Homework 10

50.520: Systems Security

Side Channels and Trusted Computing

Question 1
Consider the following function for string comparison:

```
def compare(string1, string2):
    if len(string2) != len(string1):
        return False
    for i in range(len(string2)):
        if string2[i] != string1[i]:
            return False
    return True
```

Let us assume that this function is used for password comparison, i.e., for a user input it is called as `compare(real_passwd, user_input)`

- What is the problem with such a system?
- Can you learn anything about `real_passwd` by interacting with the function? (In particular, can you recover the password?) Please demonstrate.
- Propose a fix and demonstrate that it works.

Question 2
Read about two recent attacks, Meldown[1] and Spectre[2]. Report on these attacks, briefly describing how they work, classifying them, and comparing these two attacks (the ways they work, threat models and attack scenarios, consequences of successful exploitations, and mitigations).

[1] https://meltdownattack.com/meltdown.pdf
[2] https://spectreattack.com/spectre.pdf