



Single Sign-On Privacy: We Still Know What You Did Last Summer

Maximilian Westers¹, Andreas Mayer¹, Louis Jannett²

Heilbronn University of Applied Sciences¹, Ruhr University Bochum²

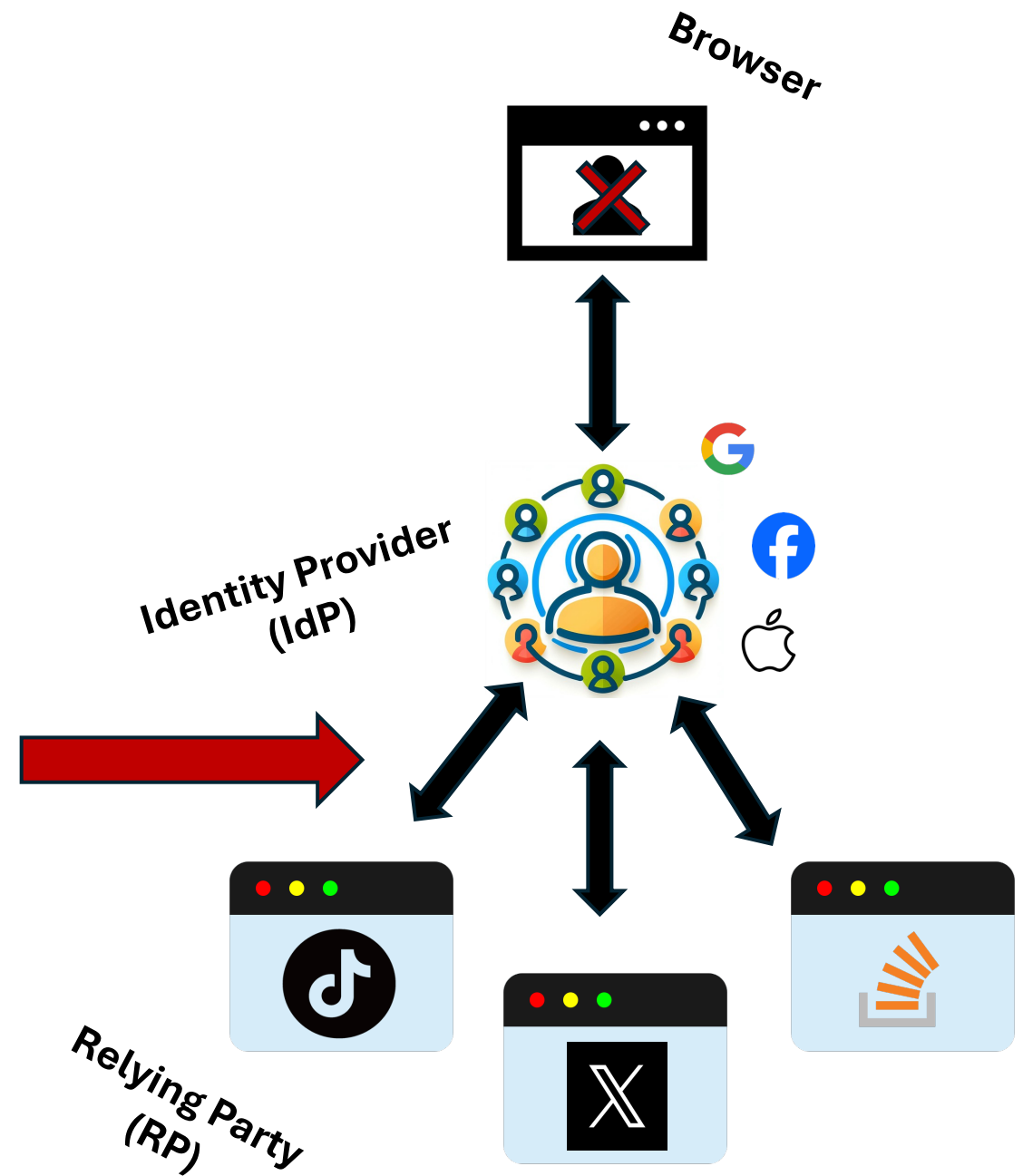
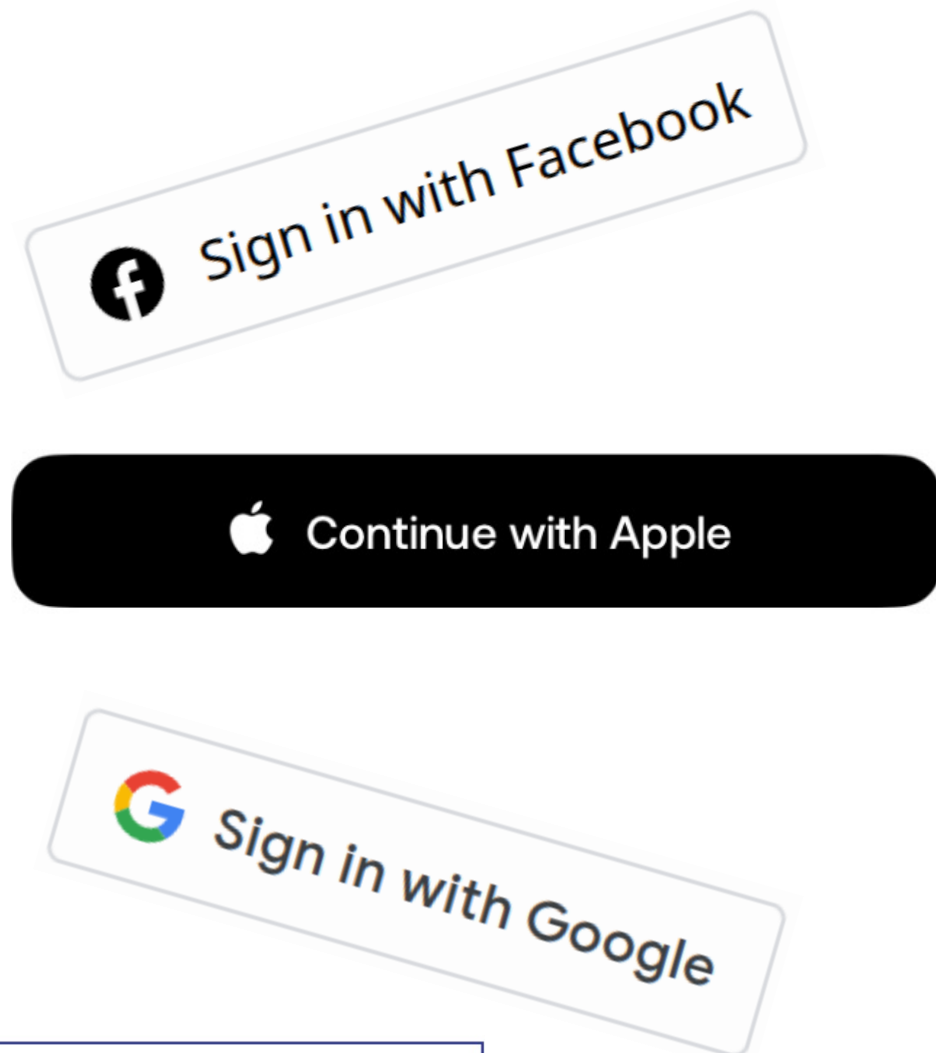


