# Access Control Assignment – Post-Cracking Questions

CPSC 348 – Computer Security

Fall 2021

Name: Stella Beemer

*Each of these questions refers to a table in “Password Cracking Results.xlsx”.*

|  |  |
| --- | --- |
| 1. Look at the first table *Salted vs. Unsalted*.    1. Look at the first row. How much time did test case 5 take? Test case 9? What was the percent increase?    2. Similarly, look at the third row. By what percent did the time increase between test cases 7 and 11?    3. Which wordlist was used in cases 5 and 9? Which in cases 7 and 11?    4. Why are attacks using the large wordlist slowed down so much more by salting than attacks using the small wordlist? | a). Case 5 took 0.669 seconds while test case 9 took 0.673 which is about a 0.6% increase  b). The percent increase between 7 & 11 is much larger at 1793.99%  c). The wordlist used in 5 & 9 was the small list, while the one in 7 & 11 is the large list  d). The large wordlist is slowed down more when salted because the number of values that need to be tried has exponentially increased. |
| 1. Look at the table *Small vs. Large Wordlist*.    1. Look at the first row. How much time did test case 1 take? Test case 3? What was the percent increase?    2. Similarly, look at the second row. By what percent did the time increase between test cases 2 and 4?    3. Was word-mangling used in cases 1 and 3?    4. Was word-mangling used in cases 2 and 4?    5. Why are attacks using the large wordlist slowed down so much more by word-mangling than attacks using the small wordlist? | a). test case 1 took 0.6751811 seconds to complete while test case 3 took 0.7536669 seconds. That’s a percent increase of 11.624%  b). There is a percent increase of 447.723% between cases 2 and 4  c). word mangling was not used in cases 1 and 3  d). word mangling was used in cases 2 and 4  e). word mangling slows down the long wordlist more than the slow wordlist because once again, the number of values that need to be tried has exponentially increased |
| 1. Look at the table *Small vs. Large Wordlist.*    1. For each row in the table, how many passwords were cracked with a small wordlist? How many with a large wordlist? What was the increase?    2. What is the average increase across all rows? | a). For the small wordlist test cases, all but the sha-1 unsalted mangling and sha-1 salted no mangling produced 0 cracked passwords. Unsalted mangling resulted in 2 cracked passwords and salted no mangling gave 1. For the large wordlist, test case 3 produced 6, case 4 produced 14, case 7 produced 8, case 8 produced 21, and case 11 produced 6. The increase across the rows is as follows: 6, 14, 8, 19, 5  b). the average increase across all the rows is 10.4 |
| 1. Look at the table *Word-Mangling vs. None*.    1. For each row in the table, how many passwords were cracked with word-mangling? How many with none? What was the increase?    2. What is the average increase across all rows? | a). in order of rows, the number of passwords cracked with mangling is: 0, 14, 2, 21, 1. For those without word-mangling, the order is: 0, 6, 0, 8, 1. The increase across the rows is: 0, 8, 2, 13, 0  b). the average increase across all the rows is 4.6 |
| 1. Based on your answers to the previous two questions, it is more important for an attacker to use word-mangling or have a large wordlist? | Definitely a large wordlist, as the increase is more than double |
| 1. Compare the time to crack test case 11 to that of test case 12.    1. Which took longer? By what percent?    2. How may entries are in “sha1-salted.txt”? How many entries are in “sha1-salted-tiny.txt”?    3. Which wordlist was used in test case 12? Was word-mangling used? Were the hashes salted?    4. Why did test case 12 take so much more time than test case 11, despite having fewer hashes to crack? | a). Test case 12 took longer by a percent increase of 122.401%  b). There are 500 entries in sha1-salted and 25 entries in sha1-salted-tiny  c). In test case 12, the large wordlist was used with word-mangling and the hashes were salted.  d). It took longer because it had to go through the salt and the word mangling, both of which are shown to make john try an exponentially increasing number of possibilities. |
| 1. Compare the time to crack test case 9 to that of test case 13. What is the only difference between the test cases (besides number of passwords cracked and time to crack)? Why does that difference cause such a dramatic difference in the time to crack? | The only difference is the hashing algorithm and it’s because sha512 produces longer hashes compared to sha1, and therefore takes longer to hash. |
| 1. Which three hash algorithms did you crack in this assignment? Which of them are still considered secure today? | We cracked md5, sha1, and sha512 and sha1 and sha512 are still considered secure hashes, although sha1 is quickly getting replaced. |