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

Maximilian Westers[1], Andreas Mayer[1], Louis Jannett[2]

Heilbronn University of Applied Sciences[1], Ruhr University Bochum[2]

HEILBRONN UNIVERSITY OF APPLIED SCIENCES

RUHR UNIVERSITÄT BOCHUM

RUB

Short Facts

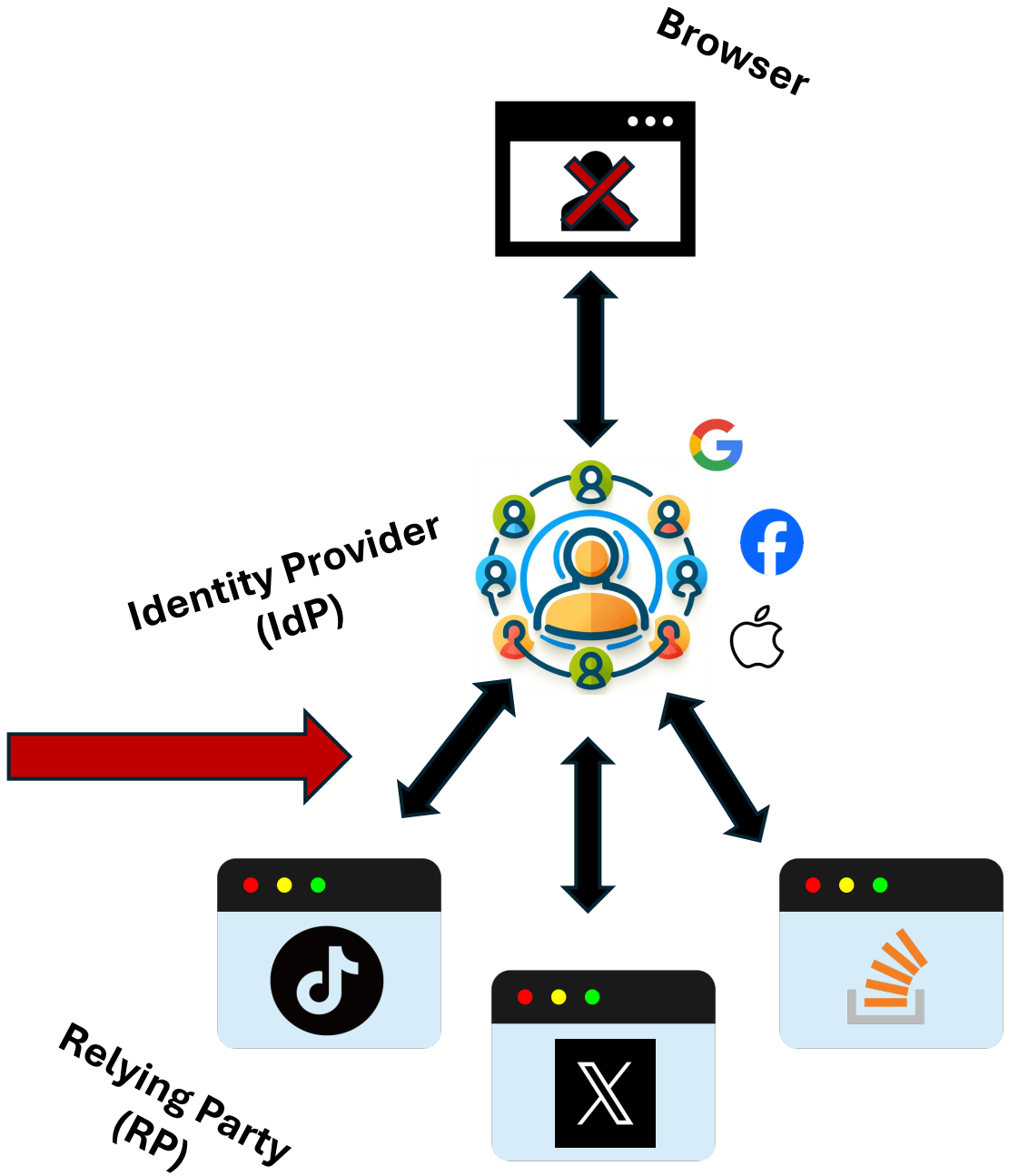
- **Findings**: Single Sign-On (SSO) may leak the identity to various parties
- **Large-scale study**: Hidden privacy leaks are widespread in SSO
- **Countermeasures**: How to mitigate privacy leaks

What is Single Sign-On?

