Fledging Will Continue Until Privacy Improves: Empirical Analysis of Google's Privacy-Preserving Advertising

Authors: Giuseppe Calderonio, Mir Masood Ali, and Jason Polakis

Presenter: Dylen Greenenwald

Presentation Overview

- Summary
- Background
- Measurement
- Attacks
- Discussion

Main Points

- **Motivation of the Google Privacy Sandbox**
  - Utility vs privacy tradeoff
  - Incentive structure of advertising ecosystem
  - Replacement of 3rd party cookies
- Measurement of FLEDGE ecosystem across experimental & production periods
- Introduction of PoC attacks against FLEDGE

Main Points

- Utility vs privacy tradeoff that motivates the Google Privacy Sandbox
- **Measurement of FLEDGE ecosystem across experimental & production periods**
- Introduced proof of concept attacks against FLEDGE

Main Points

- Utility vs privacy tradeoff that motivates the Google Privacy Sandbox
- Measurement of FLEDGE ecosystem across experimental & production periods
- **Introduced proof of concept attacks against FLEDGE**

Background

Terminology

- *Buyers* refer to any entity who manages the purchase of ad space
- *Sellers* refer to any entity who manages the sale of ad space
- *Ad networks* refer to intermediaries in the ad ecosystem
- Protected Audience API ~ FLEDGE API

Terminology

- ***Buyers* refer to any entity who manages the purchase of ad space**
  - e.g., advertisers, Demand-Side Platforms (DSPs)
- *Sellers* refer to any entity who manages the sale of ad space
- *Ad networks* refer to intermediaries in the ad ecosystem
- Protected Audience API ~ FLEDGE API

Terminology

- *Buyers* refer to any entity who manages the purchase of ad space
- ***Sellers* refer to any entity who manages the sale of ad space**
  - e.g., publishers, Supply-Side Platforms (SSPs)
- *Ad networks* refer to intermediaries in the ad ecosystem
- Protected Audience API ~ FLEDGE API

Terminology

- *Buyers* refer to any entity who manages the purchase of ad space
- *Sellers* refer to any entity who manages the sale of ad space
- ***Ad networks* refer to intermediaries in the ad ecosystem**
  - e.g., DSPs, SSPs, ad exchanges
- Protected Audience API ~ FLEDGE API

Terminology

- *Buyers* refer to any entity who manages the purchase of ad space
- *Sellers* refer to any entity who manages the sale of ad space
- *Ad networks* refer to intermediaries in the ad ecosystem
- **Protected Audience API ~ FLEDGE API**

Terminology

Questions?

- *Buyers* refer to any entity who manages the purchase of ad space
- *Sellers* refer to any entity who manages the sale of ad space
- *Ad networks* refer to intermediaries in the ad ecosystem
- Protected Audience API ~ FLEDGE API

The Protected Audience (FLEDGE)

- ***Intended*** **Privacy Advancements**

The Protected Audience (FLEDGE)

- *Intended* **Privacy Advancements**
  1. **The *browser* holds info about user interests.**
  2. Advertisers *cannot combine interests* with other information about users.
  3. Publishers and intermediaries are *not permitted to learn* about user ad interests.

The Protected Audience (FLEDGE)

- *Intended* **Privacy Advancements**
  1. The *browser* holds info about user interests.
  2. **Advertisers *cannot combine interests* with other information about users.**
  3. Publishers and intermediaries are *not permitted to learn* about user ad interests.

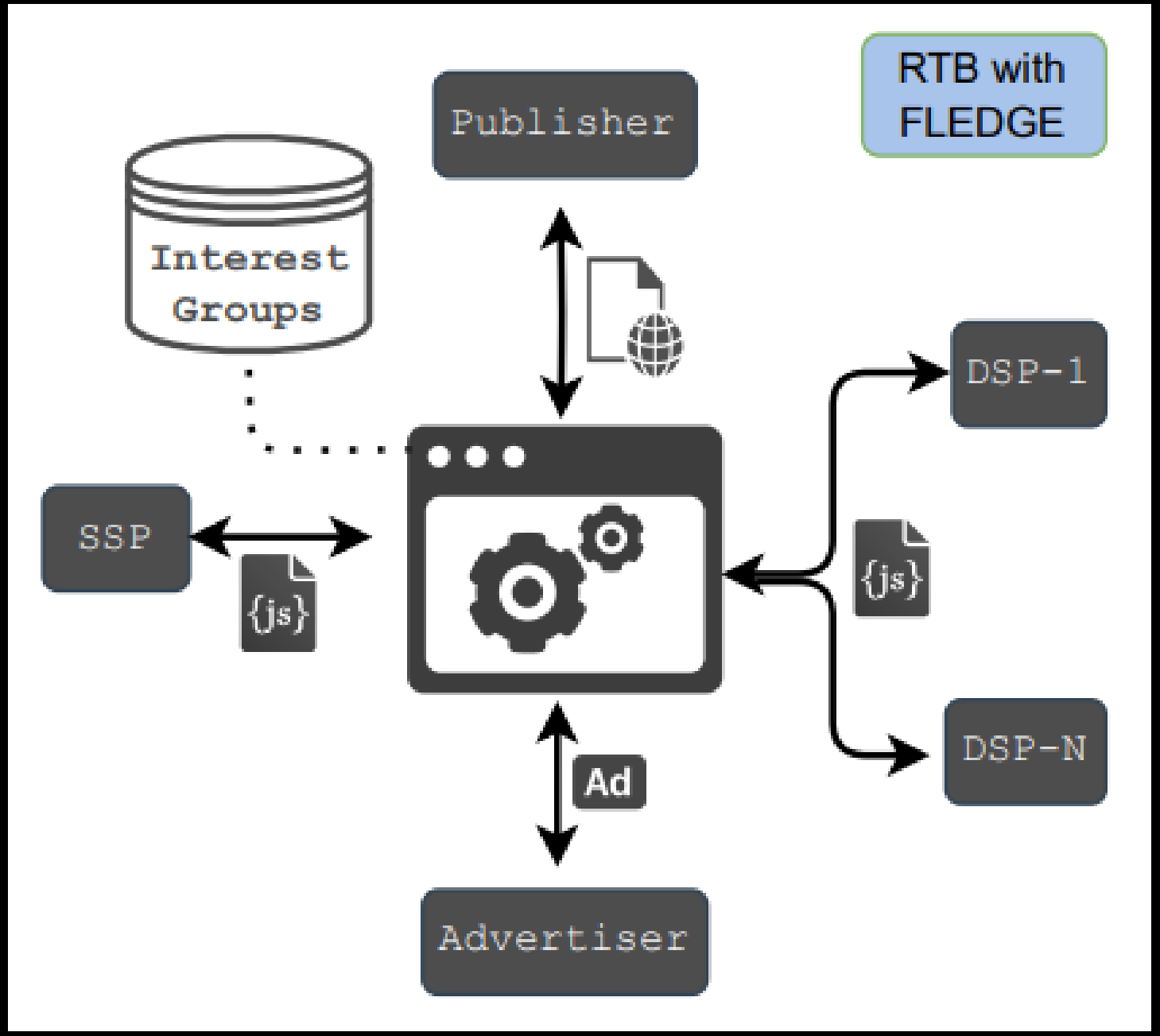
The Protected Audience (FLEDGE)

