State of browser privacy evolution

Latest news Jul 27, 2023

Google's Web Environment Integrity API spec and explainer was recently publicized (2023-07-21) . It has garnered negative comment including at this Request for Mozilla Position on an Emerging Web Specification and much press.

This API is presented to assist a destination site in determining whether a browser client represents a real user or a bot.

The explainer contrasts the implementation to the Cloudflare/Apple Privacy Pass work that is now being discussed in an IETF working group. The double blind implementation in Privacy Pass allegedly prevents feedback about errors theoretically making a future exploit of an attestor's implementation harder to manage.

One reaction to the proposal, quoted at The Register:

> *Ondej Pokorný, a freelance technology consultant, offered similar sentiment, via Mastodon. "The problem with many of these new APIs from the whole 'Privacy Sandbox' and other proposals intended to replace 'legitimate' third-party use-cases is that it's turning the browser from a User-Agent into double agent working also in the interest of advertisers and other corporate players, often not aligned with user interests," he argued.*

Some reflection on how Google's ... reCAPTCHA has a dark side points to corporate players vs user interests in this space.

Past news items

For background on standard bodies and their concerns regarding unsanctioned tracking, see [W3C TAG 2015] and [RFC-7258].

We care because authentication protocols strongly resemble the privacy threat called "navigational tracking" including "bounce tracing" and "link decoration." Other privacy and anti-tracking efforts also affect various elements of the higher ed technical infrastructure. This page identifies the term used generally, the threat to users, the mitigations being considered by the browsers, and the impact those have on federated identity systems.

FedCM is one of several additions to browser technology that is designed to allow users to tell browsers that certain cross-site communication – whether through cookies or bounces – is "sanctioned" by the end user. FedCM doesn't block any protocols; FedCM is a way for a user to signal trust to a browser that is otherwise protecting the user's privacy.

This is our focus

As browsers continue to threaten the cross-site methods used in authentication protocols to fight navigational tracking, we see that R&E community investment in testing as a way to have a strong influence in the evolution of these changes. The two issues currently unaddressed by FedCM (were we to use it as a signal to allow SAML protocol transactions) are

1. IdP picking from a list – and the massive scale they need to support for our in our community, – and
2. the hops that are implemented in many authentication flows involving hub federations, federated proxies, and proxies bridging non-compliant IdPs into the federation.

Overview

FedCM

FedCM is one of three APIs that appear to have broad support among the three browser engine teams. Broad support means that it's likely all three will eventually support the standard, not that it is implemented. FedCM was released in Chrome in November 2022, and is also implemented in Edge and Opera (built on the Chrome engine). Firefox has a FedCM project tracker in bugzilla indicating active work. Apple stated in the Webkit developer making list that they are generally supportive.

The specification from the W3C FedId community group is under active development. That community group is working on proposing a W3C working group, which has greater authority; at this point, it is in negotiation where the spec will continue development.

Documentation from browser developers can be found for Chrome and Mozilla. See State of FedCM and SAML for more in depth discussion.

Privacy initiatives

	How does it work	Mitigations	Impact
Navigational tracking	Bounce tracking transfers a user via redirect (or POST) from one site to another, exchanging information in the process. A common pattern is to have "decorated links" that have embedded identifiers for the user.	Safari: Intelligent Tracking Prevention – W3C Privacy CG draft, additional protections when private browsing in Safari 17 – announcement at WWDC23 Firefox desktop: Enhanced Tracking Protection – Mozilla and W3C Privacy CG draft Proposal Draft: when a user has no interaction with a site (at eTLD+1 level), limit cookies to an hour lifetime. **EVOLVING PRACTICE:** FedCM is a possible signal to allow a more aggressive mitigation of bounce tracking while protecting SSO.	Authentication protocols use cross-site redirection with "link decoration" and POST to exchange information about the sites and the user. While SSO is understood as a critical element, it is understood much more as a single bounce, consumer side authentication, without the many bounces to translate across protocls and implementations, nor is there understanding the trust models and authorization elements involved. This is the main focus of REFEDS Working group interaction with the W3C groups.
Third party cookies	"Third party cookies" are those sent or set in a browser when the top level document (the URL in the browser bar) makes image or iframe calls to other sites.	• *Storage Access API* or *Shared Storage API* allows a site to ask a user to allow third party cookies for that site's use – documentation from Mozilla. Implemented in Firefox, with caveats in Chrome, Edge, Safari • *FedCM* : a new way for an authentication token to be exchanged – see above • *Cookies Having Independent Partitioned State (CHIPS, also know as Partitioned cookies)* allows an iframe to set cookies that the iframe can retrieve across a specific top level site, but no other site – documentation from Mozilla and Chrome	Third party cookies are not needed at any protocol specification. However, some consumer authentication libraries embedded in various sites and apps use third party cookies. Within SAML, identity federation, and higher ed, implementations of logout (Why are third party cookies relevant to single logout) and of Seamless Access are affected. In Seamless Access, the "smart button" is not available without third party cookies and introduces additional clicks in the flow for sites using advanced integration.
Cross site request cookies (2021)	Cookies received by a site when a user is directed to that site via a link from another site.	In a proposal shared in the W3C WebAppSec WG regarding "Standardizing Security Semantics of Cross-Site Cookies", the authors note a pattern they call "Top-Level Cross-Site POST Requests." The document recommends "Given the existing widespread usage and lack of clear alternatives, we recommend following the current state of the web and not blocking cross-site cookies in this scenario."	This applies to any SAML SP that has 1. integrates using the recommended POST binding of the SAML response 2. uses SP initiated and saves state using cookies before sending the user for SAML authentication 3. and expects those cookies to be presented on the response in order to correlate the response to a session state with initial request parameters.
IP address obfuscation	Apple's Private Relay for iCloud+ customers is a "lite" relay network used only with Safari and TCP Port 80 (aka http) traffic. All DNS requests are encrypted and go through Apple. Google has in October 2023 declared intent to obfuscate IP addresses of Chrome users. GoogleOne subscribers have access to Google VPN Mozilla offers a VPN	Network relays and proxies can obscure the IP address of the users device or a network's WAN IP address(es) to protect endusers from being associated with a specific origin.	Apple's relay is the most "friendly" providing details about the IP address ranges and documentation: Campus networks that need users on the network to not go through a relays but to appear to originate from the network must make changes documented at "Prepare your network or web server for iCloud Private Relay." Systems that assume region or city level geo-accuracy when interpreting IP address may only get country level accuracy if the user chooses that setting in the relay configuration. Google and Mozilla's VPNs do not seem to have publicized their final IP address ranges, nor any DNS to block in order to signal that VPN or relay use is unwelcome on the network. Google obfuscating the IP makes it unclear where the user is coming from.
Robot identification	CAPTCHA solving is hard on mobile, challenging for accessibility reasons. Some CDNs essentially fingerprint browsers to distinguish "real" from "bot" surfing.	**Privacy Pass** was introduced by Cloudflare (06/08/2022) and Apple (as Private Access Tokens). Work has been transferred to the IETF PrivacyPass working group. There are PrivacyPass plugins for Firefox and Chrome; believe its built into Safari. Web Environment Integrity API was announced by Google (2023-05-08) with a spec and explainer publicized (2023-07-21) and discussion (apparently) in the W3C Anti-Fraud Community Group.	No impact to federated authentication. Potential impact at sites that use CDNs to manage traffic.

