From Authorization Logics to Types for Authorization

Radha Jagadeesan

School of CTI, College of CDM, DePaul University, Chicago, IL 60604, USA

Abstract. Web services and mashups are collaborative distributed systems built by assembling components from multiple independent applications. Such composition and aggregation involves subtle combinations of authorization, delegation, and trust. Consequently, how to do so securely remains a topic of current research.

Authorization logics elegantly record the change of context from sender to receiver when messages are transmitted in distributed systems. Such logics are well suited to specify security policies since they satisfy a non-interference property: namely, that the dependencies between the statements of principals arise solely from the user-defined non-logical axioms. Building on the prior work of Abadi, Abadi and Garg, and Garg and Pfenning, we describe a semantic approach to such non-interference results.

Authorization logics constitute the logical foundations of our type-and-effect system for TAPIDO, a calculus of distributed objects. The effects are "object-centric" and record the rights associated with the object. Object effects are validated at the point of creation, ensuring that the security policy permits the creation of the object. When such an object is received, the associated rights, perhaps constrained by provenance information, are delegated as a benefit accrued to the recipient. A TAPIDO program is safe if every object creation at runtime is in conformance with the security policy of the system. Well-typed programs are safe even in the face of dishonest opponent processes that aim to subvert the global authorization policy by creating unauthorized objects.

This talk is based on joint work with Abramsky and joint work with Cirillo, Pitcher and Riely.

G. Ramalingam (Ed.): APLAS 2008, LNCS 5356, p. 255, 2008.