Short Facts



- **Findings:** Single Sign-On (SSO) may leak the identity to various parties
- **Large-scale study:** Hidden privacy leaks are widespread in SSO
- **Countermeasures:** How to mitigate privacy leaks





What is Single Sign-On?



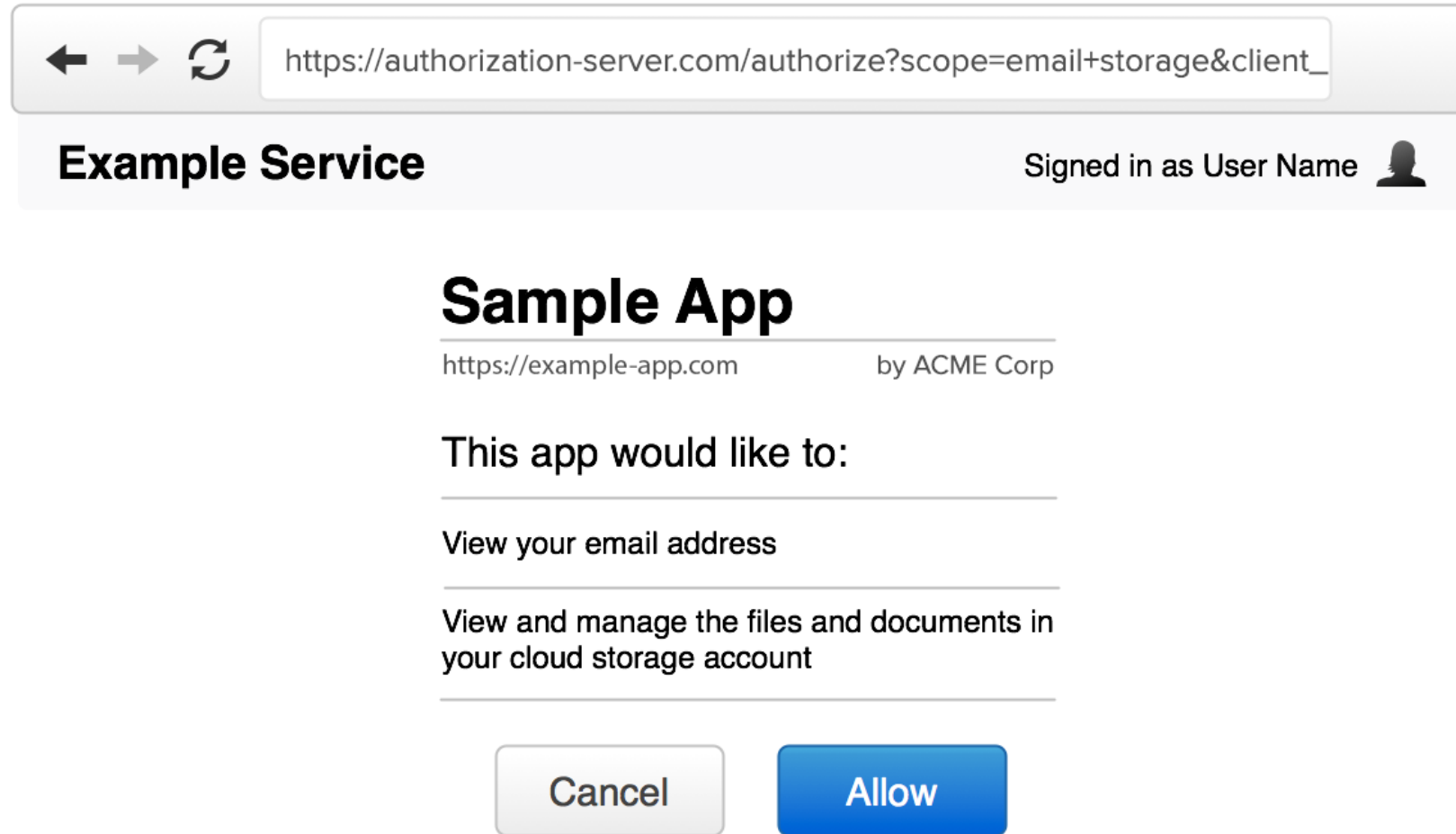
Initial Context

-  No session at RP
-  No login process at RP

-  Valid session at IdP
-  Logged in into RP using IdP at least once in the past



Limitation – Logged in once







The screenshot shows a web browser interface. At the top, there is a navigation bar with a back arrow, a forward arrow, and a refresh icon. The address bar contains the URL: `https://authorization-server.com/authorize?scope=email+storage&client_`. Below the address bar, the page header displays "Example Service" on the left and "Signed in as User Name" with a user profile icon on the right. The main content area features a large heading "Sample App" followed by the URL `https://example-app.com` and the text "by ACME Corp". Below this, the text "This app would like to:" is followed by a list of permissions: "View your email address" and "View and manage the files and documents in your cloud storage account". At the bottom of the dialog, there are two buttons: a grey "Cancel" button and a blue "Allow" button.



