Building Systems that Flexibly Control Downloaded Executable Context

Trent Jaeger and Atul Prakash, University of Michigan
Aviel D. Rubin, Bellcore

Abstract

Downloading executable content, which enables principals to run programs from remote sites, is a key technology in a number of emerging applications, including collaborative systems, electronic commerce, and web information services. However, the use of downloaded executable content also presents serious security problems because it enables remote principals to execute programs on behalf of the downloading principal. Unless downloaded executable content is properly controlled, a malicious remote principal may obtain unauthorized access to the downloading principal's resources. Current solutions either attempt to strictly limit the capabilities of downloaded content or require complete trust in the remote principal, so applications which require intermediate amounts of sharing, such as collaborative applications, cannot be constructed over insecure networks. In this paper, we describe an architecture that flexibly controls the access rights of downloaded content by: (1) authenticating content sources; (2) determining content access rights based on its source and the application that it is implementing; and (3) enforcing these access rights over a wide variety of objects and for the entire computation, even if external software is used. We describe the architecture in the context of an infrastructure for supporting collaborative applications.