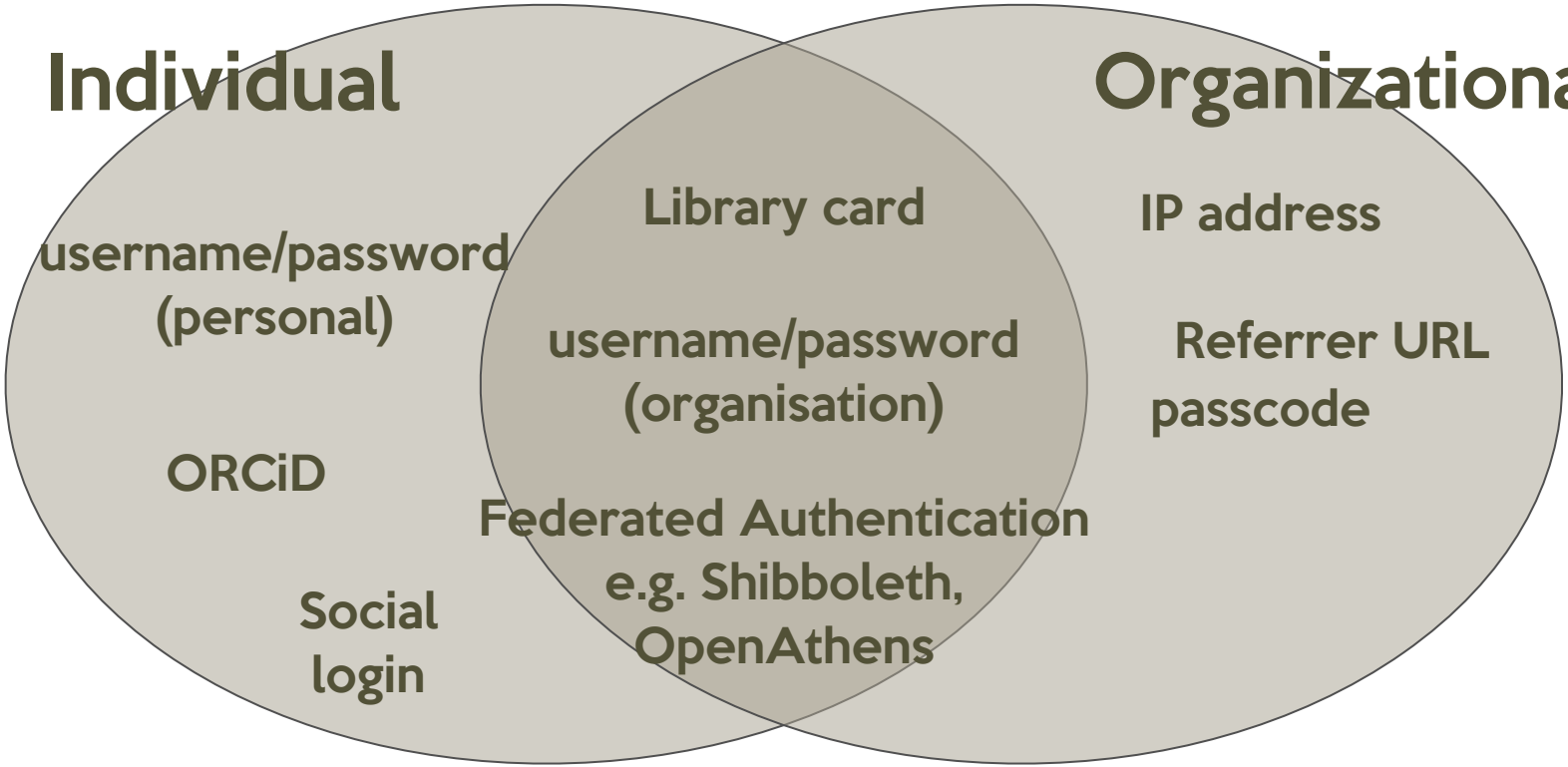
The Future of Authentication: Landscape & Challenges

Computers in Libraries 2022

Jason Griffey
Director of Strategic Initiatives
National Information Standards Organization

What methods are used?



Each methods offers different trade-offs

	Implement	Maintain	Privacy	Security	Personalize
IP Auth	easy	[sigh]	yes*	varied	no
Fed Auth	hard	easy	yes*	high	yes
Uname/ Pword	easy	easy	no	depends	yes
Passcode	easy	depends	yes	low	no
Referrer URL	easy	easy	yes	low	no

The Coming Authentication Apocalypse

- Problem Statement
- About Tracking
- Timing and Browser Development Activities
- Next Steps

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

General Problem Statement

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

Federated Identity Looks Like Tracking

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.

Features that Can Be Used for Tracking

- If it can be used for tracking, it is under consideration for a major redesign
- Third-party cookies are high on the list of features to be removed in favor of a more privacy-preserving default web experience
- Browser vendors differ on how they are prioritizing development

Something to Remember

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

- Implications: browser developers don't understand government, academic, fintech, healthcare, ...

How Does Tracking Happen?

