ECAM
BRUSSELS ENGINEERING SCHOOL

Winter 2020
Sébastien Combéfis

SE507μ Hacking Password Hashes with Rainbow Tables

Mission 1: Secure password hashing

This assessment evaluates the following competencies:

- *CS210 – Understand how passwords can be stored securely in databases* *(+1)*
- *CS205 – Write an application that stores passwords securely* *(+1)*
- *CS109 – Understand what is a cryptographic hash function* *(+1)*

In this mission, you have to find out how to securely hash a password following the Unix scheme (with a salt) with your favourite programming language, and write a small demonstration program that compute a hash for a given password and then checks whether a provided password matches the one stored in the hash. To succeed the mission, you have to:

1. Find how to compute a secure hash to store a password with your favourite programming language.
2. Write the program that computes a hash and then checks a password.
3. Explain to the teacher what you found and how your program works, make him/her a demonstration.

You have to read the documentation of the functions you are using to hash, to find out what is the (cryptographic) function behind it.