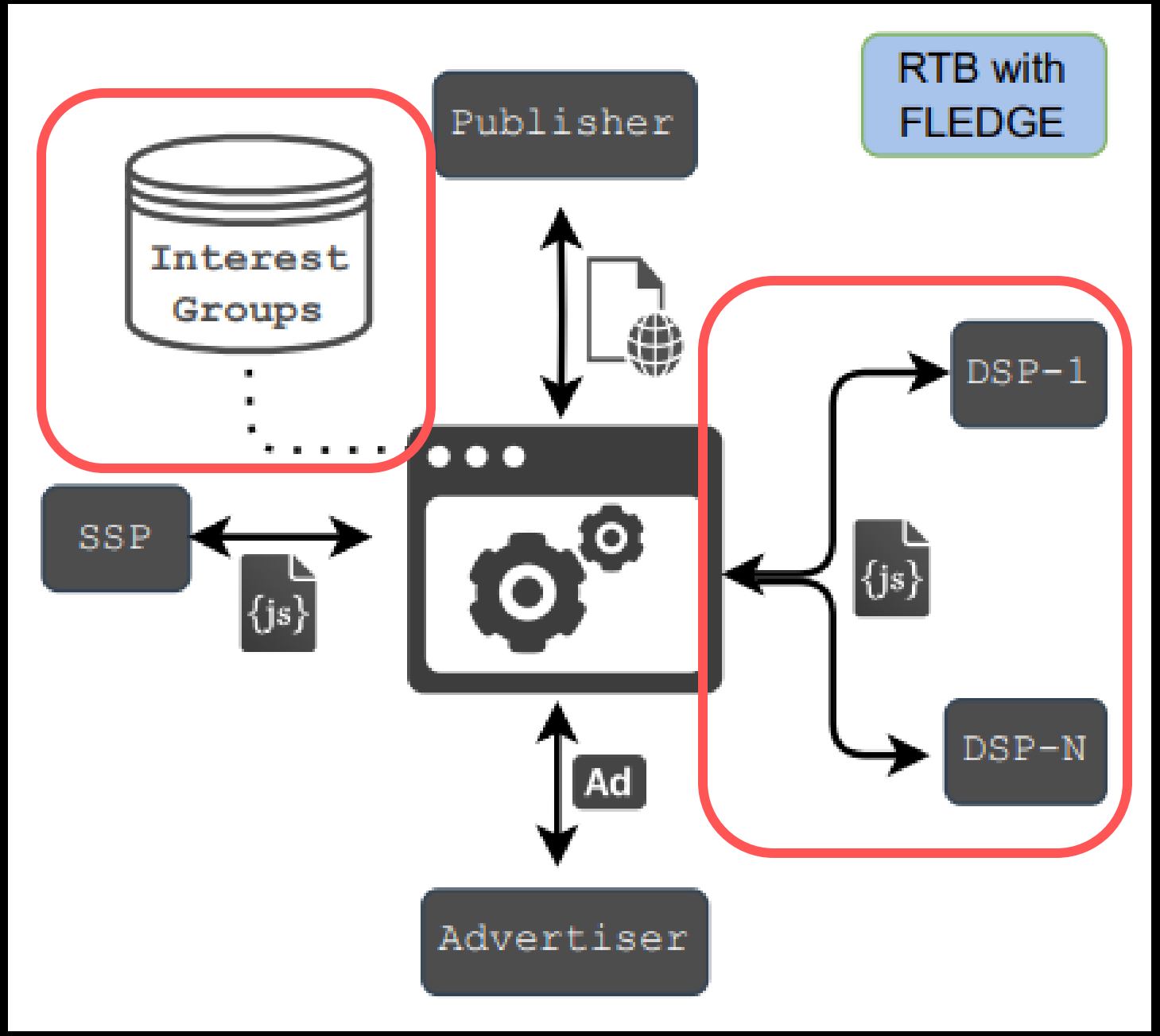
- *Intended* **Privacy Advancements**
  1. The *browser* holds info about user interests.
  2. **Advertisers *cannot combine interests* with other information about users.**
  3. Publishers and intermediaries are *not permitted to learn* about user ad interests.

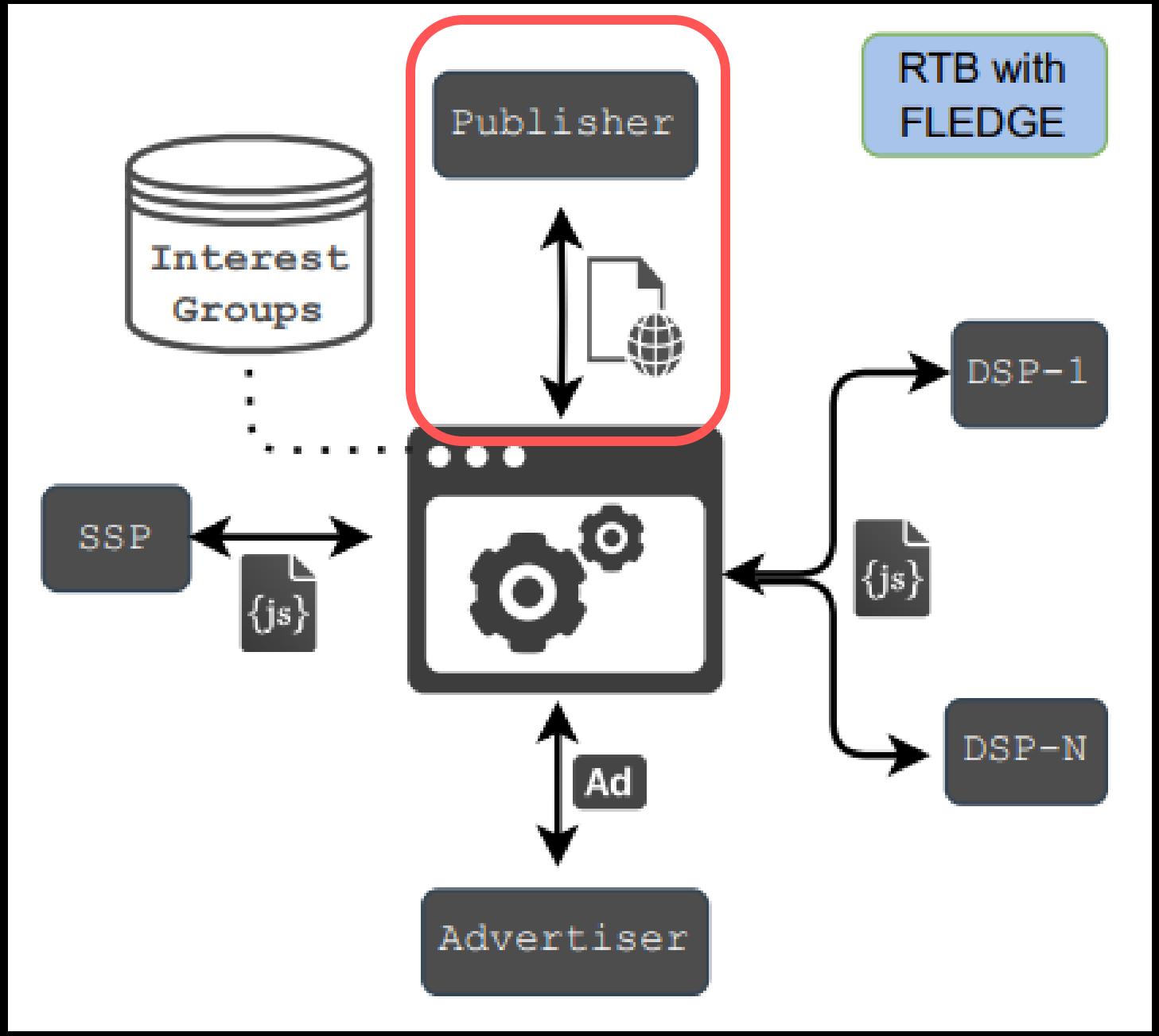
Why is this important?

