

**Stony Brook University  
The Graduate School**

Doctoral Defense Announcement

**Abstract**

**From Rules to Efficient Algorithms for Cyber Trust Applications**

By

**Katia Hristova**

Cyber trust applications require correct and efficient algorithms for solving complex analysis problems. We address this challenge by generating efficient algorithms and implementations from high-level specifications of these problems expressed using rules. We use extended Datalog rules to intuitively specify analysis problems in the areas of model checking, information flow analysis, and trust management, and then generate efficient algorithms and implementations systematically from the rules. Our work resulted in new and more efficient algorithms for some problems and new and improved time and space complexity analysis for others.

In the model checking area, we describe an efficient algorithm with improved complexity analysis for linear temporal logic model checking of pushdown systems. This model checking framework can express and check many practical properties of programs, including many dataflow properties and general correctness and security properties. For secure information flow analysis, we describe the development of the first linear-time algorithm for inferring information flow types of programs for a formal type system. We also extend the algorithm with informative error reporting to facilitate error detection and corrections. In the area of trust management, we describe efficient algorithms for analysis of trust management policies specified in SPKI/SDSI, a well-known trust management framework designed to facilitate the development of secure and scalable distributed computing systems. Our approach of expressing policy analysis problems as rules is much simpler than previous techniques, in addition to deriving better, more precise time complexities. We show the efficiency of these algorithms by performing precise time and space complexity analysis and confirming them through experiments.

Lastly, we describe a method to generate efficient algorithms for answering rule-based queries. The method is based on the well-known magic set transformation. We apply the method to query problems for graph reachability, as well as in model checking, information flow analysis, and security policy frameworks.

**Date:** October 26, 2007

**Time:** 12:30 p.m.

**Place:** Computer Science, Room 2311

**Program:** Computer Science

**Dissertation Advisor:** Yanhong A. Liu