Sign in with Facebook

Continue with Apple

Sign in with Google



Initial Context

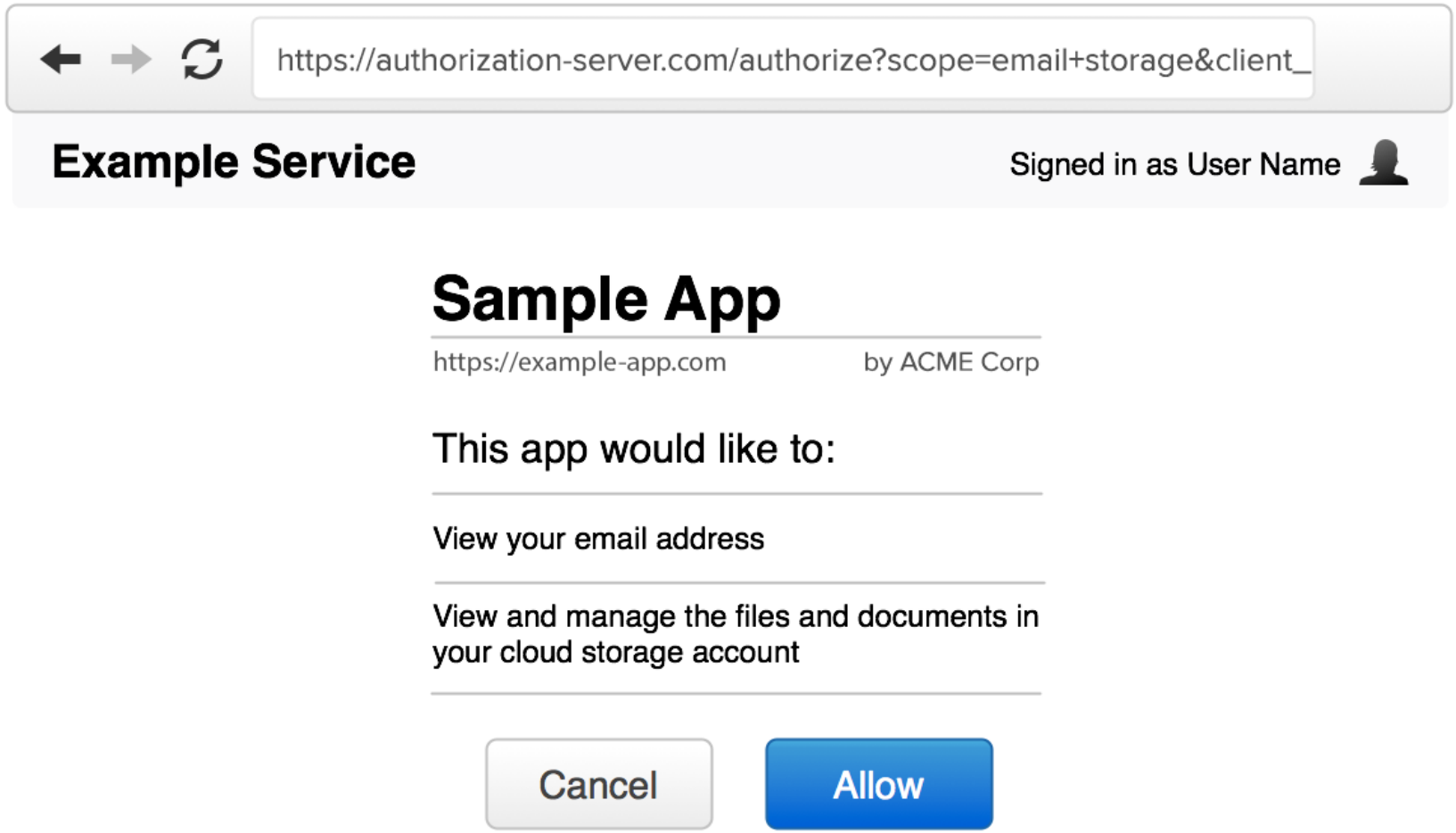
🍪 No session at RP

🖱️ No login process at RP

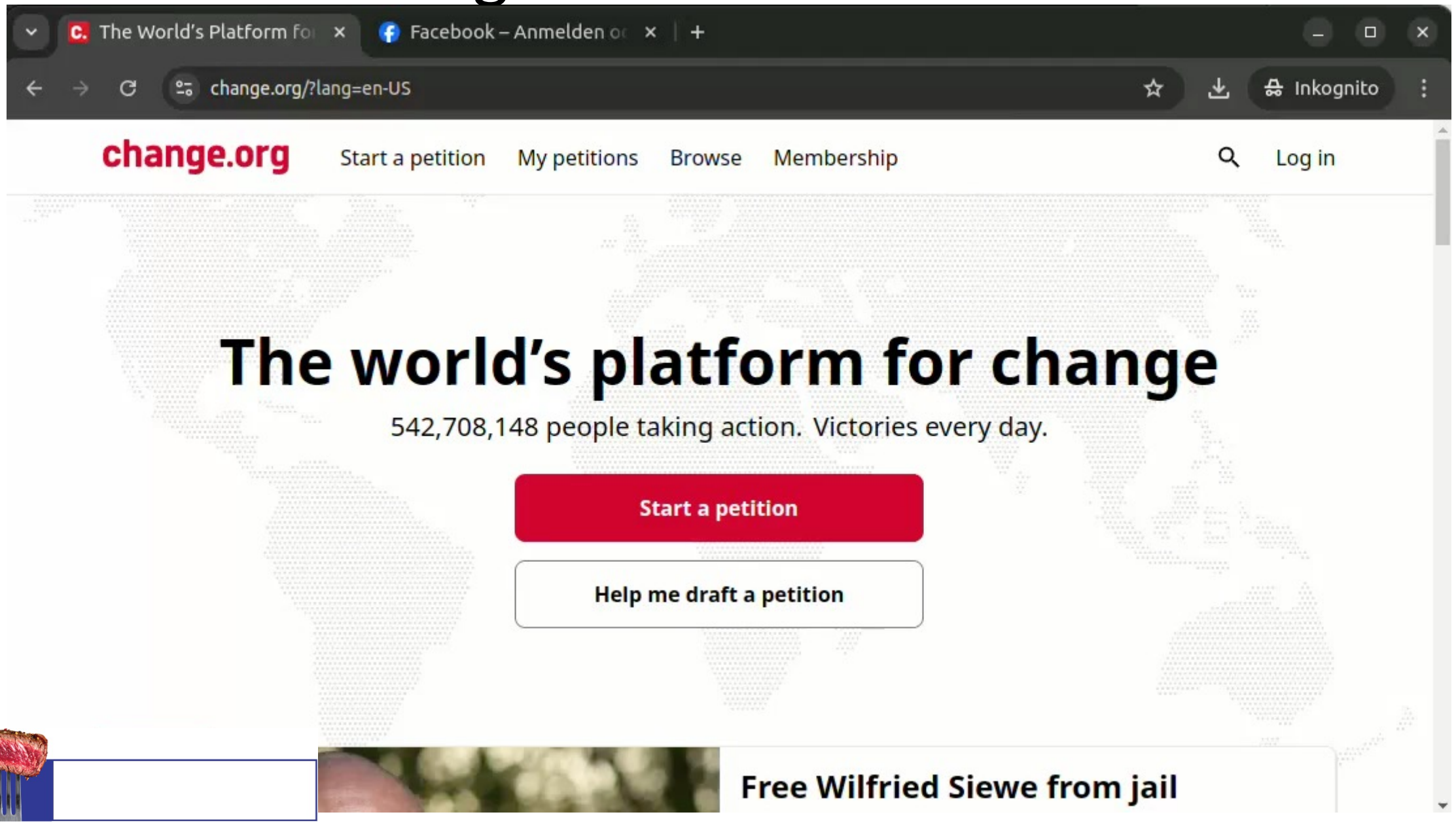
🔗 Valid session at IdP

✅ Logged in into RP using IdP at least once in the past

