

ConfigAssure¹: Dynamic System Configuration Assurance for National Intelligence Community Cyber Infrastructure

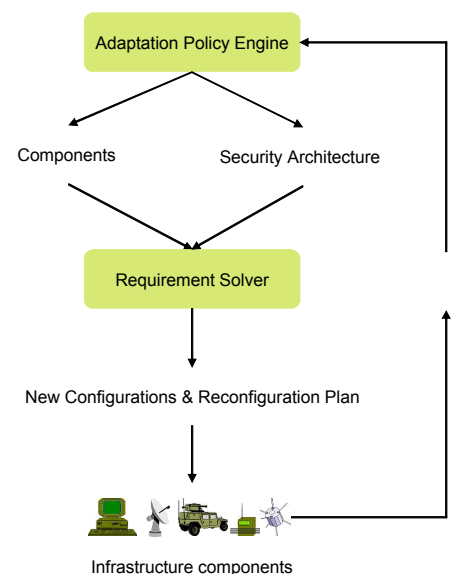
The ability to rapidly, automatically, and correctly reconfigure end-systems and network devices in response to contingencies such as emerging threats, detected attacks, device & system failures, and change in policies & requirements is essential for creating a secure National Intelligence Community (NIC) cyber infrastructure. The demand for real-time reconfiguration is difficult to satisfy today. There are no tools to compose security technologies into a security architecture, to automatically compile the architecture into device configurations, to diagnose and fix configuration errors, and to *safely* change the current configuration to the desired one in real-time. Compounding the challenge is the fact that security cannot, in general, be considered in isolation with other infrastructure properties such as functionality, performance and reliability. There is an inherent tension between these: security is about preventing bad things whereas others are about enabling good things. Incorrect resolution of this tension can disable mission-critical services and potentially cause as much harm as allowing adversary access to those services.

Telcordia and partners MIT and Princeton are developing a system called ConfigAssure to solve the above problem of rapid, automatic, and correct re-configuration of end-systems and network devices. Our metrics for evaluating success are response time: 90% improvement in the speed of reconfiguring security architectures in response to contingencies, accuracy: 90% reduction in security-related configuration errors, and scalability: ability to reconfigure infrastructures with 1000s of components, governed by 100s of requirements. The innovative features of ConfigAssure are:

1. A new Adaptation Policy Engine that allows security administrator to specify just “what” the security architecture is, not “how” it is to be implemented. This architecture takes the form of constraints upon component configuration parameters. The specification language is based upon first-order logic.
2. A new Requirement Solver that automatically computes “how” to configure components to implement a security architecture, and “how” to safely and incrementally move system configuration to the desired state. The Requirement Solver exploits modern constraint solvers based on model-finding for first-order logic and Boolean SAT solvers.

The proposed technology will be evaluated against the above metrics on the DETER testbed or on the infrastructure of a major enterprise. Other suggestions are invited.

For more information, contact Dr. Sanjai Narain at narain@research.telcordia.com, 908-337-3636 (M), 732-699 2806 (I)



¹ The material is based on work supported by the United States Air Force and the Disruptive Technology Office under the Air Force Research Laboratory under Contract Number FA8750-07-C-0030. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Air Force Research Laboratory.