Abstract

Ajax is a new model for web applications to provide more responsive and faster user interfaces resembling more closely that of applications. Typical usage areas are user input validation without page submission, integrating small elements from several servers on a single page, and simulating push-services. Especially the latter are promising for enhancing groupware applications and for realizing them directly in browsers without plug-ins or additional software.

The Ajax programming model introduces new security issues, which could be especially dangerous as they were not fully accounted for in previous threat models or considered as of less importance. This paper investigates the security implications of Ajax and discusses possible solutions with a special focus on the context of groupware. It explains security issues which are inherent to the Ajax programming model or are exacerbated through it, and which especially affect cooperative application.