Limitation – Logged in once



SSO Hidden Logins



SSO Hidden Logins

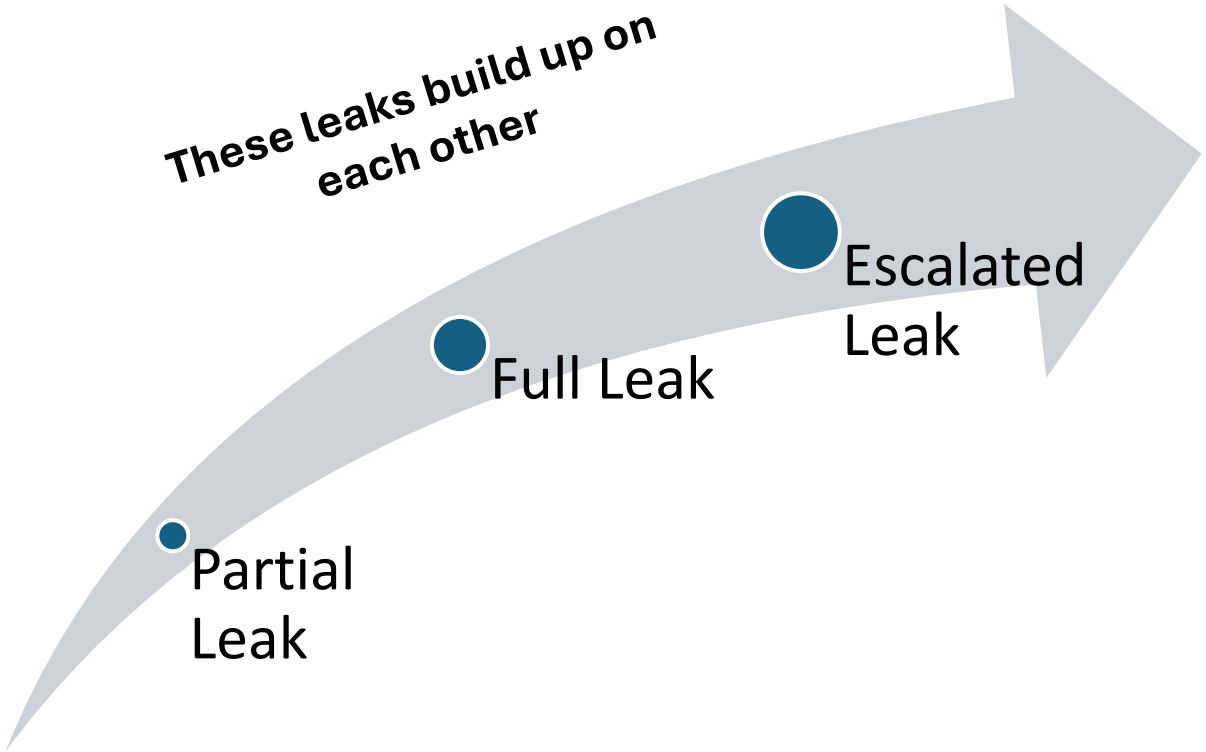
- Automatic request to Facebook
- Automatic response (w/o user's notice) with user's identity
- Single Sign-On was executed!
- More IdPs affected?

