A Model-Theoretic Semantics of the Multilevel Relational Model *

Xiaolei Qian
Computer Science Laboratory, SRI International
333 Ravenswood Avenue, Menlo Park, CA 94025

Abstract

A multilevel relational database represents information in a multilevel state of the world, which is the knowledge of the truth value of a statement with respect to a classification level in a security lattice. We develop a model-theoretic semantics of the multilevel relational modal with tuple-level classification, which formalizes the notion of validity in multilevel relational databases. We also identify the multilevel security constraints that precisely characterize the validity of multilevel relational databases.

1 Introduction

A state of the world could be envisioned as a set of elements linked together by relationships. Information in a state of the world is the knowledge of the truth value of a statement [9], which could be either an elementary fact as "Enterprise is on mission #101 to Rigel" or a general law as "every starship has a unique destination".

A relational database captures a finite set of elements linked together by relationships. Elementary facts are represented as tuples in relations, and general laws are represented as integrity constraints. These are the only information explicitly captured by a relational database, from which implicit information could be derived. For example, from the explicit elementary fact "Enterprise is on mission #101 to Rigel" represented by the tuple "(Enterprise, 101, Rigel)", we could derive the implicit information "there is a starship Enterprise". A relational database is valid if the relations form a model of the integrity constraints [9].

A multilevel state of the world is a state of the world together with a classification mapping: every piece of information — either an elementary fact or a general law — is mapped to a set of classification levels in a security lattice.

*This work was supported by U.S. Department of Defense Advanced Research Projects Agency and U.S. Air Force Rome Laboratory under contracts F30602-91-C-0092 and F30602-92-C-0140.
Information in a multilevel state of the world is the knowledge of the truth value of a statement with respect to a classification level [14], which could be either a classified elementary fact as "it is top-secret that Enterprise is on mission #101 to Rigel", or a classified general law as "it is confidential that every starship has a unique destination".\(^1\)

A **multilevel relational database** with **tuple-level classification** is a relational database together with a **tuple classification scheme**, which maps every tuple in every relation to a set of classification levels in a security lattice, and every integrity constraint to the bottom level in the lattice (i.e., integrity constraints are not classified). The tuple classification scheme of a multilevel relational database is intended to represent the classification mapping of a multilevel state of the world.

Access by processes to a multilevel relational database is controlled by a **security policy**, which is an interpretation of the mandatory access control policies employed in manual systems. A well-accepted security policy is the Bell-LaPadula model [4]. In this model, every process is assigned a clearance level in the security lattice of the multilevel relational database. The security policy has two important properties which ensure that information does not flow down the lattice:

- **The Simple Security Property** A process is allowed a read access to a tuple only if the former's clearance level is identical to or higher than the latter's classification level in the security lattice.

- **The *-Property** A process is allowed a write access to a tuple only if the former's clearance level is identical to or lower than the latter's classification level in the security lattice.

The notion of integrity is problematic for multilevel relational databases. Existing approaches attempt to enforce integrity across multiple classification levels [1, 8, 15]. If a low tuple contradicts some high tuple with respect to the integrity constraints, then allowing both tuples would violate integrity, disallowing the low tuple would introduce a signaling channel — a signal to low users about the existence of the high tuple, and disallowing the high tuple would cause loss of high information. For example, the low tuple "(Enterprise, 102, Rigel)" contradicts the high tuple "(Enterprise, 101, Rigel)" with respect to the constraint "every starship has a unique mission". Disallowing the low tuple would signal to low users that Enterprise is on a high mission. In fact, Burns [1] has noticed that such integrity enforcement is in fundamental conflict with secrecy enforcement: no multilevel relational databases could simultaneously satisfy both integrity and secrecy requirements. This problem is known as **polyinstantiation** in the limited context where integrity constraints consist of key-based

---

\(^1\)The notion of a multilevel state of the world captures the knowledge at various classification levels, but not the **metaknowledge** that relates the knowledge at multiple classification levels, such as the polyinstantiation and referential security properties to be introduced in Section 3. Although we provide a characterization of the validity of multilevel relational databases using polyinstantiation and referential security properties, a thorough treatment of such metaknowledge is out of the scope of this paper.