

Enforcing Authorization Policies using Transactional Memory Introspection

Arnar Birgisson, Mohan Dhawan,
Ulfar Erlingsson, Vinod Ganapathy, Liviu Iftode

April 18, 2008

Abstract

Correct enforcement of authorization policies is a difficult task, especially for multi-threaded software. Even in carefully-reviewed code, unauthorized access may be possible in subtle corner cases. We introduce Transactional Memory Introspection (TMI), a novel reference monitor architecture that builds on Software Transactional Memory—a new, attractive alternative for writing correct, multi-threaded software.

TMI facilitates correct security enforcement by simplifying how the reference monitor integrates with software functionality. TMI can ensure complete mediation of security-relevant operations, eliminate race conditions related to security checks, and simplify handling of authorization failures. We present the design and implementation of a TMI-based reference monitor and experiment with its use in enforcing authorization policies on four significant servers. Our experiments confirm the benefits of the TMI architecture and show that it imposes an acceptable runtime overhead.