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.)

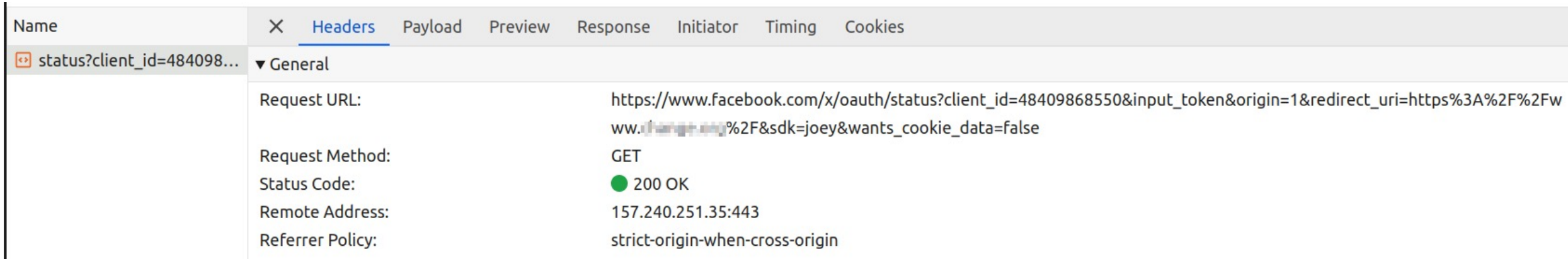
SSO Privacy Leaks

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



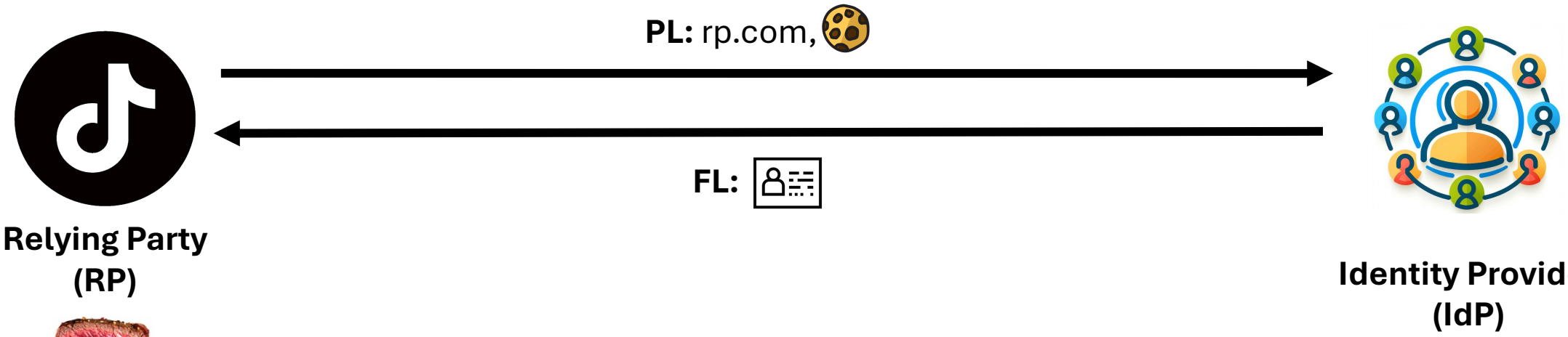
SSO Privacy Leaks

Full Leak (FL):

SSO Privacy Leaks

Full Leak (FL):