SSO Hidden Logins

The screenshot shows a web browser window with two tabs: "The World's Platform for..." and "Facebook - Anmelden...". The address bar displays "change.org/?lang=en-US". The website header features the "change.org" logo and navigation links: "Start a petition", "My petitions", "Browse", and "Membership". A search icon and "Log in" link are positioned on the right. The main content area has a world map background with the text "The world's platform for change" and "542,708,148 people taking action. Victories every day." Below this are two buttons: "Start a petition" (red) and "Help me draft a petition" (white with a red border). At the bottom, there is a blue bar with a fork and a red meat patty on the left, and a white box with a blurred image and the text "Free Wilfried Siewe from jail" on the right.

SSO Hidden Logins

- Automatic request to Facebook 
- Automatic response (w/o user's notice) with user's identity 
- Single Sign-On was executed! 
- More IdPs affected? 



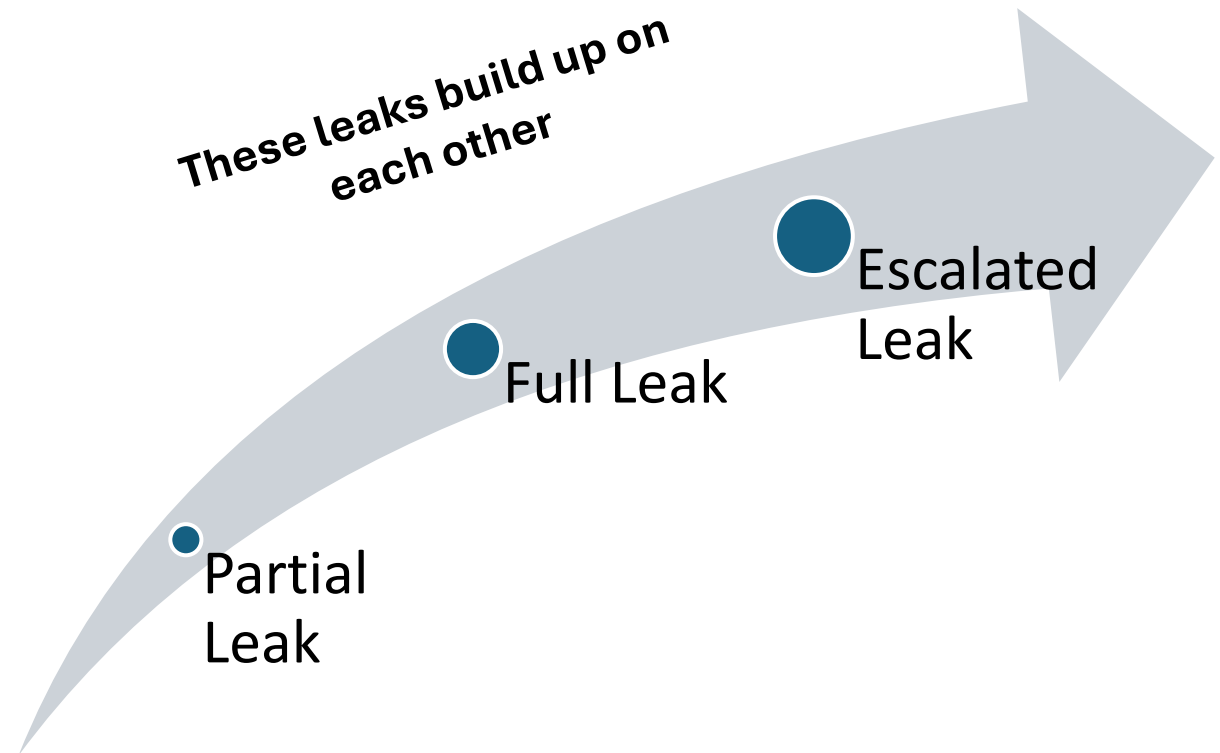
SSO Privacy Leaks

Klassen und Aufbau



SSO Privacy Leaks

- 3 classes of privacy leaks
 - Partial Leak (PL)
 - Full Leak (FL)
 - Escalated Leak (EL)




SSO Privacy Leaks

Partial Leak (PL):

- RP identifier
- User's identity (Cookies, IP, etc.)

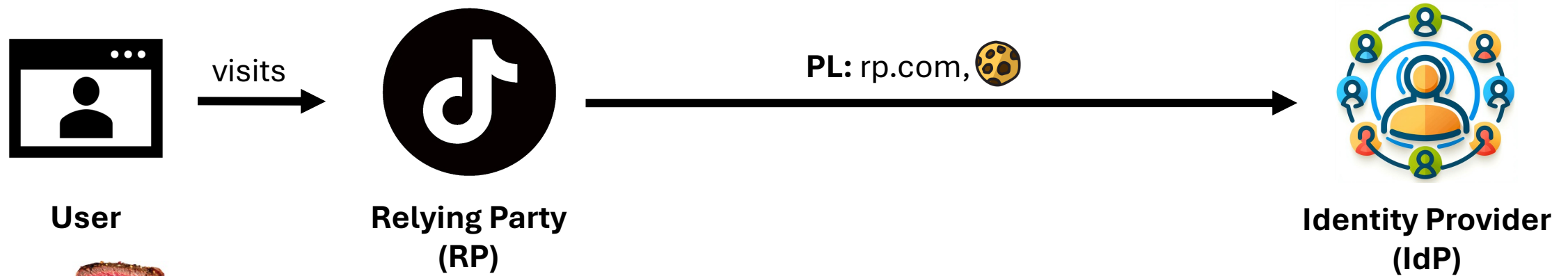


SSO Privacy Leaks

The IdP learns, which RP the user is visiting 

Partial Leak (PL):

- RP identifier
- User's identity (Cookies, IP, etc.)



