First-Party Sets TAG Discussion

April 2021

Not about SOP

Same Origin Policy

First-Party Sets **does not seek to re-define origin**.

The proposal seeks to define the ***party*** in “third-party contexts”

- Existing security mechanisms that rely on SOP will be **unchanged**
- New privacy mechanisms *may* use First-Party Sets (instead of registrable domains) to determine what is “third-party”

Use cases

Use cases

- **App domains**
  - outlook.com, live.com, microsoft.com
  - lucidchart.com, lucid.co, lucidspark.com, lucid.app
- **Brand domains**
  - amazon.com, audible.com
  - disney.com, pixar.com
- **Country-specific domains** to enable localization
  - google.co.in, google.co.uk
- **Common eTLD**
  - gov.co.uk is on the PSL and has UK government agencies as subdomains which get treated as separate registrable domains by browsers
- **Service domains** that users never directly interact with, but provide services across the same organization’s sites
  - github.com, githubassets.com
  - facebook.com, fbcdn.net
- **Sandbox domains** that users never directly interact with, but exist for security reasons
  - google.com, googleusercontent.com
  - github.com, githubusercontent.com

FPS as the new Privacy Boundary

- Draw a “box” or “boundary” around the collection of domains declared in a first-party set; and restrict information flow across that boundary to prevent cross-website tracking.

- Third-party cookies are one communication mechanism
- They are currently defined as cookies sent in cross-domain contexts
  - “Domain” is a poor substitute for party/website

Scope

New Privacy Features

- SameParty cookies
- Use as top-level “key” for double-keyed cookies and storage
- WebID issues “directed identifiers” that are keyed by FPS
- Privacy Budget applied across an entire FPS

Not a new concept

Prior Art

- The Do-Not-Track specification (developed within the W3C) allowed servers to declare domains that have the same data controller via a "same-party" property to be defined in a file hosted at /.well-known/dnt, and suggested that browsers might enable different behavior across those sets of domains.
- An IETF working group called DBOUND had been formed to allow organizations to declare sets of related domains. There are a couple of related drafts: related domains by DNS, proposal to draw policy boundaries queried via DNS.
- Firefox was already using a static "entities" list that essentially served the same purpose as FPS in their tracking prevention mode (the difference being that this list was an allowlist applied to domains that appeared on their trackers blocklist).
- John Wilander (a Safari engineer) proposed "Affiliated Domains" during a 2017 W3C WebAppSec working group call.

Cross-browser agreement

Support from browser vendors

- John Wilander (Safari) has said “*I‘ve been wanting to solve this for years, as shown by my two pitches of the idea to WebAppSec in 2017, and I really hope we can get to a definition that holds over time as new business decisions are made based on the existence of FPS and that meets user expectations*”
- Maciej (Safari) said “*It does seem that binding strictly to eTLD+1 is not good enough for web privacy features. Driving these issues to resolution is part of why we’d like to see this proposal adopted into a suitable standards or incubation group.*”
- Issues raised by Safari are under discussion in PrivacyCG
  - Desirable elements of “UA Policy”
  - Enforcement against formation of large sets

Support from browser vendors

- Melanie (Edge) expressed support “*we believe that First-Party Sets could be useful in helping unblock valid intra-organizational use cases while maintaining the right privacy promises.*”

First-Party Sets was adopted as a work item in the PrivacyCG in August 2020, and we have been iterating on the design there.

Governance

Governance

- Chrome is interested in developing a common policy that is verified by a independent entity.
- The WebPKI / Baseline Requirements may offer some precedence
    - EV/OV certs have an “Organization” field

Seeking community feedback on GitHub issue

- Desirable elements of “UA Policy”