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

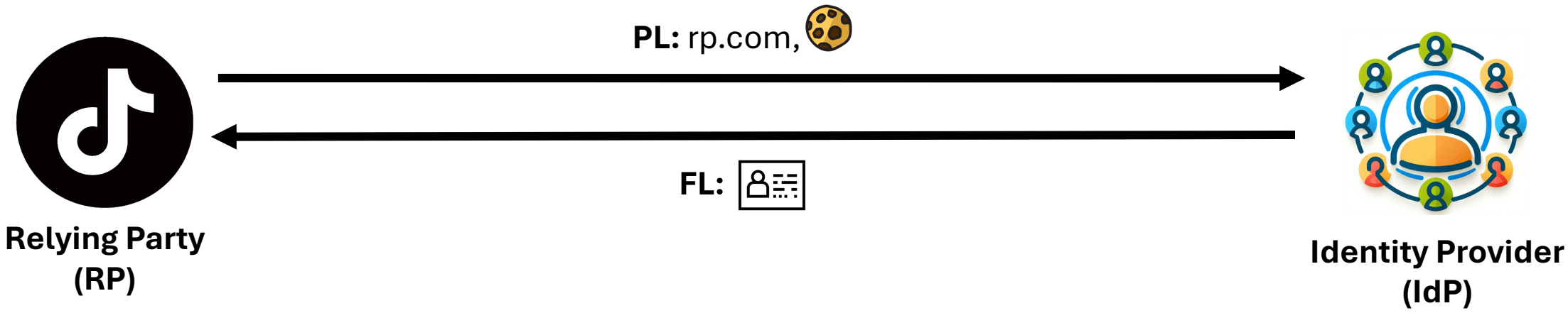


SSO Privacy Leaks

The RP learns the user's identity!

Full Leak (FL):

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



SSO Hidden Login Request Example

Fb-Ar:

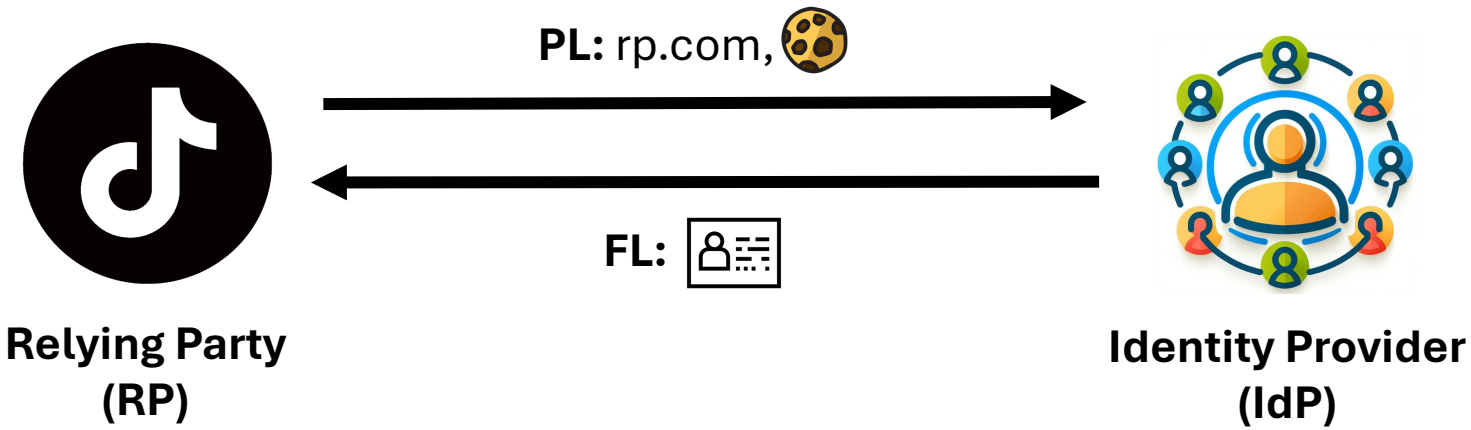
{"user_id":"122127858914299952","enforce_https":true,"access_token":"EAAAAC0VzZBQYBO0mAuoGoNeD3h76DXtPi
aCJD13tEAOykHxouuxZBZBZB2h4OsxjV3K5EplTcc
OIB0YGZCwppKQ2LKlNa9UZD","signed_request":"
RGRuRWlIN1Rwd1VJd1JxeXJxQVRUaUs3cTNQaFlf
WpmUjdPSUxMdnFJakZWcmozM1A0VmhySUt4X0I
uaTVRSzBjNWMwWUhxV1VnbHRMbmJRZGVjYzBy
VFuS1RTVXprR2VadjBvdzVfVDd0SjZwOHJOaHFiS
dRN2laSW5fX3l0VzJuVkdsN0kxT1g2MzNWX1JjW
ib2F1dGhfdG9rZW4iOiJFQUFBQUMwVnpaQlFZQk
lcGoxa1dQaFVCRHJYRmIwN29WVjA0aVV1UjM4b
M0s1RXBsVGNjYm44UGRoNDZLcUt4N1hjV0w3a3
VUdaQ3dwcEtRMkxLbE5hOVVaRCIsImFsZ29yaXR
","expires_in":5181455,"graph_domain":"facebook
","data_access_expiration_time":1739700837,"long_lived_token":"EAAAAC0VzZBQYBO0mAuoGoNeD3h76DXtPi6Otyae
"}

Fb-S:

connected

SSO Privacy Leaks

Escalated Leak (EL):