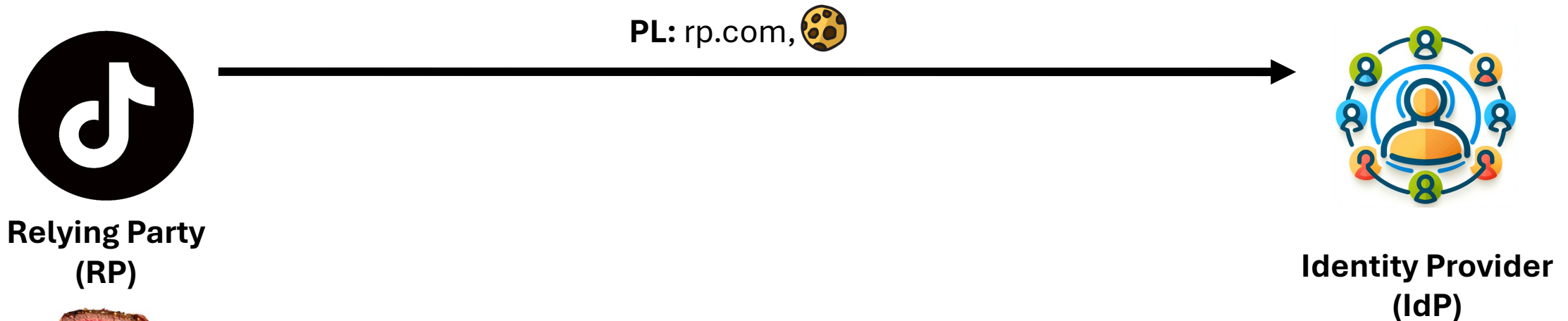
SSO Hidden Login Request Example

Name	×	Headers	Payload	Preview	Response	Initiator	Timing	Cookies
status?client_id=484098...	▼	General						
Request URL:		https://www.facebook.com/x/oauth/status?client_id=48409868550&input_token&origin=1&redirect_uri=https%3A%2F%2Fwww.ihange.org%2F&sdk=joey&wants_cookie_data=false						
Request Method:		GET						
Status Code:		● 200 OK						
Remote Address:		157.240.251.35:443						
Referrer Policy:		strict-origin-when-cross-origin						



SSO Privacy Leaks

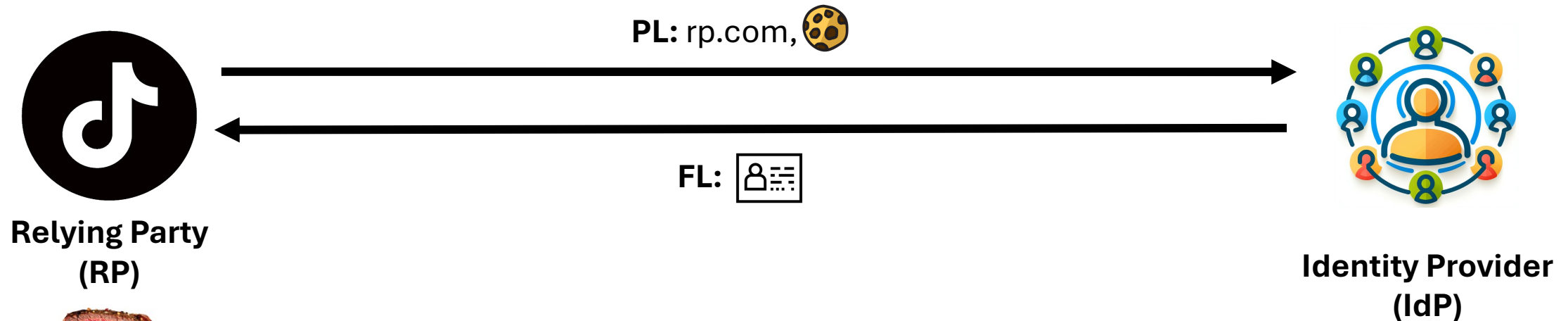
Full Leak (FL):



SSO Privacy Leaks

Full Leak (FL):

- User's identity
- Personally identifiable information (PII)

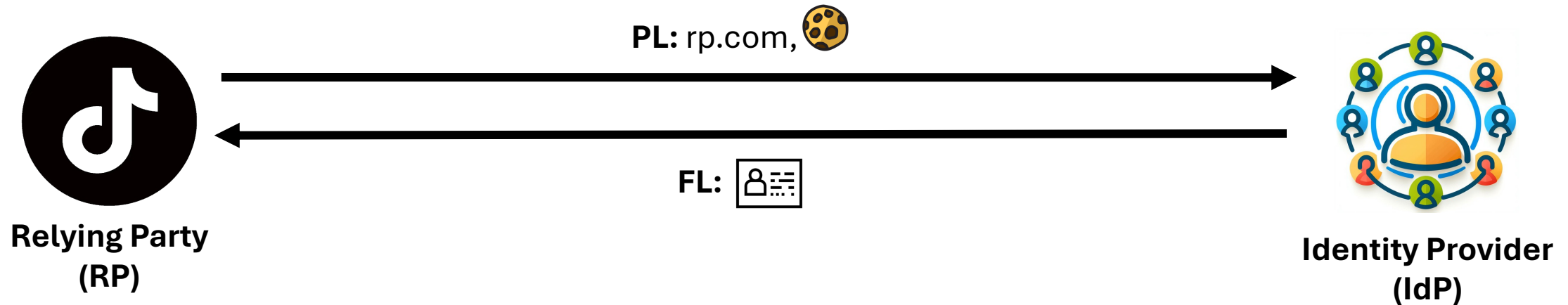


SSO Privacy Leaks

The RP learns the user's identity! ⚡

Full Leak (FL):

