CSCE 44303/54203 Homework 7 (Programming)

Release Date: November 19, 2024

Due Date: November 26, 2024

Full Grade: 100 pts

I. Task Description

In this assignment, you will implement dictionary attacks (rainbow attacks) for cracking passwords to understand the use of salt in password storage.

Suppose a system uses N-character passwords, where each character can be a number between 0 and 9, an upper-case letter, a lower-case letter, or a special symbol within set {#, $, %, ^, &, *}. N is a system parameter that the administrator can set (note: when you demo to the Grader, the Grader will choose a small value for N, so that it won't take a long time to test your program).

Part 1: Suppose the system directly stores hash of the passwords in the following format:
[username1, SHA256(password1)]
[username2, SHA256(password2)]
[username3, SHA256(password3)]
Launch dictionary attack to find out all the passwords. Record the time needed.

Part 2: Suppose the system stores salted hash of passwords in the following format:
[username1, salt1, SHA256(password1||salt1)]
[username2, salt2, SHA256(password2||salt2)]
[username3, salt3, SHA256(password3||salt3)]
Here, each salt is a 32-bit random number. Launch dictionary attack to find out all the passwords. Record the time needed.

II. Tests

You need to demo your program to the Grader. A demo sign-up sheet will be distributed to the class later. During the demo, your program will be tested in the following ways.

Test of Part 1: The Grader will send you a text file containing three [username, SHA256(password)] rows, and tell you the value of parameter N. Then your program should print out the recovered passwords and the time needed.

Test of Part 2: Similarly, the Grader will send you a text file containing three [username, salt, SHA256(password||salt)] rows, and tell you the value of parameter N. Then your program should print out the recovered passwords and the time needed.

III. Other Instructions

Programming language requirement: C/C++, Java, or Python. Any other programming language needs instructor approval.

Submit your source code and necessary support files (if any) to Blackboard as a .zip file named in this format: HW7.YourLastName.YourFirstName.zip.