DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY MADRAS

Embedded Systems Engineering (CS6898)

Deadline : 30-10-2024 **Assignment 2**
Max Marks : 30 **01-10-2024**

[Answer all questions]

1. What is the difference between a security vulnerability and an exploit? (2 marks)

2. Consider the following program and answer the questions below. (8 marks)

```
int fact(int x){
  int y;
  y = x * ((x>1)? fact(x-1):1);
  return y;
}

int main(int argc, char **argv){
  return fact(N);
}
```

   (a) This program is compiled for an x86 32-bit Intel processor as follows:

   ```
   gcc -fstack-protector -O0 -o fact.c
   ```

   i. What is the purpose of `-fstack-protector` and `-O0`?

   ii. The output of the compilation is a file called `a.out`, which has the ELF format. What is the full form of `ELF`?

   (b) During execution, the stack and code segments are set to `0x2000` and `0x1000` respectively. Each segment is of 4KB.

   i. Are `0x1000` and `0x2000` virtual addresses or physical addresses?

   ii. What is the initial value of `%esp`?

   iii. Suppose the stack frame for main and all functions that execute before it occupy 256 bytes. What is the maximum value of `N` for which the program works correctly?

   iv. For a value of `N` greater than this maximum value, what is the likely output and why does it occur?

3. Match the following. Choose one best answer from the choices. (3 marks)

(a) W ⊕ X	(i) Enabled mainly by the compiler
(b) Canaries	(ii) Enabled mainly by the Operating System
(c) ASLR	(iii) Prevents execution from certain memory pages

please turn over

4. The course CS1100 at IIT Madras has 4 teachers, 20 TAs, and 400 students. An online platform is used to communicate between the stake holders. Quiz time is very challenging for everyone because of the following rules:

   - Question papers can be created by any of the teachers and viewed by any of the teachers prior to the exam.
   - Question papers become viewable by everyone after the exam.
   - Answer scripts can be viewed by teachers and TAs but not editable by any of them.
   - A student can only view their own answer script and not anybody elses.
   - Grade sheets are editable only by teachers and can be viewed by everyone.

   Assume a Linux based online platform. Start with defining the users, groups, objects, and the access policies. (4 marks)

5. Match each entry in column 1 to *exactly* one best option in column 2 to achieve a policy in a computer system. (4 marks)

Mechanism	**Policy**
[**A**] Hardware Interrupt	[**i**] Isolate OS from user processes
[**B**] CPU rings	[**ii**] Availability of CPU to processes
[**C**] Paging	[**iii**] Memory Buffer Checks
[**D**] Fat pointers	[**iv**] Isolate user processes

6. Find the vulnerability in the following program and describe how you would exploit it. **(4 marks)**

```
int lottery_winner;

int main()
{
        char name[128];
        int guess;

        lottery_winner = random() % 256;

        printf("enter your name : ");
        scanf("%s", name);
        printf("enter your guess: ");
        scanf("%d", &guess);

        printf("Hello ");
        printf(name);
        printf("!\n");
        if (lottery_winner == guess){
                printf("You have won the lottery\n");
        }else{
                printf("You have lost the lottery\n");
        }
}
```

7. Answer in brief. (5 marks)

   (a) Give an example of an entity that can be a subject as well as an object.

   (b) There are several advantages of incorporating access control policies in the hardware. What are the disadvantages?

   (c) Two processes P1 and P2 execute simultaneously in a computer system, what prevents P1 invoking an arbitrary function in P2?

   (d) Each user in a Unix system is assigned a user identifier? How is this number assigned?

   (e) On a Linux server, user U1 belongs to group G1 and user U2 belongs to group G2. User U1 has a directory /home/U1/team and wants to permit U2 to list the files in the directory but not read the contents of any file in that directory. Write the Linux commands by which U1 can achieve this.