Information hiding algorithms
(doctoral dissertation)

mgr. inż. Tomasz Strumiński

Abstract

In the modern world we are surrounded with different kinds of information systems – they play an important role not only in our proffessional life but also in private one. As we store more and more data in these information systems, we are exposed to a wide range of attacks on the security of our data.

Computer security usually means: confidentiality, authenticity, integrity or availability of data. This dissertation is devoted to some specific aspects of confidentiality – i.e. information hiding. Three particular scenarios were considered in the context of providing methods for information hiding, namely: data deletion from storage media, releasing samples from a database and outsourcing the database to a third party. Security issues in these scenarios cannot be addressed with standard cryptographic techniques like encryption. All proposed methods for achieving security were investigated in terms of *provable security* Firstly formal and realistic threat models had been constructed. Afterwards, they were used to prove that presented methods guarantee security.

This dissertation consists of three main parts.

The first part is focused on secure (i.e. irreversible) deletion of data from a magnetic hard drive. In this, it is assumed that after applying the data deletion algorithm, the hard drive is taken over by a well-equipped attacker, whose goal is to recover seemingly deleted data. The beginning of this part reviews the physical properties of storing data on a magnetic hard drive. This analysis helped to understand why the attacker might be able to recover the already overwritten data. With this knowledge it was possible to introduce a special encoding and propose some data deletion methods together with the analysis of their performance in two different threat models. All considerations were performed using a mathematical model of data storage – suggested methods of data deletion are therefore provably secure.

In the next part of the dissertation investigates the problem of preserving privacy of individuals when releasing statistical samples from databases. Two successful attacks on anonimized database samples were a motivation for considering this scenario. It turned out that those attacks were possible because of auxiliary information and the feasibility of linking them to anonimized samples. To avoid similar threats, the definition of so called *differential privacy* has been used. This definition provides privacy guarantees and is immune to attacks based on auxiliary information. For a given database, it has been shown how to calculate the probability which can be used for privacy preserving (in terms of differential privacy)

random sampling. This part of the dissertation improves the results from K. Chaudhuri's and N. Misra's work presented on CRYPTO 2006.

The last part of this dissertation is dedicated to security analysis of a PIR scheme (*private information retrieval*) proposed by Y. Yang, X. Ding, R. H. Deng and F. Bao. Their scheme can be used to solve the problem of secure database outsourcing to an untrusted third party. Security in this scenario, stands not only for confidentiality of the data stored in the outsourced database, but also privacy of its users. It has been shown that a basic construction of mentioned scheme is secure under very strong privacy property, whereas the extended construction, efficient in terms of storage requirements, is prone to attacks on user's privacy.

In addition to aformentioned results, some auxiliary parts containing summaries of related work and description of mathematical background were presented.

This dissertation is based on four already published articles:

M. Klonowski, M. Przykucki, T. Strumiński Data Deletion with Provable Security. Presented on International Workshop on Information Security Applications – WISA 2008, Lecture Notes in Computer Sciences 5379, Springer Verlag, pp. 240-255.

M. Klonowski, M. Przykucki, T. Strumiński Data Deletion with Time-Aware Adversary Model. Presented on The 2009 IEEE/IFIP International Symposium on Trusted Computing and Communications – TrustCom 2009, IEEE Computer Society, pp. 659-664.

M. Klonowski, M. Przykucki, T. Strumiński, M. Sulkowska Practical Universal Random Sampling. Presented on International Workshop on Security – IWSEC 2010, Lecture Notes in Computer Sciences 6434, Springer Verlag, pp. 84-100.

Ł. Krzywiecki, M. Kutyłowski, H. Misztela, T. Strumiński Private Infromation Retrieval with a Trusted Hardware Unit – Revisited. Presented on China International Conference on Information Security and Cryptology – INSCRYPT 2010, Lecture Notes in Computer Sciences 6584, Springer Verlag, pp. 373-386.