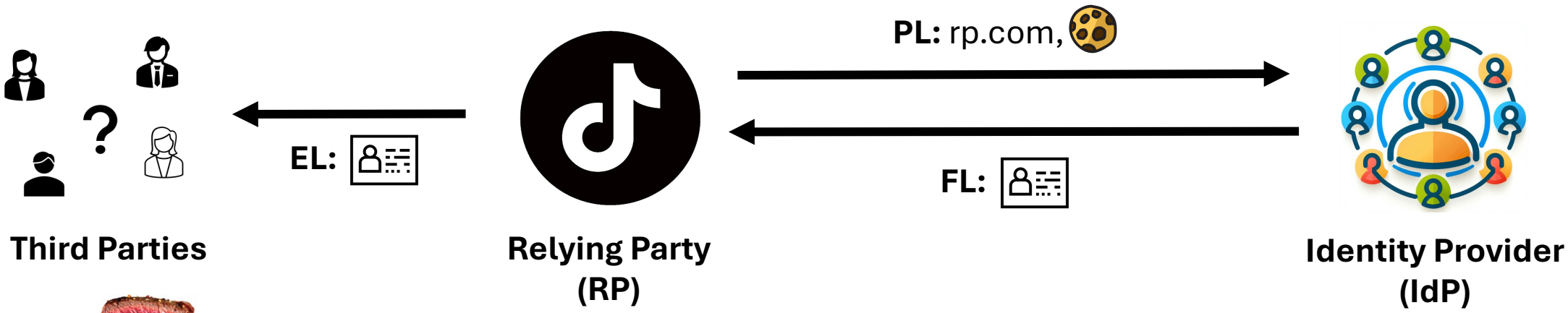


SSO Privacy Leaks

Third parties learn the user's identity!

Escalated Leak (EL):

- User's identity



Methodik und Ergebnisse

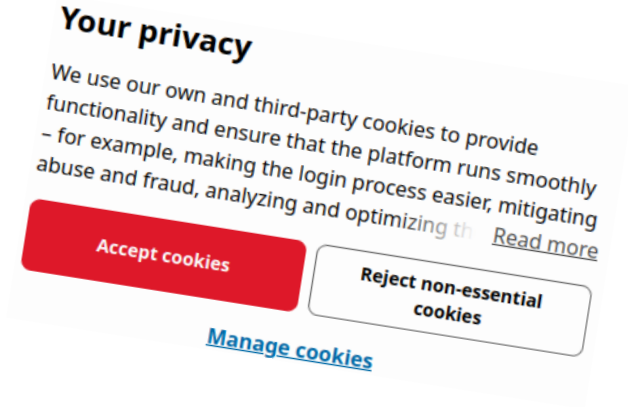
Wie sind wir vorgegangen?

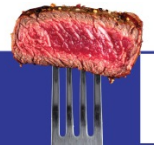
Methodology

1. Partial Leaks
   - Top 1M Tranco domains
   - Searching for hidden SSO requests[1]

Scan execution:

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





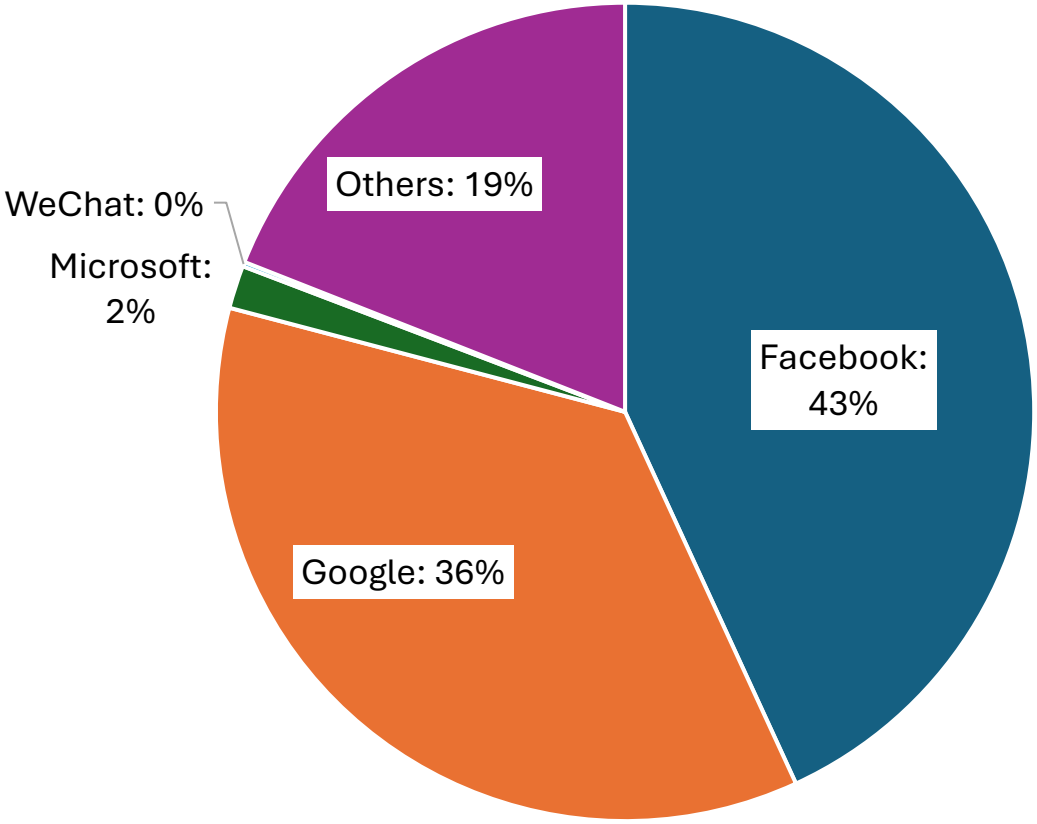
[1] 11 well known IdPs and generic pattern