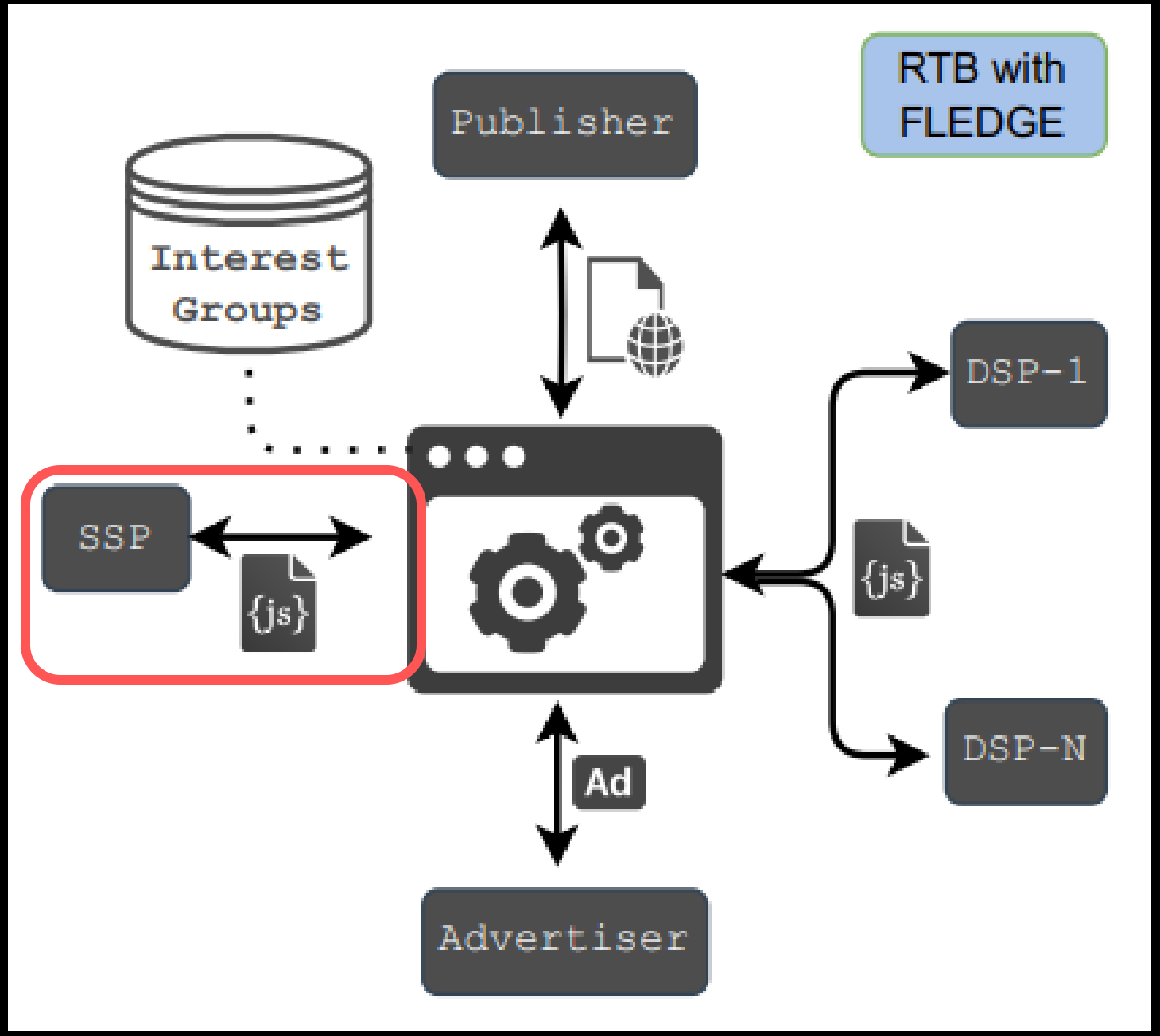
The Protected Audience (FLEDGE)

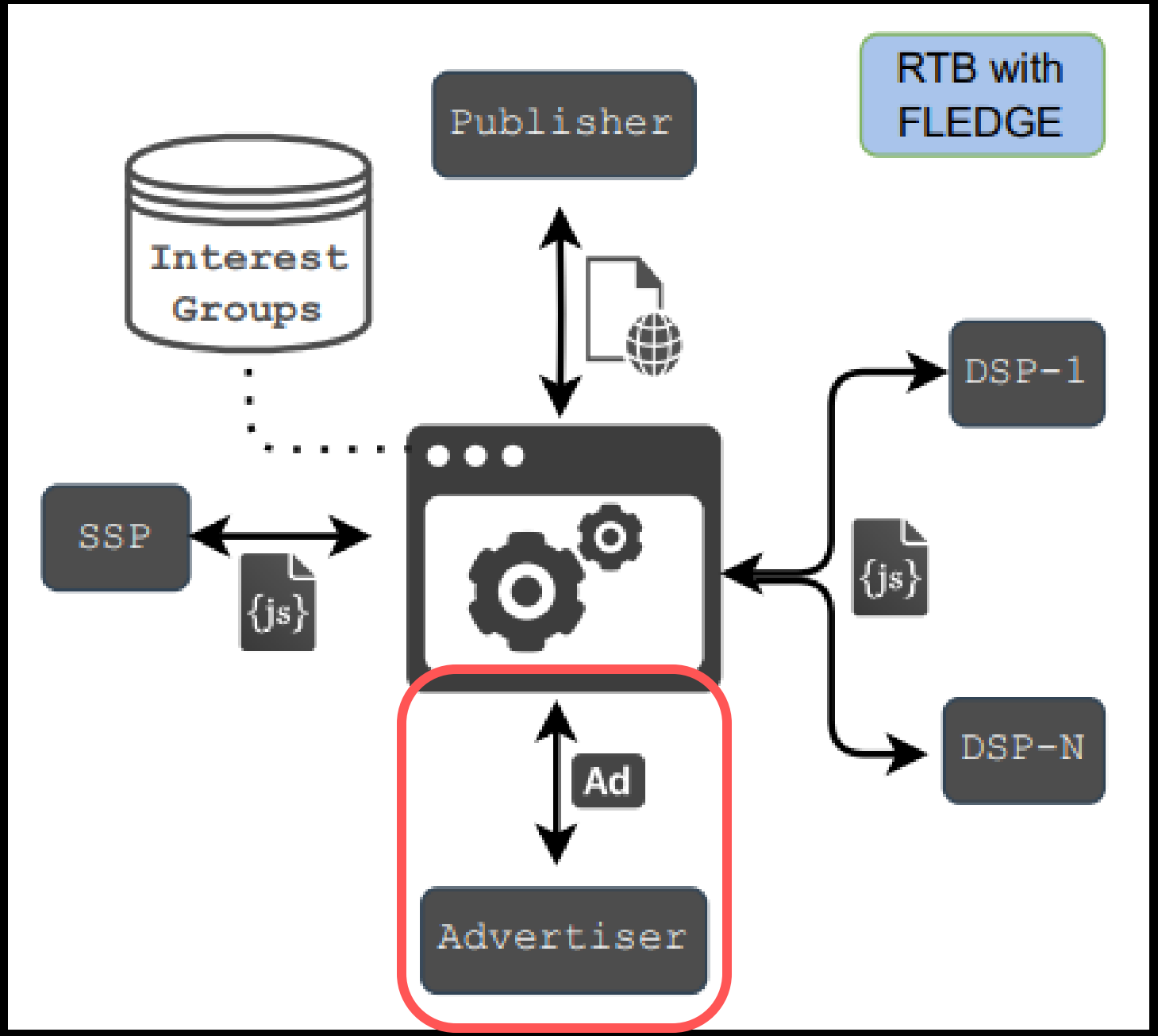
- *Intended* **Privacy Advancements**
  1. The *browser* holds info about user interests.
  2. Advertisers *cannot combine interests* with other information about users.
  3. **Publishers and intermediaries are *not permitted to learn* about user ad interests.**


