Title: Understanding and Enforcing Opacity
Authors: Daniel Schoepe, Andrei Sabelfeld
Abstract:
This paper puts a spotlight on the specification and enforcement of opacity, a security policy for protecting sensitive properties of system behavior. We illustrate the fine granularity of the opacity policy by location privacy and privacy-preserving aggregation scenarios. We present a general framework for opacity and explore its key differences and formal connections with such well-known information-flow models as noninterference, knowledge-based security, and declassification. Our results are machine-checked and parameterized in the observational power of the attacker, including progress-insensitive, progress-sensitive, and timing-sensitive attackers. We present two approaches to enforcing opacity: a whitebox monitor and a blackbox sampling-based enforcement. We report on experiments with prototypes that utilize state-of-the-art Satisfiability Modulo Theories (SMT) solvers and the random testing tool QuickCheck to establish opacity for the location and aggregation-based scenarios.