- Third-Party Cookies
- IP Addresses
- Browser Fingerprinting
- Link Decoration
- Bounce Tracking

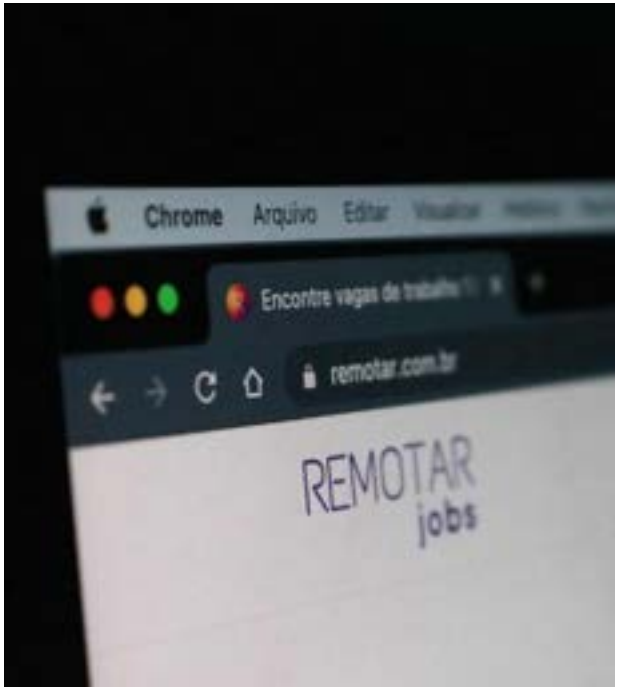
Cookies

“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

IP Addresses

- Used to identify machines and/or services
- Often used to make authorization decisions
  - Libraries
  - Enterprise Resource Planning (ERP) systems



Link Decoration

"A method of adding extra information to the URL"

- 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

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
  - ...

Bounce Tracking [aka Redirect Tracking]

- Used by trackers to get around third-party limitations
  - 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.
- Used by OIDC to validate session information between an IdP and a Relying Party
  - Implicit flow -- for browser (JavaScript) based apps that don't have a backend. The ID token is received directly with the redirection response from the OP. No back-channel request is required here.

What's Changing Now?

The Short, Short Version

- Authentication that uses SAML will continue to work as designed for at least the next 2-3 years (excepting the ability to globally log out of all SAML sessions).
- Authentication that uses OIDC (e.g., Google, PayPal) is going to partly break.
- Services (like SeamlessAccess) that use browser local storage will break in some instances.
- Services that share information between third-parties in frames (like Microsoft Teams) so that many domains can read the same data are going to have to have mixed results.
- Other features that enable tracking (IP addresses, browser fingerprinting) are already breaking, depending on which browser is being used.

Going on a Diet

Safari: third-party cookies are **already** blocked by **default**

Firefox: third-party cookies are **already** blocked by a blocklist

Chrome (desktop): “phase out third-party cookies over a three month period, starting in mid-2023 and ending in late 2023”

What Breaks When Third-Party Cookies are Gone

SAML Single Log Out will break (depending on how a vendor has implemented it)

Several OIDC/OAuth2 features will break (e.g., front-channel logout, session management, iFrame-based session extension, SPA background token renewal)

IdP persistence will break because of the third-party nature of the information (e.g., IdP discovery services, SeamlessAccess)

Cookies and Federation Behavior

- If you want to emulate the worse case of how the lack of cookies will impact software in use, test with Safari
  - Example: Microsoft Teams won't work in Safari
- If you want to emulate how Chrome (desktop) breaks, go to your preferences and turn off all third-party cookies

IP Addresses

- Apple's iCloud Privacy Relay (part of an iCloud+ subscription)
  - First assigns the user an anonymous IP address that maps to their region but not their actual location.
  - Then decrypts the web address they want to visit and forwards them to their destination.
  - This separation of information protects the user's privacy because no single entity can identify both who a user is and which sites they visit

Timelines

- Apple's timeline:
  - n/a (but they've already done a lot of work in this area)
- Mozilla's timeline:
  - n/a (but they're somewhere between where Apple is and where Google is)
- Google's timeline:
  - https://privacysandbox.com/timeline

Immediate Info for Your IT and Library Staff

From SeamlessAccess:

FAQ on Browser Privacy Changes and Library Resource Access

(Or Why Your IP Authentication is About to Break)

https://seamlessaccess.org/learning-center/browser-faq/

What To Do?

What to look for and think about moving forward

Prepare

- These issues are complex and difficult to understand, people need to start educating themselves (see also; SeamlessAccess Learning Center)
- Learn how to ID the aforementioned Browser issues, troubleshooting with users will be maddening
- Evaluate your access methodologies, and begin to understand how these changes may affect your operations and your user's experiences
- Be prepared over the next 5 years for a series of changes in how authentication, authorization, and access controls are understood and implemented

Inform

- It is unlikely that things will break in large numbers suddenly
- But communication both externally and internally will be difficult because of this…you're looking at narrow issues that expand, so don't get caught thinking these issues don't apply to you/your organization
- Because of the complicated nature of Access in general, communications will be equally complicated (your org, your service providers, your users, your IT departments)

Advocate

- Internally
  - Work with your IT/Systems department to help understand the specific data being shared, and the choices being made regarding that data
  - Work with your licensing people to understand the effect that FedAuth has on your existing contracts, and as you renew consider adopting language specific to FedAuth where necessary.
- Externally
  - Look to groups that are paying attention to and working on the big picture effects of these changes (SeamlessAccess, W3C, NISO)
  - Be ready to work with groups outside your organisation (federations and other large cooperatives) to find solutions

Thank you!

Jason Griffey
@griffey
griffey@niso.org