

Trustworthy Enforcement of Domain-independent Runtime Policies

Jay Ligatti, Lujo Bauer, and Adriana Iamnitchi

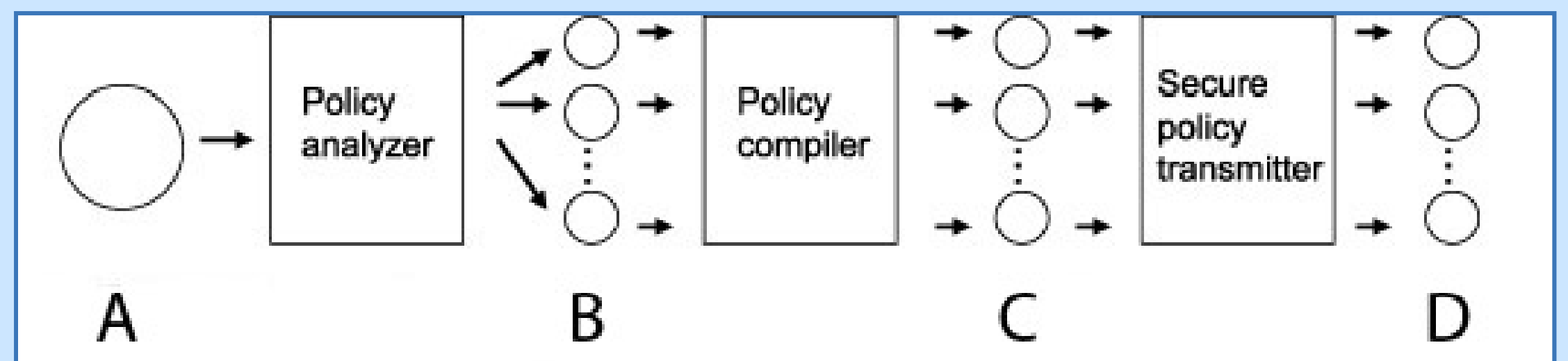
<http://www.cse.usf.edu/~ligatti>

NSF Grants CNS-0716343 and CNS-0716216

Problem and Goal

Despite the pervasiveness and real-world importance of runtime monitors, their use has far outpaced theoretical work that makes it possible to formally and rigorously reason about them and the policies they enforce.

This project aims to develop domain-independent models, tools, and mechanisms for reasoning about and implementing runtime security policies.



Proposed system design: A centrally specified, global security policy (A) is used to derive a set of node-specific policies (B) that together implement the global policy. The node-specific policies are compiled to a format suitable for enforcement (C), and are then securely distributed to the set of nodes on which they are to be enforced (D).

Approach and Impact

New approach

- Formal model of distributed runtime policy enforcement
- Language for specifying global security policies

Research Impact

- Algorithms for trustworthy global-policy enforcement
- Tools for automatically compiling and enforcing runtime policies in distributed systems

Technical Details

Our methodology entails performing four related research tasks:

1. Create a general framework for reasoning about enforcement, permitting the possibilities of concurrent, distributed computations and multi-domain policies
2. Develop a type-safe policy-specification language that will ensure that specified policies compile into well-behaved monitoring mechanisms
3. Design trustworthy algorithms for automatically translating a desired overall policy into node-specific policies that can be distributed and enforced throughout a network
4. Design, implement, and test a prototype system for specifying and enforcing expressive runtime policies with support for concurrently executing computations.

Results

- Created what appears to be the first formal proof of general-monitor uncircumventability for a flexible policy-specification language.
- Performed preliminary research on modeling distributed policy enforcement using cooperating edit automata and policies as predicates on partially ordered executions.