Use of Probabilistic Context-Free Grammars in Password Cracking

Radim Janča, ijanca@fit.vutbr.cz

This presentation will show possible use of probabilistic context-free grammars (PCFG) in password cracking. My PhD study is oriented on the field of IT security, where password security is ever present topic. One of the frequently appearing problems is determination of password when we posses only its hash value. This task usually arises in two cases: recovery of forgotten password or when attacker tries to crack leaked hashes. One of the well known methods how to determine unknown password is dictionary attack. In this case attacker tries passwords from pre-generated dictionary. This attack have higher probability of success than brute force, because users tend to choose word based passwords combined with some word-mangling technique (for example adding numbers after words) rather then random passwords. Time required for password determination depends on the order of passwords in the dictionary. It is desirable that passwords from dictionary are tried in order, beginning with the most probable passwords. These dictionaries are typically created based on passwords leaked on the Internet. However it would be useful if we were able to generate password not only based on leaked passwords but ideally based on the combined probability of password(word) and word-mangling technique. This generation can be effectively done using PCFG. Main goal of presentation is to introduce PCFG and the idea behind the generation of password guessing dictionary.

References

[1] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek. Password cracking using probabilistic context-free grammars. In *Security and Privacy, 2009 30th IEEE Symposium on*, pages 391–405, May 2009.