"May I? - Content Security Policy Endorsement for Browser Extensions"

Daniel Hausknecht

Cross-site scripting (XSS) vulnerabilities are among the most prevailing problems on the web. Among the practically deployed countermeasures is a``defense-in-depth'' Content Security Policy (CSP) to mitigate the effects of XSS attacks. However, the adoption of CSP has been frustratingly slow. This paper focuses on a particular roadblock for wider adoption of CSP: its interplay with browser extensions.

We report on a large-scale empirical study of all free extensions from Google's Chrome web store that uncovers three classes of vulnerabilities arising from the tension between the power of extensions and CSP intended by web pages: third party code inclusion, enabling XSS, and user profiling. We discover extensions with over a million users in each vulnerable category.

With the goal to facilitate a wider adoption of CSP, we propose an extension-aware CSP endorsement mechanism between the server and client.
A case study with the Rapportive extensions for Firefox and Chrome demonstrates the practicality of the approach.