Understanding and Enforcing Disjunctive Policies in Database-backed Programs

Amir M. Ahmadian

ahmadia@kth.se

KTH Royal Institute of Technology

Abstract

Database security and information flow security have traditionally been separate fields, even though they share similar foundations and enforcement mechanisms. Modern applications often rely on shared database backends to provide reliable storage to a variety of users. However, the complexity of database query languages, which nowadays resemble a full-fledged programming language, questions the adequacy of traditional database access control models. As a result, it is necessary to reconcile these two areas, both in terms of foundations and security mechanisms.

This study aims to advance this goal by examining disjunctive policies in database-backed programs. A disjunctive policy represented as P_1 or P_2 capture a scenario where a piece of data may depend on either P_1 or P_2, but not both. Such dependencies occur naturally in programs that interact with databases, where security policies may specify a range of exclusive choices to constrain the information disclosed to an external observer. An example is a gift card application that enforces a disjunctive policy, allowing users to buy any subset of items provided that the total cost does not surpass the value of the gift.

In this work we set out to answer the following key questions:

1. How to develop a semantic model to express disjunctive dependencies in database-backed programs?
2. How to enforce disjunctive policies in database-backed programs?

We develop security models to understand the semantics of disjunctive dependencies and security policies in database-backed programs, and proposes a range of provably-sound static enforcement mechanisms to check these disjunctive policies.

This is a joint work with Matvey Soloviev and Musard Balliu.