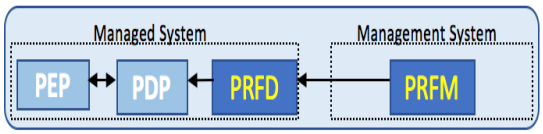
Generative Policy Architecture for Access Control Use Case

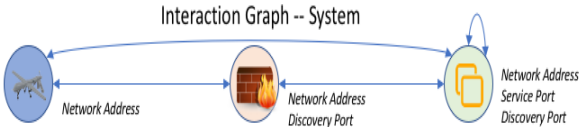
ITA Project & Task Area: Project 2 Task 1, Project 2 Task 2

Contributors: Elisa Bertino (Purdue University), Seraphin Calo (IBM US), Christian Makaya (IBM US), Dinesh Verma (IBM US), Christopher Williams (Dstl)

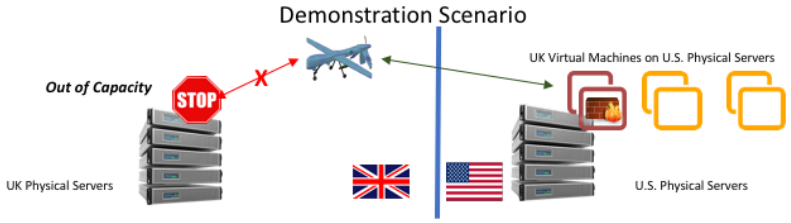
Scope: Policy-based management has been used to simplify the management and operations of complex environments in various domains. However, the current model for policy-based management has the semantics that the machine view of policies is determined by the refinement process, and the managed system has no ability to define its own policies. We proposed a new approach, called *Generative Policy Model*, which allows a flexibility and freedom of actions for the managed systems to determine their own behavior. In this demonstration, we present a coalition environment where the managed systems have the ability to generate their own policies by using the generative policy architecture for the access control scenario in a surveillance coalition mission.

Description: A key concept in the generative approach is that the managed systems have the ability to generate their own operational policies within the bounds of higher level policy structures supporting compliance with overall management constraints. In the generative policy architecture, the policy refinement process (PRF) is separated into two parts, one associated with the global management system (PRFM) and one associated with the managed system (PRFD). The PRFM is responsible for sending the overall coordination guidelines to the PRFD and it provides two types of information to each PRFD: (1) an *interaction graph* (abstract description of the various entities within the environment and contains set of attributes on the links); (2) *policy grammar* (syntax of the policies to be generated locally).





Let's consider a scenario where the US and UK forces are conducting a coalition mission. The UK has the drone for the surveillance, however UK servers are fully utilized, leading the UK requesting VMs on US servers. US has free capacity and can launch UK's VMs with auto-scaling for dynamic resource control. A firewall VM will be launched to restrict the communication only between the UK's drone and VMs running on the US servers. The provided interaction graph and the policy grammar are used by the managed systems to automatically generate their own policies and adjust to the context changes in the environment.



The demonstration shows the automatic policy generation in dynamic environments, without the need of a central configuration or policy server. The approach can be used for various type of scenarios.

Acknowledgement

This research was sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defence under Agreement Number W911NF-16-3-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defence or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon.