# JavaScript Restrictor

Webextension that improves your privacy and security

## Technical Documentation

***Libor Polčák***

TARZAN project VI20172020062 document
Faculty of Information Technology, Brno University of Technology

Last change: June 25, 2020

## 1 Introduction

JavaScript Restrictor (JSR) is a webbrowser extension supporting Firefox and Chromium-based browsers (we tested Chrome, Opera, Brava, and Edge). The goal of the extension is to protect the user from several attacks performed by JavaScript page scripts, including:

- Using the browser as a proxy to enumerate local network resources. The Firefox version is able to prevent any access from the public network to the local network.
- Timing and architectural attacks using precise timestamps.
- Computing computer clock-skew takes longer.
- Wrapping canvas to limit canvas-based device fingerprinting.
- Information leaks via XML HTTP requests (Ajax).

If you have any of the supported browsers, you can install the extension.

## 2 JSR design

JSR main components are:

- Background scripts maintain the configuration of the extension, update the badge (JSR icon shown by the browser), and perform the Network Boundary Shield (prevent abusing the browser as a proxy).
- Content scripts run at the document start and injects wrappers based on the domain name.
- Pop-up provides the user a way to quickly change settings for a domain.
- Options page lets the user to configure the extension.

The wrappers are described by the wrappers and the wrapping code is generated automatically. The goal is to provide at least a limited protection against the Firefox bug https://bugzilla.mozilla.org/show_bug.cgi?id=1267027. See the developper documentation on how to create a new wrapper.

## 3 Experiments

> TIMKO, Martin. Vylepšení rozšíření pro omezení volání JavaScriptu. Brno, 2019. Master's Thesis. Brno University of Technology, Faculty of Information Technology. 2019-06-20. Supervised by Polčák Libor. Available from: https://www.fit.vut.cz/study/thesis/21824/

Martin Timko evaluated the original architecture of the extension. He evaluated if the extension brakes web pages. He learnt that some web pages were broken. He showed that most of the breakage is caused by the Referrer and User-Agent spoofing. Although user-agent spoofing helps against some fingerprinters, if the fingerprinter observes the inconsistency between user-agent string and the real browser, spoofed user-agent can simplify the fingerprinting. We decided to drop the support for user-agent and Referrer spoofing in the revised extension version.

HORŇÁK, Peter. Přenos bezpečnostních opatření z Chrome Zero do JavaScript Restrictor. Brno, 2020. Bachelor's thesis. Brno University of Technology, Faculty of Information Technology. 2019-06-20. Supervised by Polčák Libor.

Peter Horňák evaluated the revised architecture of the extension that includes the protection from architectural attacks. He shows that the performance impact is negligible and that some web pages can still be broken, mainly due to the wrapping of Uint8Array and DataView.

JIREŠ, Michal. Využití časových značek jazyka JavaScript pro identifikaci počítače. Brno, 2020. Bachelor's thesis. Brno University of Technology, Faculty of Information Technology. 2019-06-20. Supervised by Polčák Libor.

Michal Jireš shows that JSR makes the clock-skew measurements harder. The levels with more aggressive rounding prolong the measurements. The time-randomization prolong the measurements even further. Nevertheless, the time-randomization is more effective when the rounding is to the full seconds because the randomization changes are bigger.

POHNER, Pavel. Detekce podezřelých síťových požadavků webových stránek. Brno, 2020. Master's Thesis. Brno University of Technology, Faculty of Information Technology. 2019-06-20. Supervised by Polčák Libor.

Pavel Pohner evaluated the Network Boundary Shield against local network discovery attack performed by the browser as a proxy. He also compared the extension to uMatrix and NoScript and showed that JSR provides additional protection even to these two well-known security extensions.