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

Results – Partial Leaks



Partial leaks

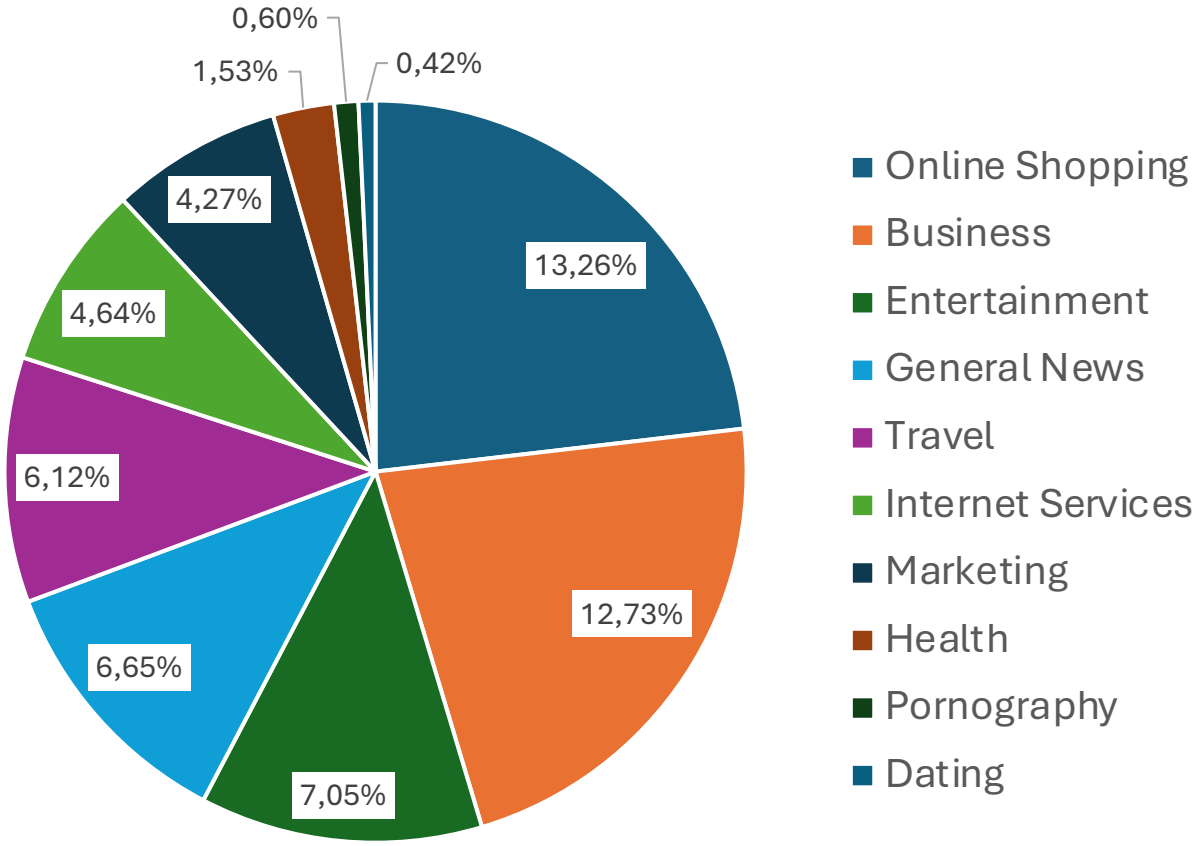
- ~11k partial leaks in total
- ~1k previously unknown IdPs
  - shop.app
  - auth0.com
  - q4inc.com
  - newscorpaustralia.com

