Safe Wrappers and Sane Policies for Self Protecting JavaScript

Jonas Magazinius, Phu H. Phung, and David Sands

Abstract. Phung *et al* (ASIACCS'09) describe a method for wrapping built-in methods of JavaScript programs in order to enforce security policies. The method is appealing because it requires neither deep transformation of the code nor browser modification. Unfortunately the implementation outlined suffers from a range of vulnerabilities, and policy construction is restrictive and error prone. In this paper we address these issues to provide a systematic way to avoid the identified vulnerabilities, and make it easier for the policy writer to construct declarative policies – i.e. policies upon which attacker code has no side effects.