Computer Security
Dept. of Computer Engineering,
Chulalongkorn University.

Activity I : Hacking Password

Created by : Krerk Piromsopa, Ph.D

Overviews

This activity demonstrates the fundamentals of password security. Several hacking techniques will be demonstrated throughout the exercises. In particular, we will learn: brute-force attack, rainbow-table attack, and password analysis.

We will use a free password dictionary from the given url as our dictionary.
https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/10k-most-common.txt

Exercises

1. Write a simple python program to use the word from the dictionary to find the original value of **d54cc1fe76f5186380a0939d2fc1723c44e8a5f7**.
   Note that you might want to include substitution in your code (lowercase, uppercase, number for letter [‘o’ => 0 , ‘l’ => 1, ‘i’ => 1]).
   Hint: Here is a snippet for sha1 and md5 functions.

```
import hashlib
m=hashlib.sha1(b"Chulalongkorn").hexdigest()
print(m)
m=hashlib.md5(b"Chulalongkorn").hexdigest()
print(m)
```

2. For the given dictionary, create a rainbow table (including the substituted strings) using the sha1 algorithm. Measure the time for creating such a table. Measure the size of the table.
3. Based on your code, how long does it take to perform a hash (sha1) on a password string? Please analyze the performance of your system.
4. If you were a hacker obtaining a password file from a system, estimate how long it takes to break a password with brute force using your computer. (Please based the answer on your measurement from exercise #3.)
5. Base on your analysis in exercise #4, what should be the proper length of a password. (e.g. Take at least a year to break).
6. What is salt? Please explain its role in protecting a password hash.