Cryptography and Network Security – HW0

Reading Topic: The Tangled Web of Password Reuse

Name: 何秉學 Student ID: R11921A16

Summary

Password security is a critical issue that we may pay attention. However, most people choose easy-remembered strings as their online-service password, which may cause the users to re-used the password as a different online service. Unfortunately, the number of network attacks is increasing, and attackers contain tons of users' information including re-used passwords. They tried to propose a guessing password algorithm including character sequence, deletions, insertion, capitalization, reversal, leet-speak, and substring movement to guess a series of candidate passwords that users may use at different websites according to a set of leaked passwords. Their prototype guessing algorithm is able to crack approximately 10% of the nonidentical password pairs in less than 10 attempts and approximately 30% such pairs in less than 100 attempts.

Strength

- The data set they collect is publicly announced
- The experiment proves that the hypothesis is true, that is, the passwords used by the same user on different websites have a very high similarity, and on the contrary, the passwords used by different people on the same website have very low similarity.
- To connect with the real world, a poll was specially conducted, and the results of the poll were compared with the data of the original experiment, which can strengthen the purpose of this paper.
- For partially identical substrings, our method requires significantly fewer guesses than ED-guesser, thus making the authors' method suitable for online attacks where the number of guesses is limited to a fixed number.

Weakness

- It's hard to guess the totally different and non including sub-string password
- The number of the testing data is quite few

Reflection

- Most of the people(43% in 6077 data) will re-use an identical password for different websites and the rest of the users will just modify part of them. This may cause critical security concerns.
- If I were the core leader of this team, I would connect deep learning and simple cracking algorithm as this paper proposed. My perspective is all passwords used by the same person should have a stronger correlation, so if you can use the general rules that most people will use in the early stage, and when you crack more passwords, you can use them individually for individuals predictors based on their respective modification habits, which should greatly increase the accuracy of predictions.