Inference-proof view update transactions with forwarded refreshments

Kolloquiums-Vortrag zum Thema Datenbank-Sicherheit

Prof. Dr. Joachim Biskup
Technische Universität Dortmund

Inference control aims at disabling a participant to gain a piece of information to be kept confidential. Considering a server-client architecture for information systems, we extend Controlled Query Evaluation (CQE), an inference control method to enforce confidentiality in static information systems under queries, to databases that are updatable by a client.

More specifically, within the framework of the lying approach to CQE, we study how the server should translate a view update request issued by a client into a new database state in an inference-proof way. In order to avoid dangerous inferences, some such updates have to be denied even though the new database instance would be compatible with the set of integrity constraints declared in the schema and supposed to be known to the client. In contrast, seen from the client's point of view some other updates leading to an incompatible instance should not be denied.

We design a control method to resolve this seemingly paradoxical situation and then prove that the general security definitions of CQE, suitably extended to capture both query evaluation and view update processing, and other properties linked to view updates hold. Moreover, we further enhance that control method by adding an inference-proof subprotocol for refreshing the views of the other clients. To ensure inference-proofness, from the other clients' point of view, any view update might be a transaction, i.e., a sequence of elementary updates.