Editor's Preface

Some of the most technically challenging questions in computer science involve optimization: how can one wring the last drop of performance out of a system in the presence of security countermeasures? This question can be asked either by an attacker or a system designer. An attacker of a network wants to minimize the effort needed to downgrade information, by moving it through the network to less-resistant nodes. The fuzzy-time technique introduced to defeat or reduce timing channels in an operating system can itself be defeated by a subtle technique. The designer of a multilevel database management system can optimize the safe concurrency of transaction execution while avoiding covert channels. These are the subjects of the papers in this issue. Addressing them involves classical mathematical techniques. For example, both the network question and the database question are shown to be related to a graph-coloring problem.

In a network, "The cascade vulnerability problem" concerns the propagation of risk due to interconnections between nodes. When the balance between system trust level (measured by, e.g., evaluation class) and acceptable risk depends on the range of security levels resident in a system, network connections can upset the balance by enlarging the range. How can one detect when this anomaly has occurred, and restore the balance by upgrading the trust level of a minimum number of machines? The first problem is the cascade detection problem, and an algorithm is given for it by J. D. Horton et al., that has lower complexity with respect to the number of security levels, in a system where security levels are linearly ordered. The second problem is the cascade correction problem, and it is shown to be NP-complete by reduction from the vertex cover problem for three-colored graphs.

The DEC fuzzy time technique had been introduced to reduce timing channels. With a 20-millisecond mean clock, timing channels were reduced to ten bits per second. In "Modelling a fuzzy time system", Jonathan Trostle devises a scheduler channel that should work at 50 bits per second under the same assumptions. The channel depends on the way that the fuzzy-time system defers I/O requests and completions, and employs an unusual and subtle method for decoding the high-to-low information.

"Achieving stricter correctness requirements in multilevel secure database management systems", by Atluri et al., shows how, and under what conditions, one can simultaneously achieve both freedom from signalling channels, and also the ideal correctness condition for concurrently executing transactions, namely, one-copy serializability. Maximum concurrency is obtained by an analysis of the transaction conflict graph. The paper also supplies a similar analysis for situations where the weaker but less restrictive condition of pairwise serializability is satisfactory. The results of the analysis lead to a transaction ordering that can be enforced by untrusted software running on a commercially available system such as Trusted Oracle that provides levelwise serializability, which guarantees security without the stronger consistency properties.

Jonathan Millen