Origin Isolation OT Feedback Summary

domenic@chromium.org, 2020-11-11

Overview

The origin trial for origin isolation began in Chrome 84 and runs through Chrome 87.

The main partner for the origin trial was Google Workspace, whose feedback is discussed below. The other token renewals were for the demo site https://origin-isolation-test.com/, and apparently one mistaken renewal that was attempting to test WebNFC.

Specifically, Gmail and Google Chat used the origin trial of the Origin-Isolation header to test the header deployment. We also ran a related Finch experiment with Google Meet. This experiment imposed origin isolation via a different code path (the browser-wide IsolateOrigins feature), which allowed us to start experimenting in Chrome 83 and gather more data to compare with the header's deployment on Gmail/Google Chat.

API feedback

For the header itself, Google Workspace confirmed it was simple and easy to deploy.

Early in the process, Workspace explained that it would be useful to gather telemetry on whether origin isolation had succeeded or not. Originally, this would require indirect observation by performing a prohibited action (such as setting document.domain) and watching it fail or succeed.

In reaction to this feedback, we:

- Added the window.originIsolated getter to allow easy determination of a site's origin-isolation status. (See spec issues #24, #31, and #32 for more discussion.)
- Added console warnings when isolation was prevented due to mismatches among the origin.

Metrics

The majority of our performance and user satisfaction metrics came from the Finch trial with Google Meet. The origin trial with Gmail/Google Chat mostly provided API feedback and bug-finding, and has not yet had a chance to run long enough (without Chrome bugs) to gather significant data from a large population of users.

That said, the initial data from a small population using the Origin-Isolation header origin trial shows no surprises, and gives us confidence that the data from the Finch trial of the IsolateOrigins feature will translate over to the Origin-Isolation header upon launch.

For the metrics themselves:

- **Crash rates:** no significant increase or decrease.
- **Memory usage:** not significantly impacted. There were slightly more renderer processes, but each renderer process used less memory.
- **Frame rates:** a modest improvement in video call frame rates, especially on Chrome OS.
- **User satisfaction:** Chrome OS users saw a modest decrease in "low quality" ratings for video calls. Other OSes saw no significant change.

Bug-finding

It turns out that changing the process model of Chromium is complicated. Testing with real-world customers was invaluable in shaking out some stability bugs with this feature.

In particular, the Gmail team helped us discover:

- crbug.com/1141721: crashes on origin-isolated pages due to incomplete implementation (see especially the summary in comment #6)
- crbug.com/1141877: an Android WebView crash induced by attempts to fix 1141721

Additionally, another tester found a crbug.com/1142894, where we were not respecting the origin isolation header on secure, but http:, URLs, such as http://localhost.