Title: Refactoring Multi-Layered Access Control Policies Through (De)Composition
Author: Matteo Casalino, Romuald Thion, LIRIS, Université Claude Bernard Lyon 1

Abstract
Policy-based access control is a well-established paradigm for securing layered IT systems. Access control policies, however, often do not focus on dedicated architecture layers, but increasingly employ concepts of multiple layers. Web application servers, for instance, typically support request filtering on the basis of network addresses. The resulting flexibility comes with increased management complexity and the risk of security-relevant misconfiguration when looking at the various policies in isolation. We therefore propose a flexible access control framework able to provide a comprehensive view of the global access control policy implemented in a given system. The focus of this paper is to lay down the theoretical foundations of this framework that allows (i) to describe authorization policies from different architecture layers, (ii) to capture the semantics of dependencies between layers in order to create a composed view of the global policy, and (iii) to decompose the global policy again into a collection of simpler ones by means of algebraic techniques inspired from database normalization theory.

Download the presentation