John Mitchell
16 mars 2011

Web Security and Untrusted JavaScript

Abstract:

JavaScript is widely used to provide client-side functionality in Web applications. Many contemporary websites incorporate untrusted third-party JavaScript code into their pages in order to provide advertisements, Google Maps, so-called gadgets, and applications on social networking websites.
Since JavaScript code has the ability to manipulate the page Document Object Model (DOM), steal cookies, and navigate the page, untrusted third-party JavaScript code may pose a significant security threat to the hosting page.
This talk will describe some of the security risks, mechanisms that have been used to combat these risks, and new provably correct language-based isolation mechanisms. In addition to realistic subsets of JavaScript that can be used in browsers conforming to the latest language standards, we also discuss a static analysis method that can verify the security of trusted JavaScript code that confines the behavior of untrusted JavaScript running in the same execution environment.

This talk is based on joint work with Ulfar Erlingsson, Sergio Maffeis, Mark Miller, Jasvir Nagra, and Ankur Taly.