Dynamic Policies Revisited

Amir M. Ahmadian
ahmadia@kth.se

KTH Royal Institute of Technology

Abstract

Information flow control and dynamic policies is a difficult relationship yet to be fully understood. While dynamic policies are a natural choice in many real-world applications that downgrade and upgrade the sensitivity of information, understanding the meaning of security in this setting is challenging. In this presentation we revisit the knowledge-based security condition proposed by Askarov and Chong (CSF'12) to reinstate a simple and intuitive security condition for dynamic policies: A program is secure if at any point during the execution the attacker's knowledge is in accordance with the active security policy at that execution point. Our key observation is the new notion of policy consistency to prevent policy changes whenever an attacker is already in possession of the information that the new policy intends to protect. We use this notion to study a range of realistic attackers including the perfect recall attacker, bounded attackers, and forgetful attackers, and their relationship. Importantly, our new security condition provides a clean connection between the dynamic policy and the underlying attacker model independently of the specific use case. We illustrate this by considering the different facets of dynamic policies in our framework.

We present DynCoVer, a tool for checking dynamic information flow policies for Java programs via symbolic execution and SMT solving. Our verification operates by first extracting a graph of program dependencies and then visiting the graph check dynamic policies for a range of attackers. We evaluate the effectiveness and efficiency of DynCoVer on a benchmark of use cases from the literature and designed by ourselves.

This work is a joint collaboration with my supervisor Musard Balliu.