Flipped Classroom Exercise 3: User Authentication

CS-E3130 Information Security, 19.09.2023

1. Brute-force attacks

Consider an electronic combination lock that accepts a numeric code, and opens if it matches a user-configurable reference value.

1. If codes are four digits...

   a. How many different codes are possible?

   b. If it takes five seconds to try each code, how long will it take, on average, for a single attacker to make before guessing the correct combination?

   c. If there are ten identical locks on the outside of a building, then how long will it take, on average, for ten thieves working together to open all the locks if all the codes are the same?

2. Another type of lock might allow different-length codes.

   a. How many different codes are allowed by a combination lock allowing...

      1. Six-digit codes?
      2. Four- to six-digit codes?

   b. Which is more secure? Six-digit codes only, or four- to six-digit codes? Why?

   c. What security features could make this lock more secure, without degrading user experience?

2. Password cracking

1. What is the entropy of...

   a. a uniformly distributed eight-character alphanumeric password?

   b. a uniformly distributed eight-to-twelve character alphanumeric password?

   c. a uniformly eight-character password, except that it contains at least one letter and one number?

2. How does a salt increase the difficulty of password cracking?

3. How many guesses, on average, does it take to crack ten uniformly-distributed eight-character alphanumeric passwords from...

   a. ...unsalted hashes.

   b. ...salted hashes.

4. How much does it cost to crack the hashes from Q2.4, assuming
   - One GPU can compute 10^9 hashes per second
   - A GPU can be rented for €1/day