Information Security Group

Université catholique de Louvain, B-1348 Louvain-la-Neuve, Belgium

---

Proposal 2010-04: TTIFA: Time-memory Trade-off Implementation First Aider

[http://sites.uclouvain.be/security/internship.html]

Level: Bachelor thesis. Can be adapted to a Master thesis. In the latter case, some theoretical improvements on the TMTO will be considered.

Keywords: Time-memory Trade-off, Cryptography, Complexity, Attacks.

Requirements: The student candidate for this thesis should have a very good background in C and not be afraid by mathematical formulas.

Theory: 
Practice: 

Abstract:

Many cryptanalytic problems can be solved in theory using an exhaustive search in the key space, but are still hard to solve in practice because each new instance of the problem requires to restart the process from scratch. The basic idea of a time-memory trade-off (TMTO) is to carry out an exhaustive search once for all such that following instances of the problem

become easier to solve. Thus, if there are N possible solutions to a given problem, a time-memory trade-off can solve it with T units of time and M units of memory. In the methods we are looking at, T is proportional to N^2/M^2 and a typical setting is $T=M=N^{2/3}$.

Cryptanalytic time-memory trade-offs have been introduced in 1980 by Hellman and applied to DES. Given a plaintext D and a ciphertext C, the problem consists in recovering the key K such that $C=E_K(D)$ where E is an encryption function assumed to follow the behavior of a random function. Encrypting D under all possible keys and storing each corresponding ciphertext allows for immediate cryptanalysis but needs N elements of memory. The idea of a time-memory trade-off is to find a trade-off between the exhaustive search and the exhaustive storage. For that, an exhaustive search is carried out once (precomputation) and only a subset of generated values is kept. In 2003, Oechslin introduced the trade-off based on rainbow tables and demonstrated the efficiency of his technique by recovering Windows passwords.

TMTO could be used in practice to solve many problems, especially in cryptography. Unfortunately, implementing an efficient TMTO is quite difficult and requires strong knowledge of the domain. Indeed, determining the correct parameters of the trade-off implies heavy and complex calculations. The goal of this thesis is to provide an efficient parametrizable generic implementation of TMTO that puts this technique within everyone's capabilities. The tool will have to evaluate the best parameters, precompute the tables, and offer an interface for on-the-fly uses. Its performances will be eventually compared with the ones of the best Windows password cracker, Ophcrack.

Further readings: Candidates for this thesis should have a look at the website OphCrack and should read the following papers: Hellman 1980, Oeschlin 2003, Avoine-Junod-Oechslin 2008. An introductive presentation is also available here.

Contact
Information Security Group
UCL / INGI / GSI
Place Saint Barbe, 2
Building Réaumur
B-1348 Louvain-la-Neuve
Belgium

Gildas Avoine
gildas.avoine@uclouvain.be