compromises a BGP router and announces a false prefix to its peers, this attacker will be able to:

(a) Read and modify all Gmail traffic going over the intercepted routes
(b) Listen in on all skype calls going over the intercepted routes
(c) Read/modify all torrent data going over the intercepted routes
(d) All of the above

Explanation: BGP routing attacks can force some traffic to go through an adversary's routers. This adversary can potentially read and manipulate all plaintext traffic going over these routers. However, Gmail uses TLS and skype traffic also uses encryption so this traffic can't be manipulated or read by the adversary. However, torrent data is not encrypted and this can be read/modified by the adversary.

Further reading: Find out how Pakistan took down YouTube for the whole world through a mismanaged BGP routing announcement.

13. What happens when a processor encounters a TLB miss while executing an instruction?

(a) A hardware circuit executes a page table walk
(b) A software handler executes a page table walk
(c) Either (a) or (b)
(d) The TLB is filled from the hard drive

Explanation: TLB misses could be handled both software or hardware page table walkers. X86 uses hardware page table walks while some MIPS processors have software page table walks.

14. Which of the following is **not** a public key cryptosystem?

(a) RSA
(b) Elliptic curve cryptography
(c) AES

Explanation: AES is an algorithm for symmetric key (not public key) encryption/decryption.

15. Both a digital signature and a message authentication code (MAC) can be used to verify the authenticity of messages. What makes them different?

(a) Digital signatures are usually computed by hashing the data, while MACs don't involve hashes.
(b) Digital signatures use public key cryptography while MACs do not.
(c) They are not different, just different names for the same thing.

Explanation: MAC ensures authenticity using a secret key, not public key cryptography.

16. A certificate authority in the context of transport layer security (TLS) is a(n):

(a) Entity who issues public/private key pairs for use in signing digital certificates.
(b) Blockchain smart contract that issues certificates of bitcoin balances.
(c) Entity who provides digital certificates that certify ownership of a particular public key.
(d) Database of authentic digital certificates.

Explanation: A certificate authority signs messages saying that a particular public key belongs to a particular entity (e.g., SBI). It does not issue private/public keys – the private key should never be revealed to any one except the owner of the private key.