RTB with FLEDGE
Publisher
Interest Groups
SSP
{js}
DSP-1
{js}
DSP-N
Ad
Advertiser

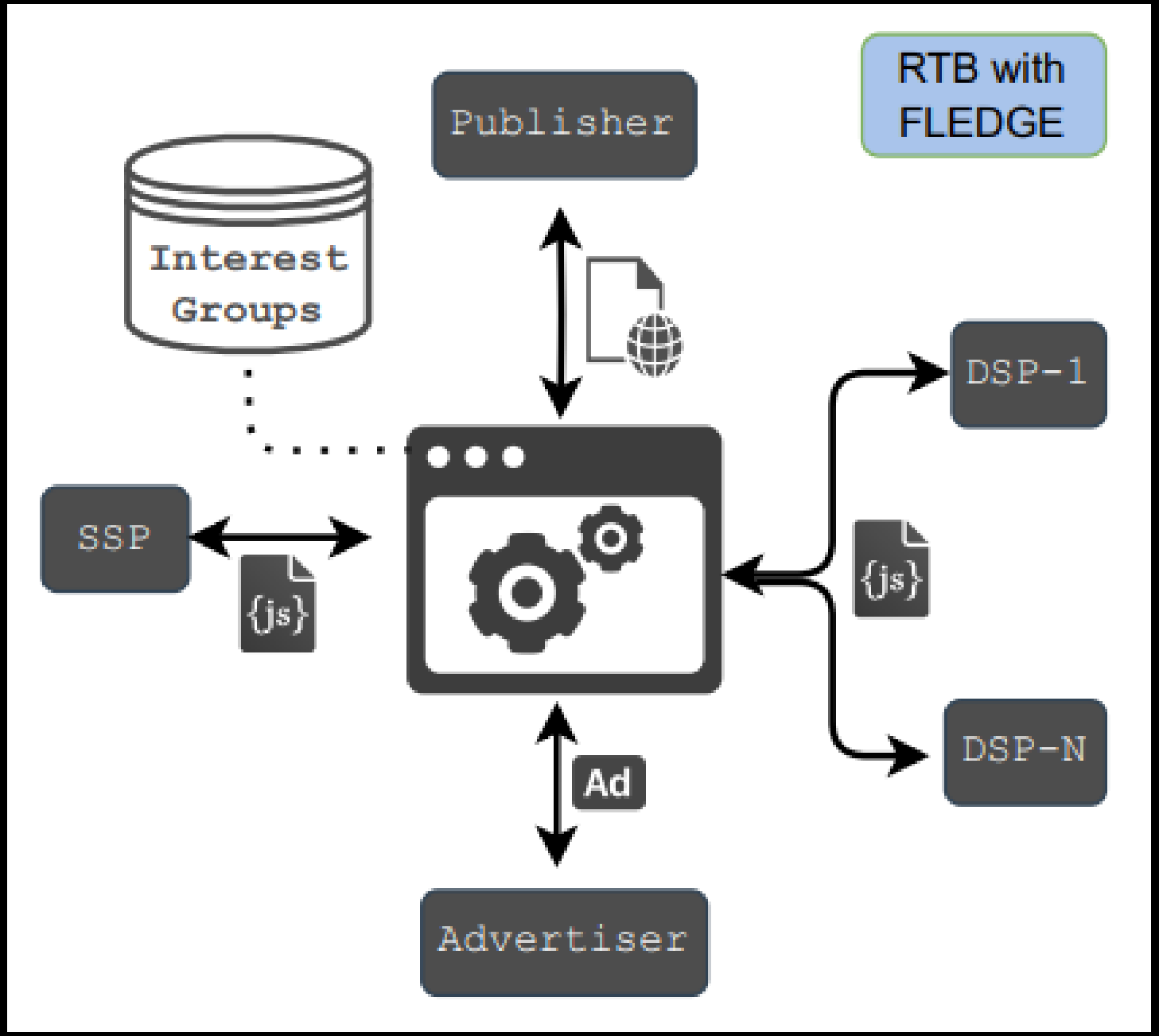

RTB with FLEDGE
Publisher
Interest Groups
SSP
{js}
DSP-1
{js}
DSP-N
Ad
Advertiser


RTB with FLEDGE
Publisher
Interest Groups
SSP
{js}
DSP-1
{js}
DSP-N
Ad
Advertiser


RTB with FLEDGE
Publisher
Interest Groups
SSP
{js}
DSP-1
{js}
DSP-N
Ad
Advertiser


RTB with FLEDGE
Publisher
Interest Groups
SSP
{js}
DSP-1
{js}
DSP-N
Ad
Advertiser

Questions?


RTB with FLEDGE
Publisher
Interest Groups
DSP-1
SSP
{js}
{js}
Ad
DSP-N
Advertiser

Measurements

Results

- **Notable artifacts**
  - Publishers
  - Sellers
  - Advertisers
  - Auctions

Results

- Notable artifacts
  - **Publishers**
    - **~10% of top 70k sites utilize FLEDGE**
    - 100% of FLEDGE API usage performed by 3rd parties
  - Sellers
  - Advertisers
  - Auctions

Results

- Notable artifacts
  - **Publishers**
    - ~10% of top 70k sites utilize FLEDGE
    - **100% of FLEDGE API usage performed by 3rd parties**
  - Sellers
  - Advertisers
  - Auctions

Takeaways?

Results

- Notable artifacts
  - Publishers
  - **Sellers**
    - **99.8% of auctions were ran by Google**
  - Advertisers
  - Auctions

Table 1: Overview of sellers over time.

Month	Seller	#Publishers	#Auctions
June	securepubads.g.doubleclick.net	1,761	5,738
July	securepubads.g.doubleclick.net	1,038	2,960
	cdn.mediago.io	1	1
September	securepubads.g.doubleclick.net	565	3,243
	cdn.mediago.io	9	17

Results

- Notable artifacts
  - Publishers
  - Sellers
  - **Advertisers**
    - **Only 7 advertisers adding browsers to interest groups**
  - Auctions

Wow!

Table 2: Interest groups' `join` and `leave` actions.

Owner	#Publishers	Interest Groups #Joined	#Left
td.doubleclick.net	2,924	12,190	2,533
fledge.as.criteo.com	370	880	-
fledge.teads.tv	229	1	-
fledge.eu.criteo.com	327	918	-
fledge.us.criteo.com	655	1411	-
fledge-eu.creativecdn.com	95	261	52
fledge-usa.creativecdn.com	65	133	37
fledge-asia.creativecdn.com	56	129	17
f.creativecdn.com	9	9	-
googleads.g.doubleclick.net	5	5	-
cdn.mediago.io	5	1	-
at-us-east.amazon-adsystem.com	1	1	-
adthrive.com	4	4	-

Results

- Notable artifacts
  - Publishers
  - Sellers
  - Advertisers
  - **Auctions**
    - ~21 scoring signals used on average during auctions
    - ~10 bidding signals passed to each buyer (via `perBuyerSignals`) during auctions
    - Avg (often obfuscated) signal depth of ~8

Results

- Notable artifacts
  - Publishers
  - Sellers
  - Advertisers
  - **Auctions**
    - ~21 scoring signals used on average during auctions
    - ~10 bidding signals passed to each buyer (via `perBuyerSignals`) during auctions
    - Avg (often obfuscated) signal depth of ~8

So what?

