

Note: If you are taking the 6 CFU exam you will have 60 minutes, otherwise you will have 120 minutes and you also need to solve part 2 (Prof. Calzavara). Solutions must be uploaded on Moodle in a single PDF file. You cannot use any material besides white paper and a pen. Please do not touch the mouse and keyboard during the exam until you are requested to submit your solution.

Exercise 1 (16 points)

1. What is the purpose of Access Control? (4 points)
2. Briefly describe the four categories of Access Control discussed in class: DAC, MAC, RBAC and ABAC. (4 points)
3. Explain why MAC policies mitigate the consequences of vulnerabilities. Illustrate with an example. (4 points)
4. Consider an application that should regulate access based on user type, resource type, and time of day. What kind of access control policy is the most appropriate and why? Illustrate with an example. (4 points)

Exercise 2 (16 points)

Consider the following fragment of a C program:

```
int f() {  
    char buffer[16];  
    gets(buffer);  
    ...  
}
```

1. Why is this program unsafe? What bug is there? (4 points)
2. Suppose there is no stack protection mechanism in place. Describe an attack that would cause the program to jump to address 0x0000000012345678 in memory. (4 points)
3. Discuss the security mechanisms studied in class that prevent and/or mitigate the attack. (4 points)
4. Provide a code fix that prevents the bug and vulnerability. (4 points)