Program Analysis for Web Security

John C. Mitchell

Stanford University

Abstract. The evolving nature of web applications and the languages they are written in continually present new challenges and new research opportunities. For example, web sites that present trusted and untrusted code to web users aim to provide isolation and secure mediation across a defined interface. Older versions of JavaScript make it difficult for one section of code to provide limited access to another, while improvements in standardized ECMAScript bring the problem closer to traditional language-based encapsulation. As a result, rigorous language semantics and acceptable limitations on the language constructs used in trusted code make provable solutions possible.

We have developed sound program analysis tools for specific versions of ECMAScript 5, providing security guarantees against threats from untrusted code in a larger language. However, many security problems remain and there are many ways that future language tools may improve web security and developer productivity.

E. Yahav (Ed.): SAS 2011, LNCS 6887, p. 4, 2011.