Usage of Theoretical Computer Science in IT Security

Dominik Breitenbacher

xbreit00@stud.fit.vutbr.cz

Faculty of Information Technology, BUT,
Bozetechova 1/2, 612 66 Brno, Czech Republic

Abstract

In this paper we will discuss the usability of theoretical computer science in security of information technology. There are many ways and possibilities how to use the knowledge of theoretical computer science for making the security more efficient or to show that some security standards or policies can be more vulnerable when the knowledge of theoretical computer science is used.

One of them is password cracking method, which uses probabilistic Context-Free Grammars. The commonly used password cracking techniques are either dictionary-based attacks or brute-force attacks. The brute-force attacks are very time and source consuming, but eventually they are able to find the right password even if the password is not a natural language based word. On the other hand the dictionary-based attacks are able to find the right password very quickly if the password is contained in the dictionary, but it will fail if it is not. So there was presented another password cracking method that tries to take the advantages of both methods and eliminates the disadvantages at the same time. This method generates password structures in highest probability order. At first thanks to the training dataset of disclosed passwords the probabilistic Context-Free Grammar is created. The created grammar then allows to generate rules, and form them, so they can be used for password guesses in password cracking attack. This approach seems to be more effective as compared to traditional methods on real password sets. In one series of experiments, training on a set of disclosed passwords, the approach was able to crack 28% to 129% more passwords than John the Ripper, a publicly available standard password cracking program.

Also Context-Free Grammars are used to guess long passwords which can be sentence-like or phrase-like passwords. There is study about the role of grammatical structures underlying such passwords in diminishing the security of passwords. It can be shown that the results of the study have direct impact on the design of secure password policies, and on password crackers used for enforcing password security. The search space can be decreased due to grammatical structures using an analytical model which is based on Parts-of-Speech tagging by more than 50%.

Furthermore the knowledge of theoretical computer science was utilized for creating authentication protocols based on Context-Free Grammars using one-time authentication information. This information can be used for generation of one-time passwords. The protocol requires that the Context-Free Grammar is difficult to learn. It means that the learning algorithms are not able to tell if the given string belongs to the language which is generated by the chosen grammar. So if the one-time password is a long string concatenated of strings of independent grammars, for attacker is very difficult to reconstruct the individual strings.

These examples and another methods and techniques providing security in IT that use knowledge of theoretical computer science will be discussed and described closely in this paper. Moreover some proofs will be made to show that the presented method or technique is secure enough to be trusted. Finally the advantages and disadvantages of individual methods will be discussed and some new ideas how to solve some issues will be presented.