- User's identity
- Personally identifiable information (PII)



SSO Hidden Login Request Example

Fb-Ar:

```
{ "user_id": "122127858914299952", "enforce_https": true, "access_token": "EAAAAC0VzZBQYBO0mAuoGoNeD3h76DXtPi6Otyae", "signed_request": "RGRuRWlIN1Rwd1VJd1JxeXJxQVRUaUs3cTNQaFlfWpmUjdPSUxMdnFJakZWcmozM1A0VmhySUT4X0IJaTVRSzBjNWMwWUhxV1VnbHRMbmJRZGVjYzByVFuS1RTVXprR2VadjBvdzVfVDd0SjZwOHJOaHFISdRN2laSW5fX3l0VzJuVkdsN0kxT1g2MzNWX1JjWib2F1dGhfdG9rZW4iOiJFQUFBQUMwVnpaQlFZQkiclcGoxa1dQaFVCRHJYRmlwN29WVjA0aVV1UjM4bM0s1RXBsVGJm44UGRoNDZLcUt4N1hjV0w3a3VUdaQ3dwcEtRMkxLbE5hOVVaRCIsImFsZ29yaXR", "expires_in": 5181455, "graph_domain": "facebook", "data_access_expiration_time": 1739700837, "long_lived_token": "EAAAAC0VzZBQYBO0mAuoGoNeD3h76DXtPi6Otyae" }
```

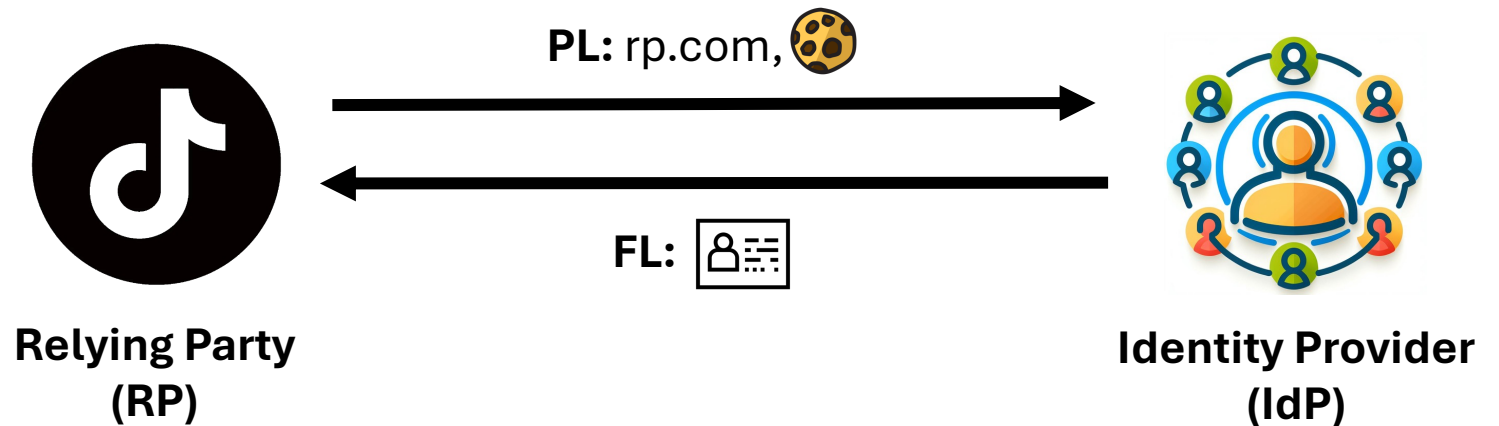
Fb-S:

connected



SSO Privacy Leaks

Escalated Leak (EL):

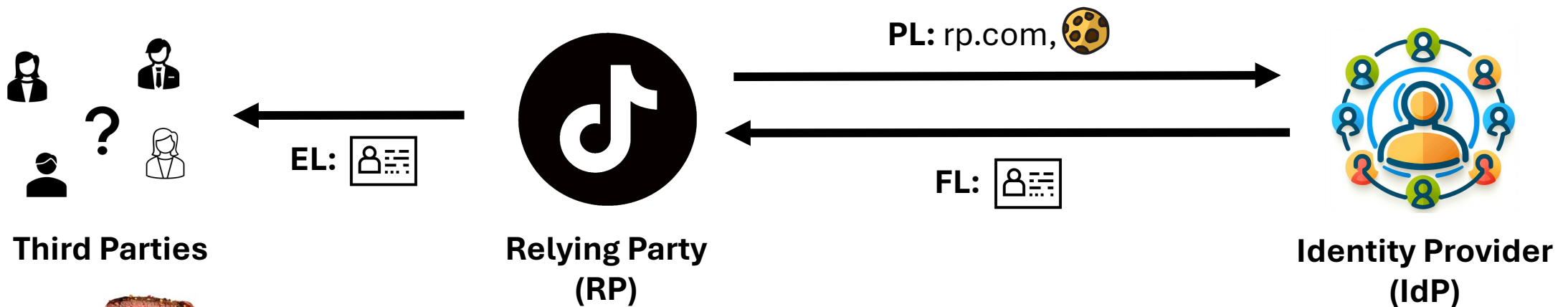


SSO Privacy Leaks

Escalated Leak (EL):

- User's identity

Third parties learn the user's identity!