Attacks

Threat Model

- Web attacker...
  - **Embedded as third-party resource** (e.g., via a `<script>`, `<iframe>` tag)
  - Using FLEDGE APIs (e.g., `navigator.runAdAuction()`)
  - Participating as buyer and/or seller in ad auctions
  - Targeting arbitrary Chrome user (past v117)

Threat Model

- Web attacker...
  - Embedded as third-party resource (e.g., via a `<script>`, `<iframe>` tag)
  - **Using FLEDGE APIs** (e.g., `navigator.runAdAuction()`)
  - Participating as buyer and/or seller in ad auctions
  - Targeting arbitrary Chrome user (past v117)

Threat Model

- Web attacker...
  - Embedded as third-party resource (e.g., via a `<script>`, `<iframe>` tag)
  - Using FLEDGE APIs (e.g., `navigator.runAdAuction()`)
  - **Participating as buyer and/or seller in ad auctions**
  - Targeting arbitrary Chrome user (past v117)

Threat Model

- Web attacker...
  - Embedded as third-party resource (e.g., via a `<script>`, `<iframe>` tag)
  - Using FLEDGE APIs (e.g., `navigator.runAdAuction()`)
  - Participating as buyer and/or seller in ad auctions
  - **Targeting arbitrary Chrome user** (past v117)

What do you see?

Table 3: Summary of our attacks, the mechanism they misuse, privacy advancements they violate, and planned mitigations.

Type	Mechanism	Field	Attacker Role	Future Mitigation	Violation
Tracking	Bidding Helpers	biddingWasmHelperUrl	Advertiser & Seller	Not Planned	PA2
Tracking	Real-time Rendering of Winning Bids	biddingLogicUrl	Advertiser & Seller	Fenced Frames	PA2
Tracking	Bidding Logic	ads	Advertiser & Seller	Not Planned	PA2, PA3
Tracking	Trusted Bidding Signals	trustedBiddingSignals	Advertiser & Seller	Trusted Server	PA1, PA2
Tracking	Non-aggregated Win Reporting	reportWin	Advertiser & Seller	Private Aggregation	PA2, PA3
Tracking	Non-aggregated Win Reporting	sendReportTo	Advertiser & Seller	Private Aggregation	PA2
Tracking	Non-aggregated Event-level Reporting	reportEvent	Advertiser & Seller	Fenced Frames	PA2, PA3
Cross-site Leak	Gathering Interest Group Owners	decisionLogicUrl	Advertiser (Run Auctions)	Not Planned	PA2, PA3
Cross-site Leak	Interest Group Leaks	trustedScoringSignal	Advertiser (Run Auctions)	Trusted Server	PA1, PA2, PA3
DoS	Browser Crash	trustedBiddingSignals	Advertiser & Seller	Fixed	Other
DoS	Blocking Ad Auctions	interestGroups.sqlite3	Advertiser (Join Groups)	Not Planned	Other
Pollution	Polluting Doubleclick Interest Groups	Interest Group size limit	Other (Add iframes)	Not Planned	Other

What do you see?

Table 3: Summary of our attacks, the mechanism they misuse, privacy advancements they violate, and planned mitigations.

Type	Mechanism	Field	Attacker Role	Future Mitigation	Violation
Tracking	Bidding Helpers	biddingWasmHelperUrl	Advertiser & Seller	Not Planned	PA2
Tracking	Real-time Rendering of Winning Bids	biddingLogicUrl	Advertiser & Seller	Fenced Frames	PA2
Tracking	Bidding Logic	ads	Advertiser & Seller	Not Planned	PA2, PA3
Tracking	Trusted Bidding Signals	trustedBiddingSignals	Advertiser & Seller	Trusted Server	PA1, PA2
Tracking	Non-aggregated Win Reporting	reportWin	Advertiser & Seller	Private Aggregation	PA2, PA3
Tracking	Non-aggregated Win Reporting	sendReportTo	Advertiser & Seller	Private Aggregation	PA2
Tracking	Non-aggregated Event-level Reporting	reportEvent	Advertiser & Seller	Fenced Frames	PA2, PA3
Cross-site Leak	Gathering Interest Group Owners	decisionLogicUrl	Advertiser (Run Auctions)	Not Planned	PA2, PA3
Cross-site Leak	Interest Group Leaks	trustedScoringSignal	Advertiser (Run Auctions)	Trusted Server	PA1, PA2, PA3
DoS	Browser Crash	trustedBiddingSignals	Advertiser & Seller	Fixed	Other
DoS	Blocking Ad Auctions	interestGroups.sqlite3	Advertiser (Join Groups)	Not Planned	Other
Pollution	Polluting Doubleclick Interest Groups	Interest Group size limit	Other (Add iframes)	Not Planned	Other

What do you see?

Table 3: Summary of our attacks, the mechanism they misuse, privacy advancements they violate, and planned mitigations.

Type	Mechanism	Field	Attacker Role	Future Mitigation	Violation
Tracking	Bidding Helpers	biddingWasmHelperUrl	Advertiser & Seller	Not Planned	PA2
Tracking	Real-time Rendering of Winning Bids	biddingLogicUrl	Advertiser & Seller	Fenced Frames	PA2
Tracking	Bidding Logic	ads	Advertiser & Seller	Not Planned	PA2, PA3
Tracking	Trusted Bidding Signals	trustedBiddingSignals	Advertiser & Seller	Trusted Server	PA1, PA2
Tracking	Non-aggregated Win Reporting	reportWin	Advertiser & Seller	Private Aggregation	PA2, PA3
Tracking	Non-aggregated Win Reporting	sendReportTo	Advertiser & Seller	Private Aggregation	PA2
Tracking	Non-aggregated Event-level Reporting	reportEvent	Advertiser & Seller	Fenced Frames	PA2, PA3
Cross-site Leak	Gathering Interest Group Owners	decisionLogicUrl	Advertiser (Run Auctions)	Not Planned	PA2, PA3
Cross-site Leak	Interest Group Leaks	trustedScoringSignal	Advertiser (Run Auctions)	Trusted Server	PA1, PA2, PA3
DoS	Browser Crash	trustedBiddingSignals	Advertiser & Seller	Fixed	Other
DoS	Blocking Ad Auctions	interestGroups.sqlite3	Advertiser (Join Groups)	Not Planned	Other
Pollution	Polluting Doubleclick Interest Groups	Interest Group size limit	Other (Add iframes)	Not Planned	Other