<u>SDKs are the main reason for privacy leaks in SSO</u>

Results – Partial Leak Categories

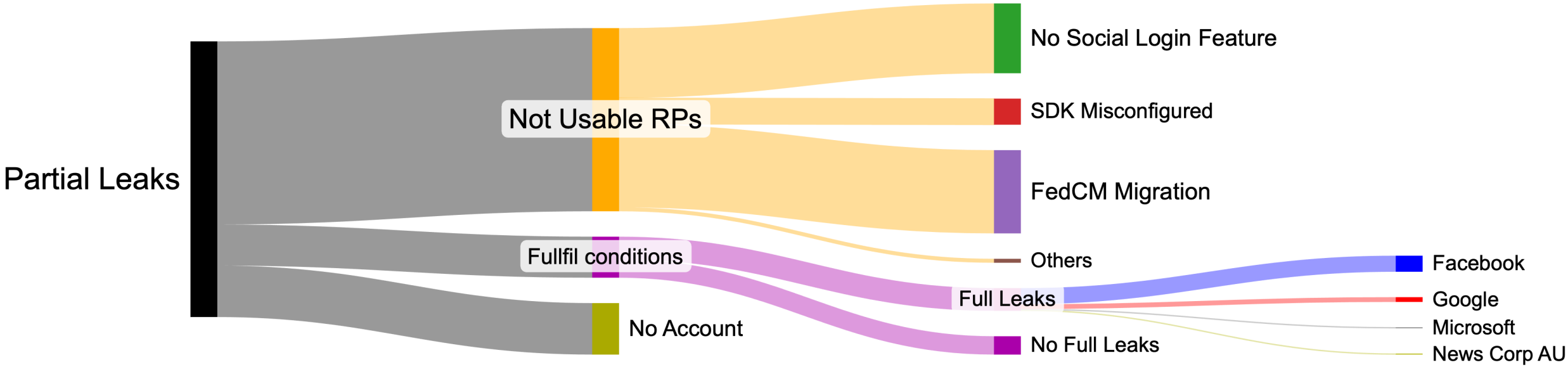
Leak Categories

- Categories vary widely
- Privacy sensible categories



<u>These categories may reveal much about problems, fears, needs, and attitudes of users.</u>

Results – Full Leaks



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

Results – Escalated Leaks

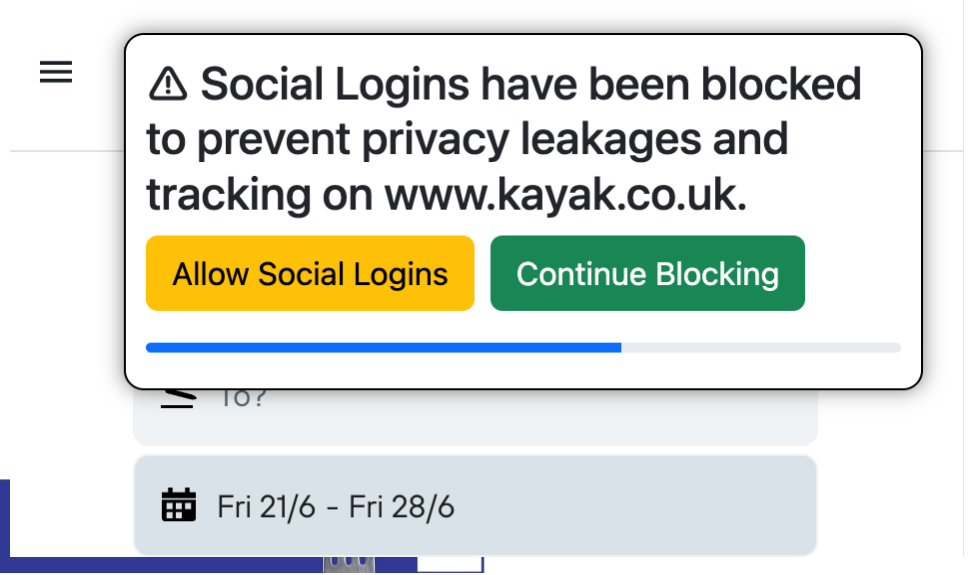
Escalated Leaks

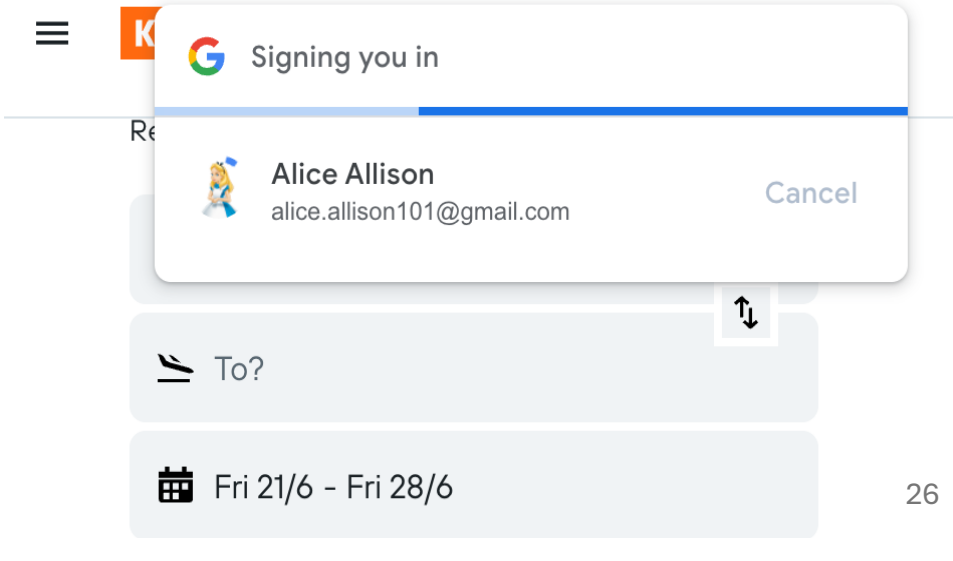
- Only 6 websites leaked their tokens to a third party
  - Facebook: 4
  - Google: 2

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