Methodik und Ergebnisse

Wie sind wir vorgegangen?



Methodology

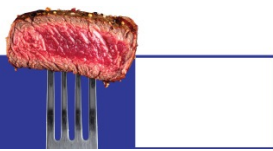
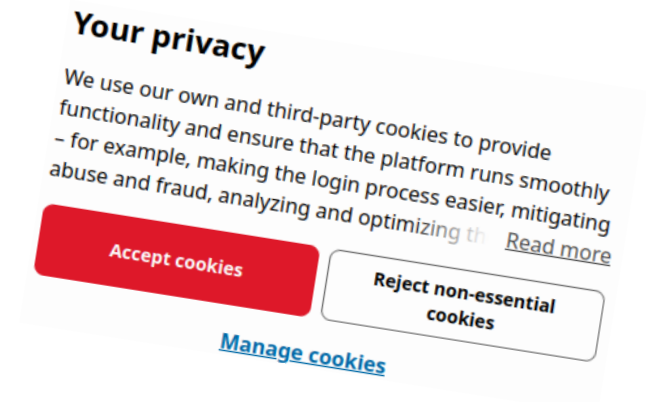
1. Partial Leaks

- Top 1M Tranco domains
- Searching for hidden SSO requests¹



Scan execution:

- Cookie banners have neither been accepted nor declined
- Only the start page was analyzed



¹ 11 well known IdPs and generic pattern

Methodology

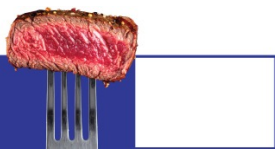
2. Full Leaks

- Created fresh IdP accounts
- Scanned all websites with PLs again with an active IdP session profile



3. Escalated Leaks

- Analyzed the HTTP traffic to find privacy leaks to third parties

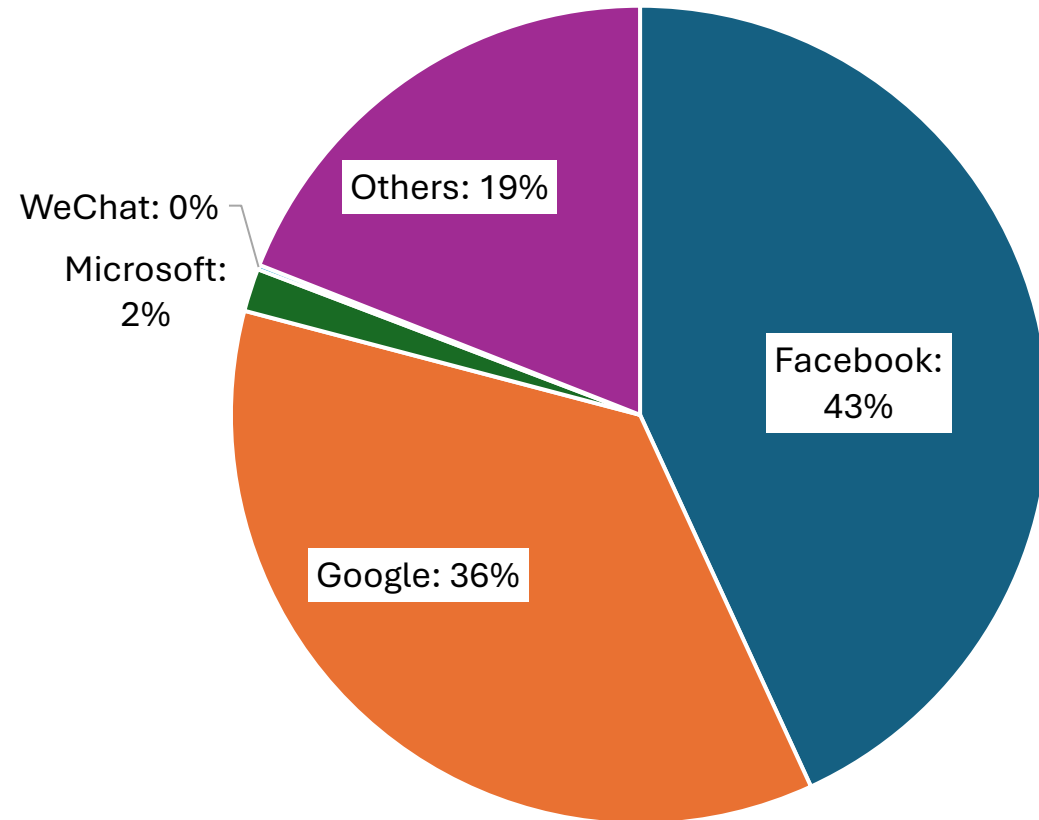




PL: rp.com, 



Results – Partial Leaks



Partial leaks

- ~11k partial leaks in total
- ~1k previously unknown IdPs
 - shop.app
 - auth0.com
 - q4inc.com
 - newscorpaustralia.com

