Efficient Web Services Policy Combination

This algorithm serves as the basis for reliable, fast, and automatic network communications.

NASA's Jet Propulsion Laboratory, Pasadena, California

Large-scale Web security systems usually involve cooperation between domains with non-identical policies. The network management and Web communication software used by the different organizations presents a stumbling block. Many of the tools used by the various divisions do not have the ability to communicate network management data with each other. At best, this means that manual human intervention into the communication protocols used at various network routers and endpoints is required. Developing practical, sound, and automated ways to compose policies to bridge these differences is a long-standing problem. One of the key subtleties is the need to deal with inconsistencies and defaults where one organization proposes a rule on a particular feature, and another has a different rule or expresses no rule. A general approach is to assign priorities to rules and observe the rules with the highest priorities when there are conflicts.

The present methods have inherent inefficiency, which heavily restrict their practical applications. A new, efficient algorithm combines policies utilized for Web services. The method is based on an algorithm that allows an automatic and scalable composition of security policies between multiple organizations. It is based on defeasible policy composition, a promising approach for finding conflicts and resolving priorities between rules.

In the general case, policy negotiation is an intractable problem. A promising method, suggested in the literature, is when policies are represented in defeasible logic, and composition is based on rules for non-monotonic inference. In this system, policy writers construct metapolicies describing both the policy that they wish to enforce and annotations describing their composition preferences. These annotations can indicate whether certain policy assertions are required by the policy writer or, if not, under what circumstances the policy writer is willing to compromise and allow other assertions to take precedence. Meta-policies are specified in defeasible logic, a computationally efficient non-monotonic logic developed to model human reasoning.

One drawback of this method is that at one point the algorithm starts an exhaustive search of all subsets of the set of conclusions of a defeasible theory. Although the propositional defeasible logic has linear complexity, the set of conclusions here may be large, especially in real-life practical cases. This phenomenon leads to an inefficient exponential explosion of complexity.

The current process of getting a Web security policy from combination of two meta-policies consists of two steps. The first is generating a new meta-policy that is a composition of the input meta-policies, and the second is mapping the meta-policy onto a security policy. The new algorithm avoids the exhaustive search in the current algorithm, and provides a security policy that matches all requirements of the involved meta-policies.

This work was done by Farrokh Vatan and Joseph G. Harman for NASA's Jet Propulsion Laboratory. Further information is contained in a TSP (see page 1).

The software used in this innovation is available for commercial licensing. Please contact Daniel Broderick of the California Institute of Technology for NASA's Jet Propulsion Laboratory at danielb@caltech.edu.

Refer to NPO-47279.