CS 628A: Background Evaluation Pop Quiz

Instructor: Pramod Subramanyan

7 Jan 2019 (16 points/12 minutes)
Due: 11:59 PM on 8 Jan 2019 @ Moodle

This quiz is meant to help you identify weak spots in your background. Answer the quiz without referring to text books, the internet or talking to other students – the goal of this quiz is to help *you* understand how much of the required background *you* have, if you do any of the above, that purpose will be defeated. Also, everyone is expected to get 100% of the points (see the grading section below), so cheating will only help you cheat yourself as to how much you really know.

We will analyze your responses and give you feedback on what areas to prepare based on your responses.

Instructions: The following are (almost) all multiple-choice questions. There is only one correct option. You need to choose the most appropriate option among the answers provided.

Submission: You will create a text file where the first line is your roll number, the second line is your name and each subsequent line consists of question numbers followed by the answer. In most cases the answer will be a lower-case letter: ‘a’, ‘b’, ‘c’ or ‘d’ (without the quotes). The question number and answer must be separated by a single space (without any other characters). For the fill-in-the-blank question, write out the full answer on the same line.

Grading: You will get 100% of the points for this quiz if you: (a) submit a file which attempts all the questions and (b) answer at least one question correctly.

---

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

```c
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

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.

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

____

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

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

(a) Yes
(b) No

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

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.

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.

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).

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

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

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

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

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

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

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

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

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.

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.