What I see

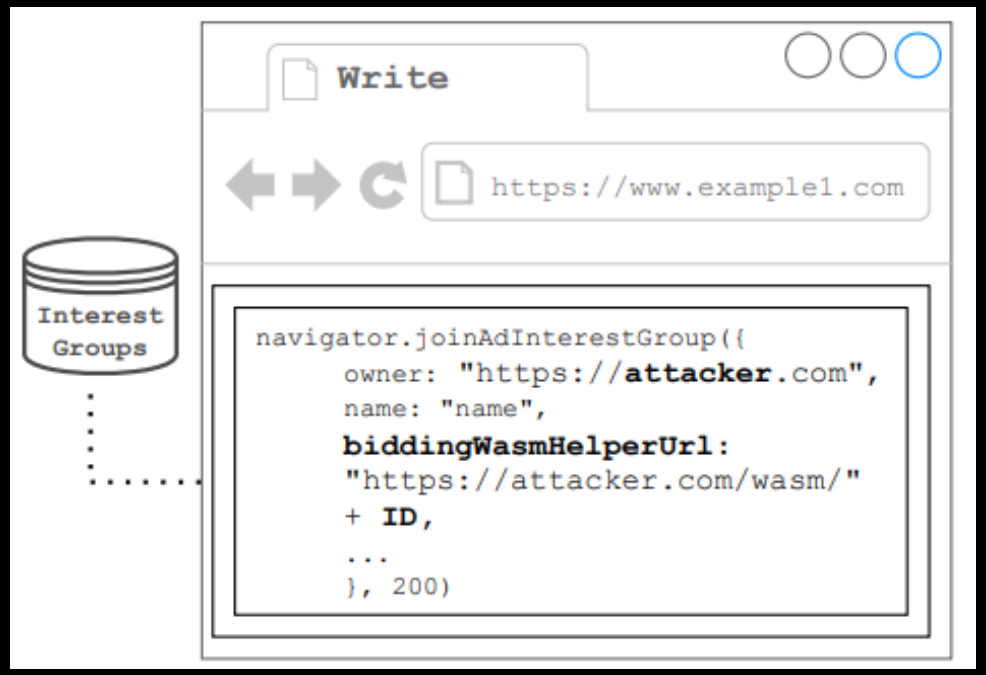
Critical attack

- Single interest group attack
- No planned mitigation

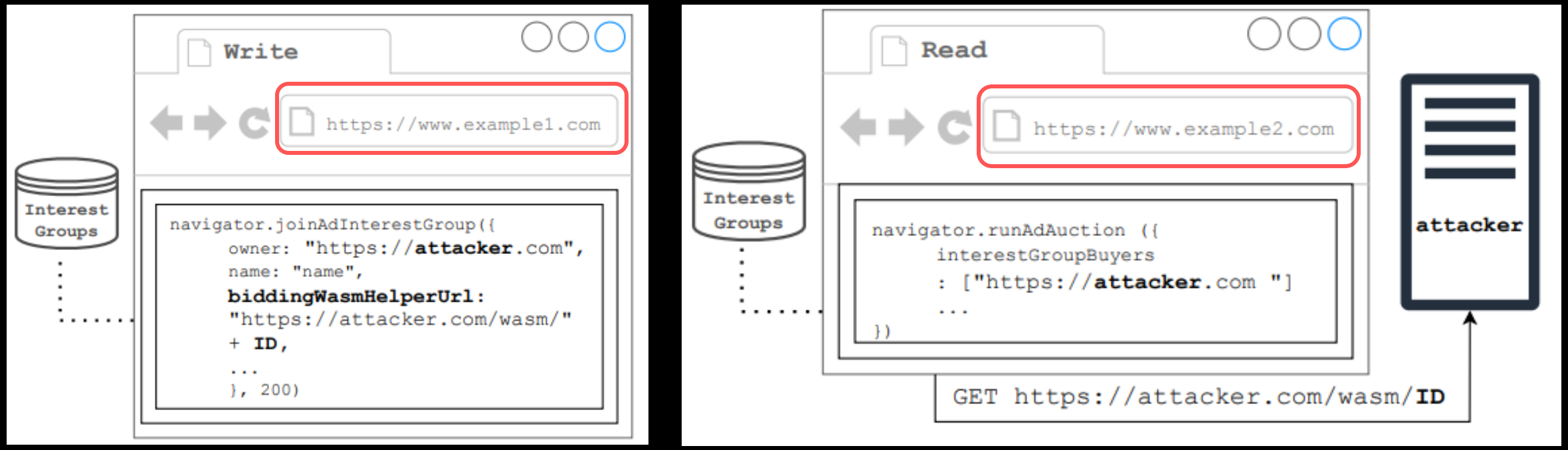
Table 3: Summary of our attacks, the mechanism they misuse, privacy advancements they violate, and planned mitigations.

Type	Mechanism	Field	Attacker Role	Future Mitigation	Violation
Tracking	Bidding Helpers	biddingWasmHelperUrl	Advertiser & Seller	Not Planned	PA2
Tracking	Real-time Rendering of Winning Bids	biddingLogicUrl	Advertiser & Seller	Fenced Frames	PA2
Tracking	Bidding Logic	ads	Advertiser & Seller	Not Planned	PA2, PA3
Tracking	Trusted Bidding Signals	trustedBiddingSignals	Advertiser & Seller	Trusted Server	PA1, PA2
Tracking	Non-aggregated Win Reporting	reportWin	Advertiser & Seller	Private Aggregation	PA2, PA3
Tracking	Non-aggregated Win Reporting	sendReportTo	Advertiser & Seller	Private Aggregation	PA2
Tracking	Non-aggregated Event-level Reporting	reportEvent	Advertiser & Seller	Fenced Frames	PA2, PA3
Cross-site Leak	Gathering Interest Group Owners	decisionLogicUrl	Advertiser (Run Auctions)	Not Planned	PA2, PA3
Cross-site Leak	Interest Group Leaks	trustedScoringSignal	Advertiser (Run Auctions)	Trusted Server	PA1, PA2, PA3
DoS	Browser Crash	trustedBiddingSignals	Advertiser & Seller	Fixed	Other
DoS	Blocking Ad Auctions	interestGroups.sqlite3	Advertiser (Join Groups)	Not Planned	Other
Pollution	Polluting Doubleclick Interest Groups	Interest Group size limit	Other (Add iframes)	Not Planned	Other

