

Provably Secure Optimisation of Database Queries under Fine-Grained Access Control

Stanley Clark

Eindhoven University of Technology

`s.clark@tue.nl`

Security-aware query processing aims at the secure evaluation of queries under access control. Ideally, a security-aware query evaluation algorithm should ensure that access control policies are enforced correctly and that their introduction does not affect performance. Unfortunately, commercial systems fail to meet these criteria, potentially leaking sensitive data. In this presentation, we present a proposal for a prototype *security-aware query optimiser* for an expressive fragment of the relational algebra. To this end, we introduce *sec-RA*, a security-centric extension to the relational algebra. We present our analysis of existing methods for policy enforcement in the context of *sec-RA* with respect to their security and establish how to obtain a provably secure baseline query plan. Further, we introduce specialised query rewrites based on the *sec-RA* operators that can be used for query optimisation while preserving security guarantees. We present the results of extensive experiments on a widely used benchmark dataset using our prototype optimiser thus demonstrating the effectiveness and viability of our approach .