SDKs are the main reason for privacy leaks in SSO



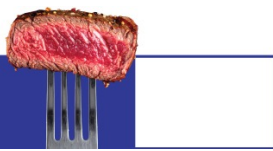
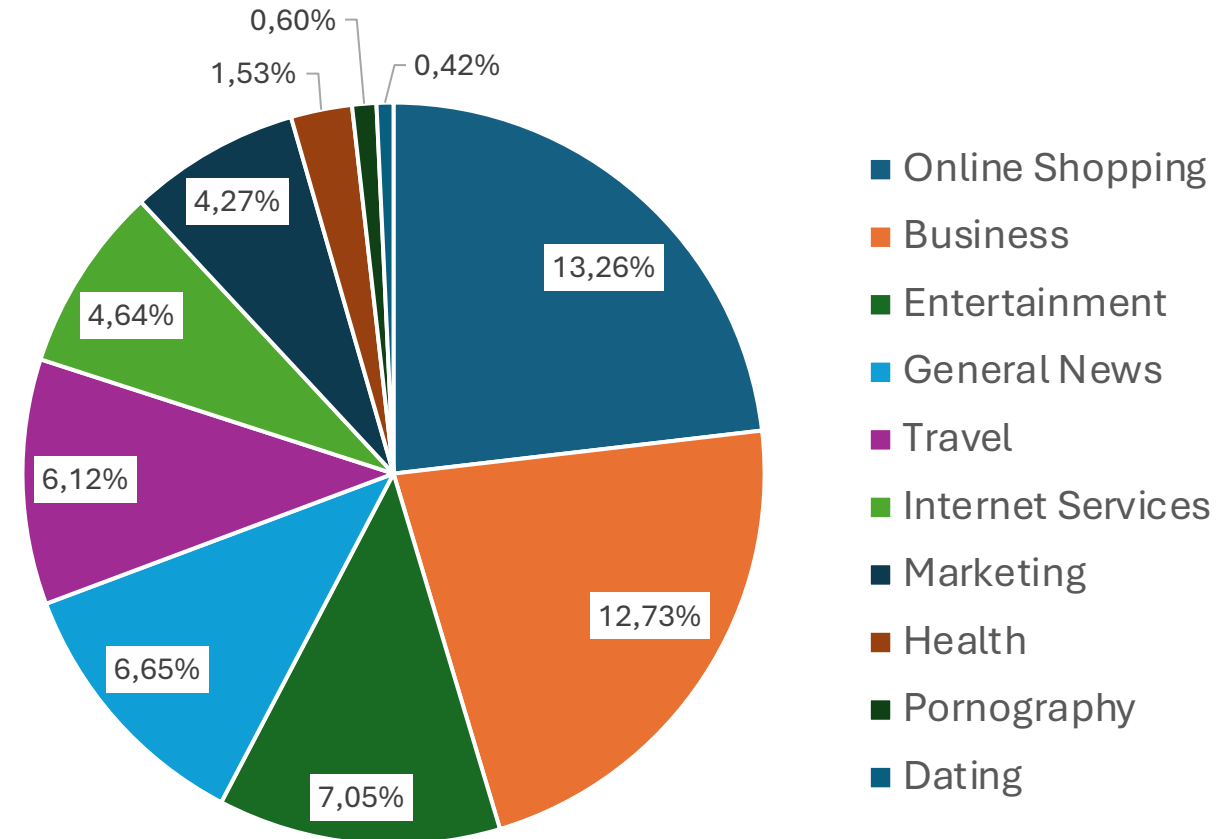


Results – Partial Leak Categories

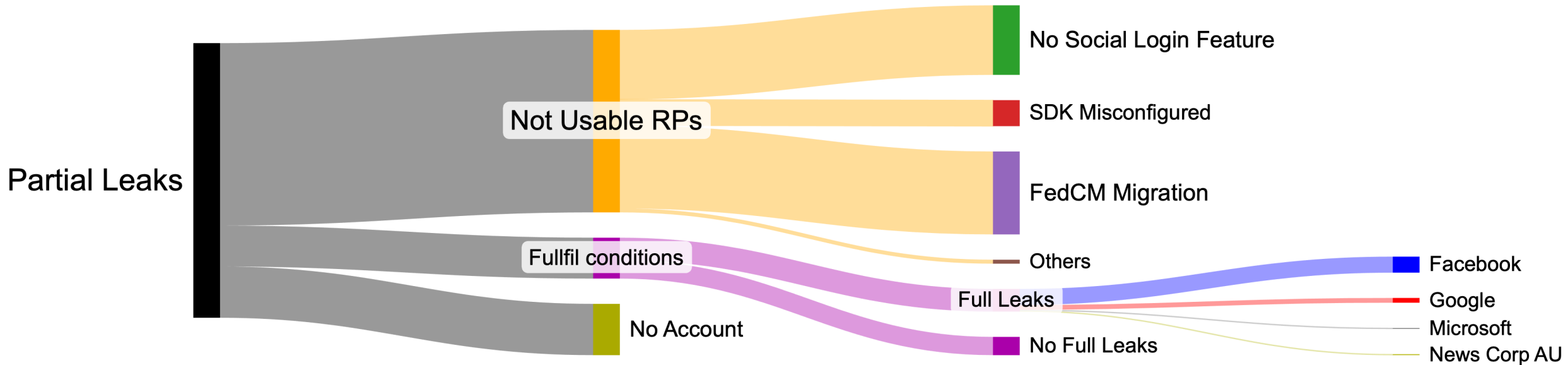
Leak Categories

- Categories vary widely
- Privacy sensible categories

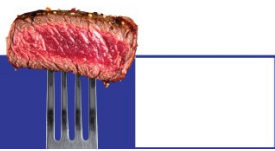
These categories may reveal much about problems, fears, needs, and attitudes of users.