Bidding Helper Attack Overview

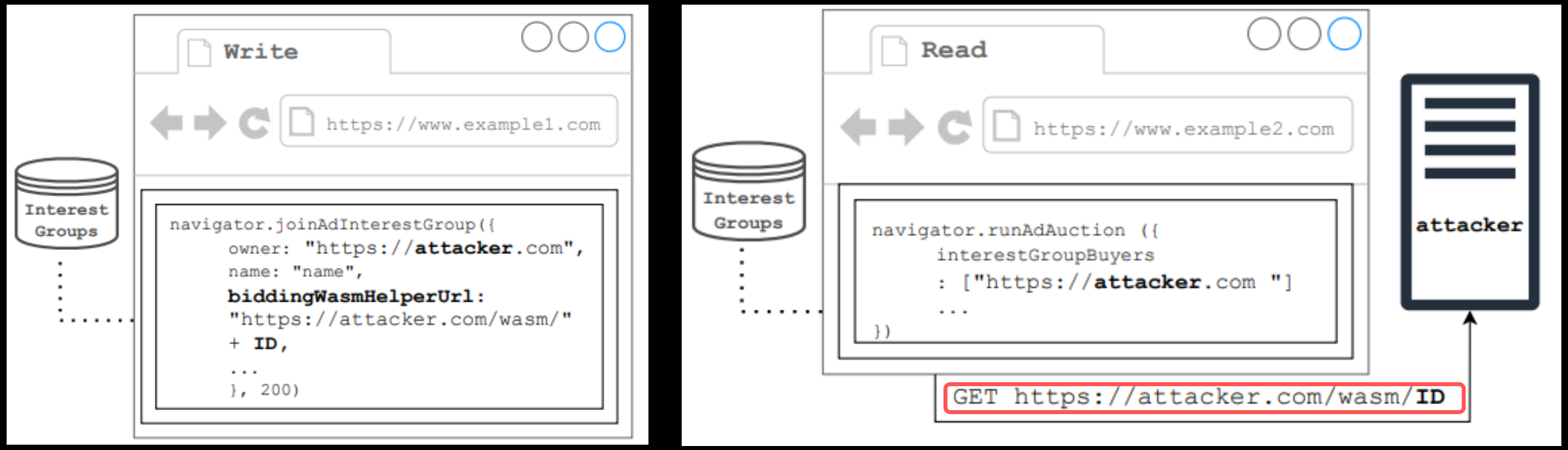


Bidding Helper Attack Overview

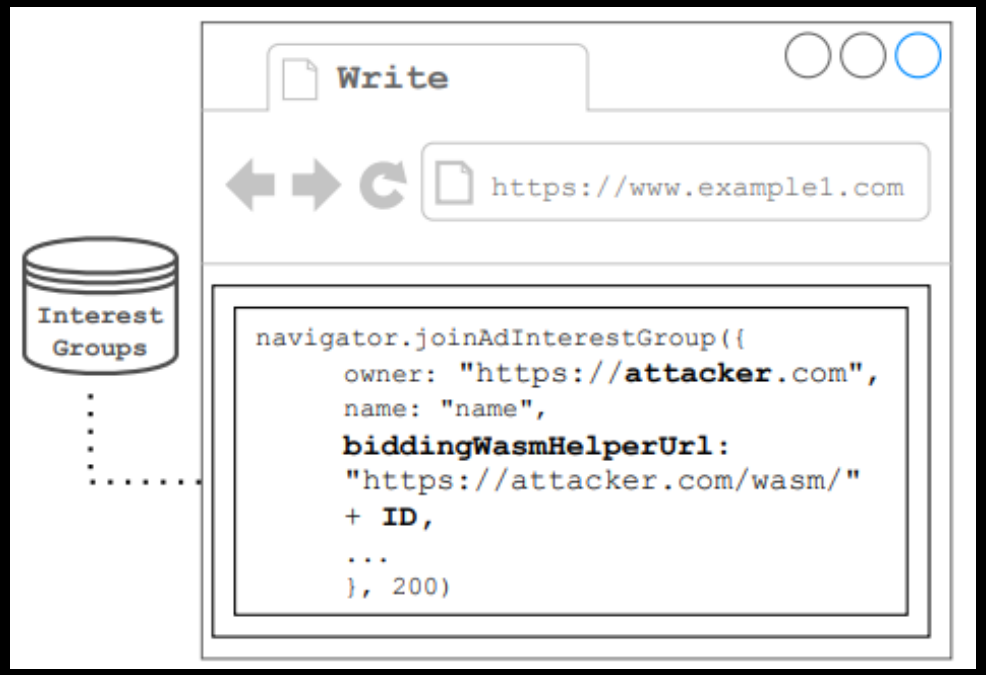


Bidding Helper Attack Overview

Bidding Helper Attack Overview



Bidding Helper Attack Overview



Questions?

What I see

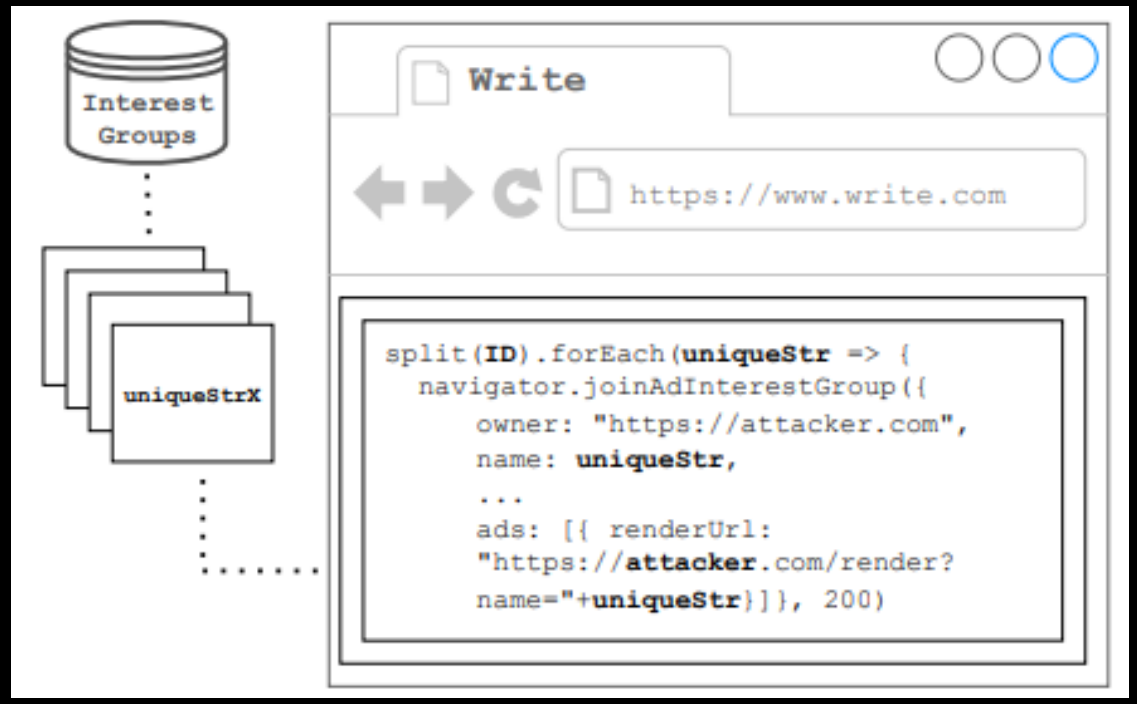
Critical attack

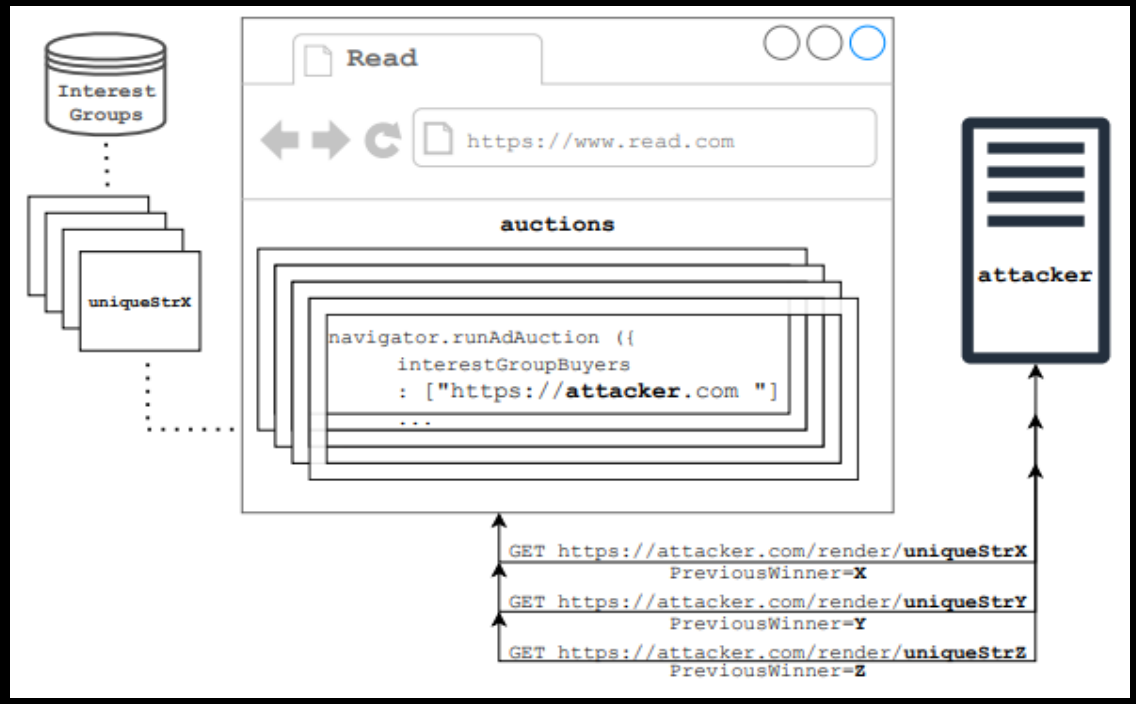
- Multiple interest group attack
- k-anonymity: k=10
- Fenced Frames required "no sooner than 2026"

Table 3: Summary of our attacks, the mechanism they misuse, privacy advancements they violate, and planned mitigations.

