Title: Fingerprinting Browser Extensions via Web Accessible Resources
Author name(s): Alexander Sjösten, Steven Van Acker, Andrei Sabelfeld

Browser extensions provide a powerful platform to enrich browsing experience. At the same time, they raise important security questions. From the point of view of a website, some browser extensions are invasive, removing intended features and adding unintended ones, e.g. extensions that hijack Facebook likes. Conversely, from the point of view of extensions, some websites are invasive, e.g. websites that bypass ad blockers. Motivated by security goals at clash, this paper explores browser extension fingerprinting, through an effective, non-behavioral, technique, based on detecting extensions' web accessible resources. We report on an empirical study with free Chrome and Firefox extensions, being able to detect over 50popular security- and privacy-critical extensions such as AdBlock (standard and Pro), LastPass, Avast Online Security, and Ghostery. We also conduct an empirical study of non-behavioral extension fingerprinting on the Alexa top 10,000 websites. Finally, we discuss the dual measures of making fingerprinting easier in the interest of websites and making fingerprinting more difficult in the interest of extensions.