Security 1

January 14, 2021

Exercise 1 (10 points)

Operating systems security is very important and complex as, among other things, the operating system mediates all accesses from applications to devices and resources.

1. Discuss what is an *attack from below*, in the context of operating system security. (2 points)
2. What aspects are typically considered when planning operating system security? (3 points)
3. Discuss the importance of the *least privilege principle* in the context of operating system security and provide examples of its successful application. (3 points)
4. Why are device drivers typically problematic for what concerns security? Discuss in terms of the least privilege principle. (2 points)

Exercise 2 (10 points)

Network security aims at protecting data transmitted by hosts and applications.

1. Interception is a typical attacker's action on a network. Explain how an ARP spoofing attack makes it possible to intercept packets on a switched LAN. (2 points)
2. What is a *security protocol*? What security properties does it typically provide? What technique is it typically based on? (3 points)
3. Illustrate an example of a security protocol discussed in class, pointing out the adopted techniques and the provided security properties. (3 points)
4. Explain what a Virtual Private Network (VPN) is and discuss in which extent it allows for secure communication, even when applications do not adopt cryptography. (2 points)

Exercise 3 (10 points)

Consider the following fragment of a C program:

```
char buffer[2];                // buffer for user input

printf("Do you want to go back to the main manu? (y/n) ");
gets(buffer);                  // reads user input
if (memcmp(buffer,"y",1)==0)   // if first char of buffer is equal to y
      return 0;                // returns to the calling function
...
```

1. Why is this program unsafe? What vulnerability is present? (2 points)
2. Assume the variable `buffer` is allocated N bytes before the function *return address*. Sketch the stack layout and describe an attack on the above code that would make it possible to jump to an arbitrary address A in memory. (3 points)
3. Explain what *stack canary* is and discuss how it would prevent the previous attack. (3 points)
4. Suggest a fix for the program (pseudo-code is fine). (2 points)