Enforcing Modular Fine-Grained Security Policies for Untrusted JavaScript in ECMAScript 5

Phu H. Phung

Department of Computer Science and Engineering
Chalmers University of Technology, Sweden

ABSTRACT

We present a mechanism to specify and enforce fine-grained security policies for untrusted JavaScript scenarios. The context of this study is ECMAScript 5 where its new features make possible to create a sandbox environment to load and execute untrusted JavaScript code. The defined policies are enforced on mediator objects, which are virtual versions of original critical objects such as the DOM. The technique to construct mediator objects is ensured that the critical objects are fully mediated with some static policies. The policy definition and enforcement are performed within a sandbox to ensure that the policy code cannot leak the critical objects. The enforced objects are then provided as APIs to untrusted code through a sandbox environment so that the untrusted code can only access the hosting page via interface given by the APIs. We demonstrate the effectiveness of the mechanism by deploying some real-world case studies.