Security 1

January 28, 2021

Exercise 1 (10 points)

Consider the following fragment of a C program displaying the content of file list.txt:

```
char name[]="list.txt";        // the file to print
char buffer[2];                // buffer for user input

printf("Do you want to show the list? (y/n) ");
gets(buffer);                  // reads user input
if (memcmp(buffer,"y",1)==0)   // if first char of buffer is equal to y
      show_file_content(name); // prints the content of file "name"
```

1. Why is this program unsafe? What vulnerability is present? (3 points)
2. Assume variable `buffer` is allocated right before variable `name`. Sketch the stack layout and describe an attack on the above code that displays the content of file `sec.txt`. (3 points)
3. Explain what *stack canary* is and discuss why it does not prevent the attack. (2 points)
4. Suggest a fix for the program (pseudo-code is fine). (2 points)

Exercise 2 (10 points)

Denial of Service (DoS) attacks are becoming extremely popular and dangerous.

1. What is a DoS attack? What kind of resources does DoS attacks typically target? (3 points)
2. Explain what security property is compromised by DoS, discussing practical examples. (2 points)
3. Illustrate a typical *flooding* attack scenario and explain the role of *source address spoofing*. (3 points)
4. Describe possible defences to DoS attacks. (2 points)

Exercise 3 (10 points)

Access Control regulates the use of resources according to a security policy.

1. Briefly describe the four categories of policies discussed in class: DAC, MAC, RBAC and ABAC. (3 points)
2. Explain why MAC policies mitigate the consequences of malware infections. (2 points)
3. Illustrate the Bell-LaPadula (BLP) policy and explain why it prevents users/malware to directly leak data towards lower security levels. (3 points)
4. Provide a definition of BLP using ABAC. **Hint**: encode security levels as subject/object attributes and define the two predicates `can_read(s,o)` and `can_write(s,o)` in terms of attributes. (2 points)