Emerging Database Security Solutions

Goals

Emerging Database Security Solutions is a follow-up project to the “Next Generation Database Security” study, which was carried out in 2008. It aims at further research and development in three different areas and consequently inventing innovative database security solutions.

Description

Design secure database applications: System developers tend to neglect security requirements or to only deal with them at the end of the development process. There is no way to verify that security requirements are defined, validated and implemented. The project of developing Security Method and Tool within the scope of Emerging Database Security Solutions is intended to address these problems by developing a methodology and a supporting software tool that will force developers, in particular the database designers, to deal with database security requirements related to authorization in the early stages of development.

Anonymize exported data: Data holders have an obligation to protect a respondent’s identity when releasing data about individuals. K-Anonymity is a model of protecting exported data in which each piece of disclosed data is equivalent to at least k-1 other pieces of disclosed data over a set of attributes that are deemed to be privacy sensitive. Existing K-Anonymity solutions either suffer from inefficiency, insufficient quality of preserved data, scarce data or the method requires prior domain knowledge to allow application to different databases. The new K-Anonymity algorithm shall correspond to designated requirements.

Smart database audit: Currently users usually receive a pooled connection to the database when accessing the database via a web server. It appears to the specific database that such a connection is always established by the same user (the web server itself). The Emerging Database Security Solutions project intends to develop a method called “Smart database audit” which enables the identification of the real user by the database. Identifying the real user by the database results in better logs, which entails better intrusion detection and prevention.