TLS (as privacy depends on security)	Sites are identified by their server certificate, and then encrypt the transaction with an algorithm negotiated between server and client.	Authenticating the sites depends on the trust chain in the certificates. Google (as part of the "Moving Forward, Together" program) has proposed to the Certification Authority/Browser (CA/B) Forum that server certificates should have a 90 day certificate validity period.	Discussed at ACAMP in September 2023. Depending on how institutions and CAs manage certs, it may introduce confusion at least.

Secondary sources and articles

- **Chrome's "Privacy Sandbox", phasing out some third party cookies and including Shared Storage, starts general availability in Q3 2023**
    - Chavez, Anthony. “The next Stages of Privacy Sandbox: General Availability and Supporting Scaled Testing.” *The Privacy Sandbox News*, May 18, 2023.
    - Lardinois, Frederic. “Google Will Disable Third-Party Cookies for 1% of Chrome Users in Q1 2024.” *TechCrunch*, May 18, 2023.
        - " Starting in early 2024, Google plans to migrate 1% of Chrome users to Privacy Sandbox and disable third-party cookies for them"
    - Merewood, Rowan, and Alexandria White. “Preparing to Ship the Privacy Sandbox Relevance and Measurement APIs.” *Chrome Developers*, May 18, 2023.
        - "CHIPS: Allow developers to opt-in a cookie to partitioned storage, with a separate cookie jar per top-level site. CHIPS became available in Chrome Stable in February 2023."
        - "Federated Credential Management (FedCM): Support federated identity without sharing the user's email address or other identifying information with a third-party service or website, unless the user explicitly agrees to do so. FedCM shipped in November 2022."
- **Web Environment Integrity**
    - https://www.theregister.com/2023/07/25/google_web_environment_integrity/
- **Privacy Pass**
    - Thibault Meunier, *Cloudflare* https://www.usenix.org/conference/pepr23/presentation/meunier Tuesday, September 12, 2023 - 11:50 am–12:10 pm

We also have a collection of Slides, blogs, and videos from the community.

Useful references

[Hamilton] Dave Hamilton, “Digging into Apple’s ICloud Private Relay,” *The Mac Observer*, June 9, 2021, accessed May 24, 2023, https://www.macobserver.com/tips/deep-dive/digging-into-apples-icloud-private-relay/.

[Kitamura] E. Kitamura, “Understanding ‘same-site’ and ‘same-origin,’” *web.dev*, 10-Jun-2020. [Online]. Available: https://web.dev/same-site-same-origin/.

[RFC-7258] S. Farrell and H. Tschofenig, “RFC-7258 BCP-188 Pervasive Monitoring Is an Attack,” IETF, Best Current Practice RFC7258, May 2014 [Online]. Available: https://tools.ietf.org/html/rfc7258. [Accessed: Feb. 03, 2016]

[W3C TAG 2015] M. Nottingham, “Unsanctioned Web Tracking,” W3C, W3C TAG Finding, Jul. 2015 [Online]. Available: https://www.w3.org/2001/tag/doc/unsanctioned-tracking/. [Accessed: Aug. 20, 2021]