Review “Guess Again”

Name: Wenhui Zhang
Email: wuz49@ist.psu.edu

Paper Name *:*

Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., ... & Lopez, J. (2012, May). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *Security and Privacy (SP), 2012 IEEE Symposium on* (pp. 523-537). IEEE.

Contribution:

In this paper, Patrick Gage Kelley and other authors propose a technique for evaluation of password strength. They perform a more comprehensive study on password analysis, and show basic16 is superior to comprehensive8 when it comes to scenarios where large numbers of password-guesses are made. The study also shows that dictionary-selection impacts a lot on effectiveness of dictionary check of passwords. Finally authors prove that Shannon entropy could not provide accurate correlation with guess resistance.

Motivation:

There lacks comprehensive evaluation metrics for password strength in research community.

Related works:

Most prior password studies works with small data corpus for password effectiveness analysis. Several studies has done work on evaluating impacts of different password policies based on metrics of entropy or guessability. Studies have shown that Weir’s algorithm is the most effective of all password-cracking techniques.

Methodology:

The first step of this approach is collecting different types of plaintext password data under 8 conditions. These conditions include basic8survey, basic8, basic16, dictionary8, comprehensive8, blacklistEasy, blacklistMedium and blacklistHard, which represent a range of NIST values. Second step of this approach is using different password guessing algorithms, such as Weir algorithm and a variation of the Markov model, to evaluate and compare effectiveness of password guessability.

Results:

This paper compares effectiveness of different password guessing algorithms by effectiveness of password guessability. After evaluation, this paper states that: (1) Shannon entropy is only useful when adversary has opportunity to make large number of guesses; (2) Basic16 is safer than others in attacking-situations with large corpus of password guesses; (3) Choice of close matching training data is crucial to successful cracking of passwords.

Take away:

Effectiveness of passwords setting depends on complexity and weather password creators use rare-in-practice composition policies.