

Ninth Annual PARIS C. KANELLAKIS Memorial Lecture



Safety on the Wild and Woolly World-Wide Web: Sandboxing Untrusted JavaScript

John C Mitchell, Stanford University

Thursday, December 3, 2009

at 4:00 PM, Room 368

Thomas J. Watson Sr. Center for Information Technology

Brown University, Providence, RI

Abstract: Many Web-based applications, such as publishers showing advertisements, social networking sites, and online shopping sites combine trusted and untrusted content within the same page. If the untrusted content includes JavaScript code, this code must be prevented from maliciously altering pages, stealing sensitive information, or causing other harm.

This talk will outline some of the practical security problems that have arisen in recent years as a result of combining trusted and untrusted content and describe methods for solving these problems. Using a formal semantics of Ecma-262 Standard JavaScript, we have studied techniques to control untrusted JavaScript code, using Facebook FBJS, Yahoo! ADSafe, and Google Caja as motivating and illustrative examples. We have found that a combination of filtering, rewriting, and library wrapping can provide provably safe methods for displaying advertisements, user-supplied applications, and other active content from untrusted sources. (Joint work with Sergio Maffei and Ankur Taly.)

Lecture Series: This lecture series honors Paris Kanellakis, a distinguished computer scientist who was an esteemed and beloved member of the Brown Department of Computer Science. Paris joined the Department in 1981 and became a full professor in 1990. His research area was theoretical computer science, with emphasis on the principles of database systems, logic in computer science, the principles of distributed computing and combinatorial optimization. He died in an airplane crash on December 20, 1995, along with his wife, Maria Teresa Otoyá, and their two young children, Alexandra and Stephanos Kanellakis.



BROWN