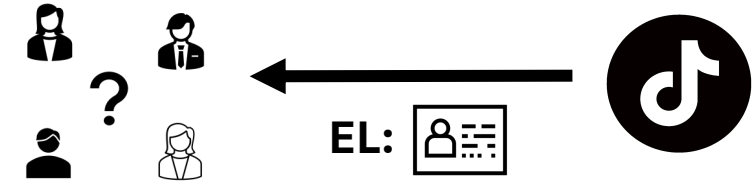
Results – Full Leaks



- In total, we analyzed 1,666 RPs and found 922 FLs

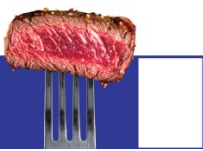


Results – Escalated Leaks



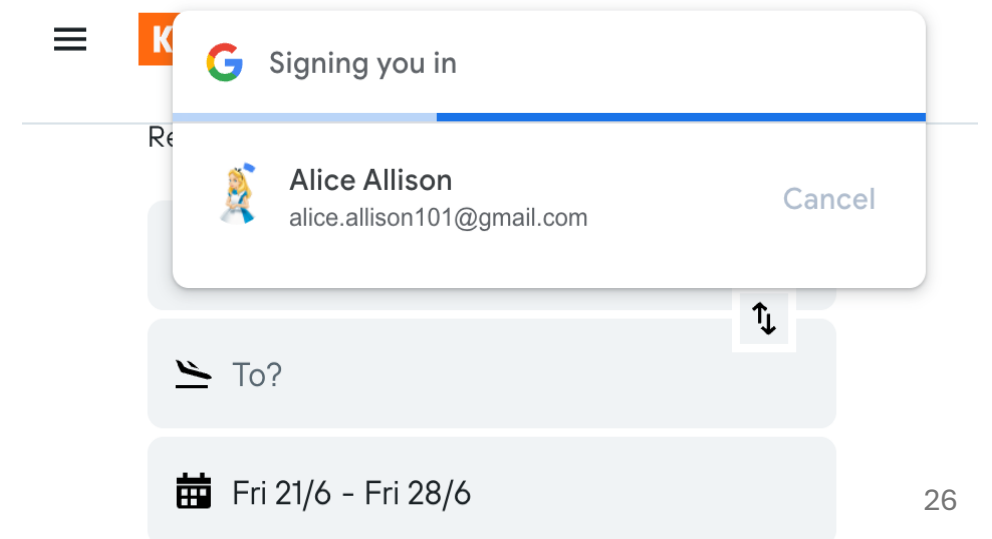
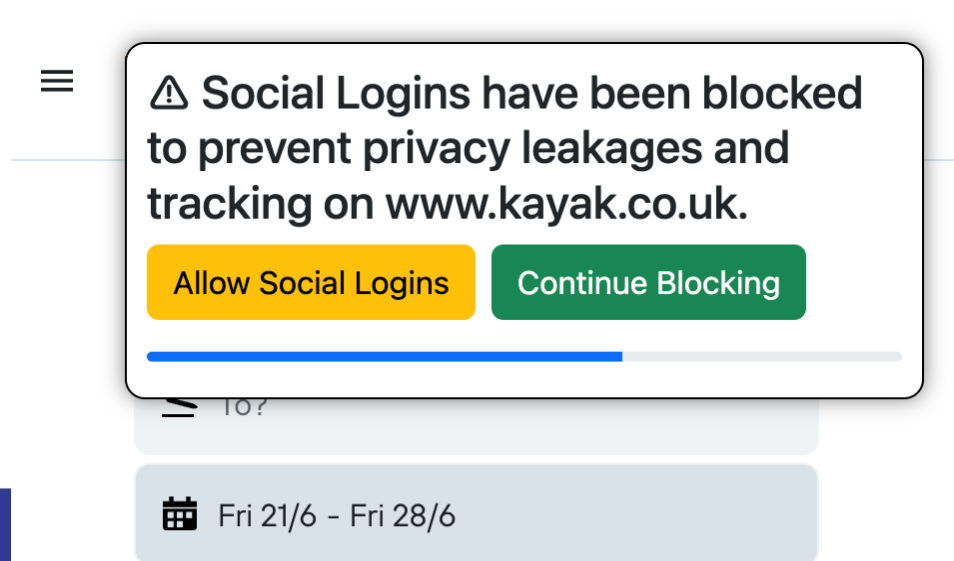
Escalated Leaks

- Only 6 websites leaked their tokens to a third party
 - Facebook: 4
 - Google: 2



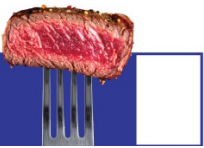
Countermeasures: How to fix it?

- Opt Out:
 - Depends on the implementation of the social login feature
- SSO-Guard
 - Browser extension that detects and prevents all SSO privacy leaks



Countermeasures: How to fix it?

- Opt Out:
 - Depends on the implementation of the social login feature
- SSO-Guard
 - Browser extension that detects and prevents all SSO privacy leaks
- Federated Credential Management API (FedCM)
 - New browser API that enables privacy-preserving SSO
 - Fixed 3,379 of 4,023 PLs for Google
 - Currently only available in Chromium-based browsers and as an experimental feature in Firefox



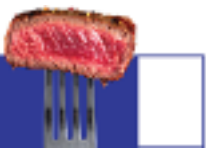
Responsible Disclosure

"We have carefully reviewed your submission with the relevant product and engineering teams and have determined that it does not qualify as a privacy or security concern."

- Facebook 

"We've investigated your submission and made the decision not to track it as an abuse bug. These requests are essential in facilitating users with one-tap sign-in experience."

- Google 



Thanks for your attention!

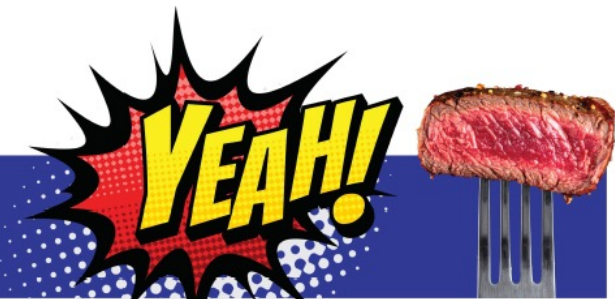
Paper 



Artifacts 



<https://sso-privacy.me>





Results – Partial Leaks vs. Tranco

