REFEDS Community Chat: Federated Identity and Browsers (Update)

Heather Flanagan,
Wearer of All The Hats

Playlist for Today

Problem Statement

About Tracking

Timing

R&E Hackathon Report

Next Steps

Problem Statement for the Web

Non-transparent, uncontrollable tracking of users across the web needs to be addressed and prevented.

(Thank you, GDPR)

Federated Authentication Addendum

Many applications and services need to work through the browser to support SSO/federated login, and yet federated login and tracking tools **use the same features** and **are indistinguishable** from the browser’s perspective.

Academia, Enterprise, etc, are important, but…

The experience and lead driver of the browser vendors is in the consumer web.

If you want to succeed, think to how you can take advantage of as many consumer-web features as you can.

It’s About More Than Just Federation

Sites use features like cookies for more than just authentication and authorization

- Storing user preferences
- Session information across frames
- Demographic info for targeted advertising / content

LEARNING ABOUT TRACKING

How Does Tracking Happen

Third-Party Cookies

IP Addresses

Browser Fingerprinting

Link Decoration

Bounce Tracking

Cookies

HTTP cookies (also called web cookies, Internet cookies, browser cookies, or simply cookies) are **small blocks of data created by a web server** while a user is browsing a website and **placed on the user's computer** or other device by the user’s web browser.

- First-Party Cookies
  - *Accessible only by the domain that created it*

- Third-Party Cookies
  - *Accessible to any site at any domain*

IP Addresses

Used to **identify machines and/or services**

- Tracking mitigations for Browser Fingerprinting often impact IP address information
- Often used to make authorization decisions in:
  - Libraries
  - Enterprise Resource Planning (ERP) systems

- All major browser vendors are offering built-in VPN services that block IP addresses, etc

Browser Fingerprinting

Information collected about the software and hardware of a remote computing device for the purpose of identification

Includes capture of information such as

- Browser used
- Fonts used
- Add-ons used
- Browser security configuration
- IP address
- …

Link Decoration

A method of **adding extra information to the URL**. Also known as "navigation-based tracking"

Used for:

- Query strings
- Some authentication tokens (i.e., "Front-channel")
- Tracking information

https://customer.sspnet.org/SSP/Events/2022-Annual-Meeting/ssp/AM22/Home.aspx**?hkey=25db5ee4-3ea6-4a35-8f4a-a6229e9c194a**

Bounce Tracking

Used by trackers to **get around third-party limitations**, also known as redirect tracking

- Website A sends the browser to the tracker to get a first-party cookie.
    - The tracker then sends the browser on to the user's destination with additional information stored in the browser that will allow the tracker to ‘follow’ the user around the web.

- The end-user does not see this transition; they only see Website A and then the destination page.

IMPLICATIONS FOR ACADEMIA

Browsers vs Browser Engines

- Browsers = Chrome, Firefox, Safari, Edge, Brave
- Browser engines = Blink (aka, Chromium), Gecko, WebKit
- Functionality is based on the browser engine more than the browser
  - ALL browsers on iOS and iPadOS are actually built on WebKit; WebKit does not support third-party cookies
  - Edge and Chrome are built on Blink; they will show much the same behaviors when it comes to features

This matters when you start troubleshooting why someone can't get to a website or service

Implications to Remember

- Authentication that uses SAML should continue to work as designed for at least the next 1-3 years.
    - (except, the ability to globally log out of all SAML sessions)
- WAYF IdP Discovery services will continue to work.
    - (previous organizations will likely be forgotten (e.g., SeamlessAcccess).
- Services that share information between third-parties in frames (e.g., Teams, ILS/LMS) will have mixed results.
- Other features that enable tracking (IP addresses, browser fingerprinting) are already breaking, depending on which browser is being used.
- WAYFless linking (link decoration) may be affected depending on implementation.

Timelines

- Apple’s timeline:
  - n/a (but they’ve already done a lot of work in this area; they started blocking third-party cookies in 2017 as part of Intelligent Tracking Protection)
- Mozilla’s timeline:
  - n/a (but they’ve turned on Total Cookie Protection by default in June 2022)
- Google’s timeline:
  - https://privacysandbox.com/timeline
  - “As developers adopt these APIs, we now intend to begin phasing out third-party cookies in Chrome in the second half of 2024.”

R&E Hackathon and Other Late-Breaking News

R&E “Hackathon”

- Purpose:
  - To take an active, proposal-focused approach on solving the core problems of tracking and federation
  - To understand the FedCM API
  - To explain the R&E Federation use cases

Proposals

- Idp-sp-storage API (https://github.com/fedidcg/proposals/issues/4)
  - Fewer “miracles occur”
- Offloading Trust (https://github.com/fedidcg/proposals/issues/5)
  - More concrete trust models, heavier lift

Areas of Concern re: FedCM

- A few big problems to solve that the current FedCM model doesn't address
  - **Scale (number of IdPs)**
  - Origin (browser) vs endpoints (SAML/OIDC)
    - Proxy services
  - Interferes with at least the SAML protocol on a level outside of 3pc
  - Session timing (i.e., sessions may be very short-lived)
  - SAML and OIDC have similar but not the same behavior, esp. when it comes to circles of trust

Ongoing Issues and Concerns

- Browsers need IdPs and RPs using OIDC and/or SAML to test and provide feedback
  - No, the browser teams working on new APIs is not tightly coupled with an IdP team
- Better to have proposals instead of arguments
  - R&E FedCM "Hackathon" definitely helped (necessary but not sufficient)
- Particularly important for R&E and certain identity and cloud service providers: figuring out how proxies will work

Next Stop

- Internet Identity Workshop (18-20 April 2023, Mountain View, California)
  - Expect to focus on the proxy scenario
- TNC23 Side Meeting (Thursday 8 June, 08:30-10:30, Tirana, Albania)

Want to Learn More?

To be a part of developing the solution (or at least lurk and learn)

- Federated Identity Community Group
  - https://www.w3.org/community/fed-id/
- Private Advertising Technology Community Group
  - https://www.w3.org/community/patcg/
- Privacy Community Group
  - https://privacycg.github.io/
- REFEDS Browser Changes and Federation
  - https://wiki.refeds.org/display/GROUPS/Browser+Changes+and+Federation

Q&A