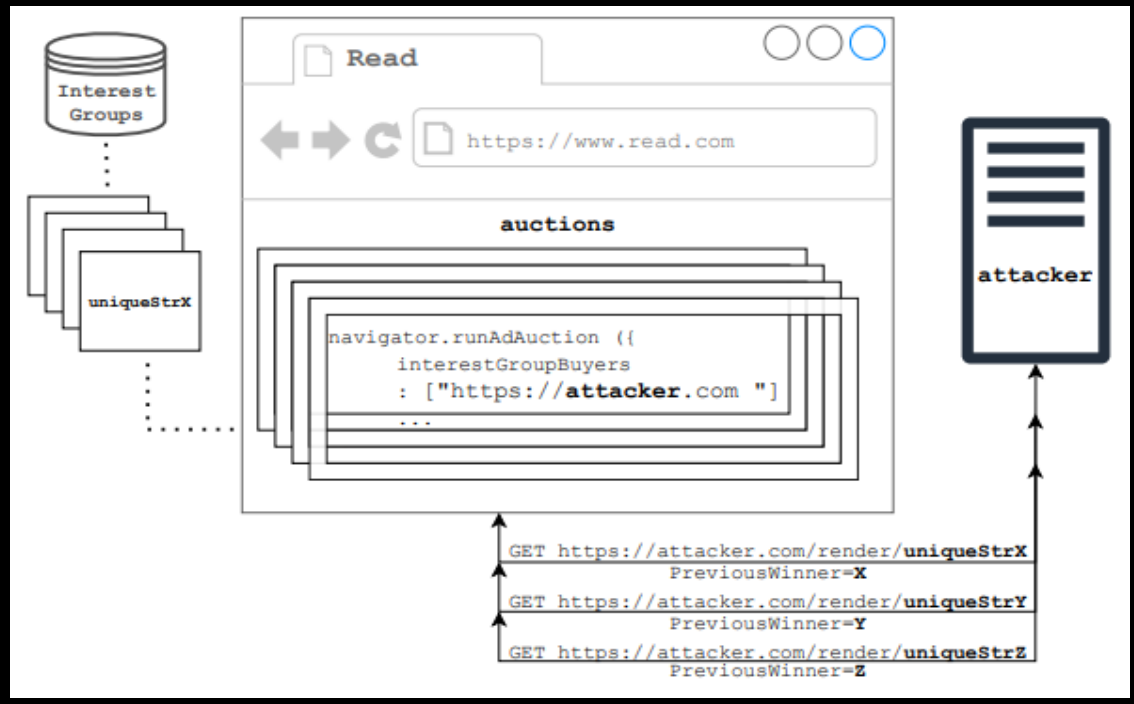
Type	Mechanism	Field	Attacker Role	Future Mitigation	Violation
Tracking	Bidding Helpers	biddingWasmHelperUrl	Advertiser & Seller	Not Planned	PA2
Tracking	Real-time Rendering of Winning Bids	biddingLogicUrl	Advertiser & Seller	Fenced Frames	PA2
Tracking	Bidding Logic	ads	Advertiser & Seller	Not Planned	PA2, PA3
Tracking	Trusted Bidding Signals	trustedBiddingSignals	Advertiser & Seller	Trusted Server	PA1, PA2
Tracking	Non-aggregated Win Reporting	reportWin	Advertiser & Seller	Private Aggregation	PA2, PA3
Tracking	Non-aggregated Win Reporting	sendReportTo	Advertiser & Seller	Private Aggregation	PA2
Tracking	Non-aggregated Event-level Reporting	reportEvent	Advertiser & Seller	Fenced Frames	PA2, PA3
Cross-site Leak	Gathering Interest Group Owners	decisionLogicUrl	Advertiser (Run Auctions)	Not Planned	PA2, PA3
Cross-site Leak	Interest Group Leaks	trustedScoringSignal	Advertiser (Run Auctions)	Trusted Server	PA1, PA2, PA3
DoS	Browser Crash	trustedBiddingSignals	Advertiser & Seller	Fixed	Other
DoS	Blocking Ad Auctions	interestGroups.sqlite3	Advertiser (Join Groups)	Not Planned	Other
Pollution	Polluting Doubleclick Interest Groups	Interest Group size limit	Other (Add iframes)	Not Planned	Other

Ad Rendering Attack Overview

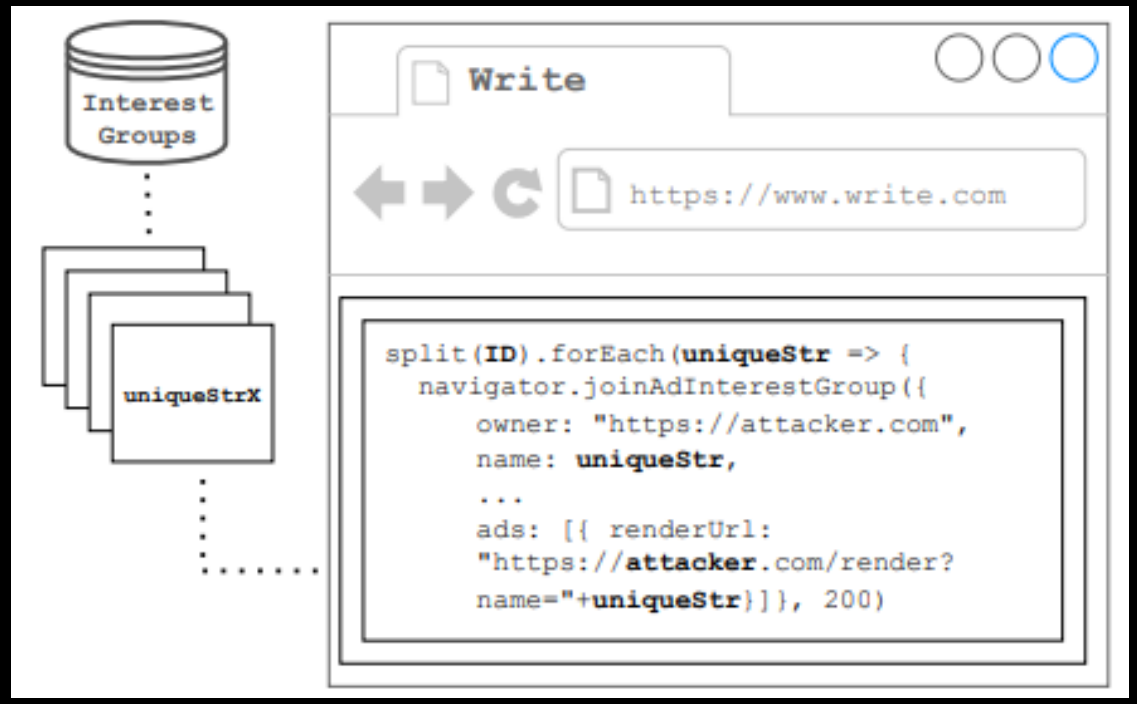


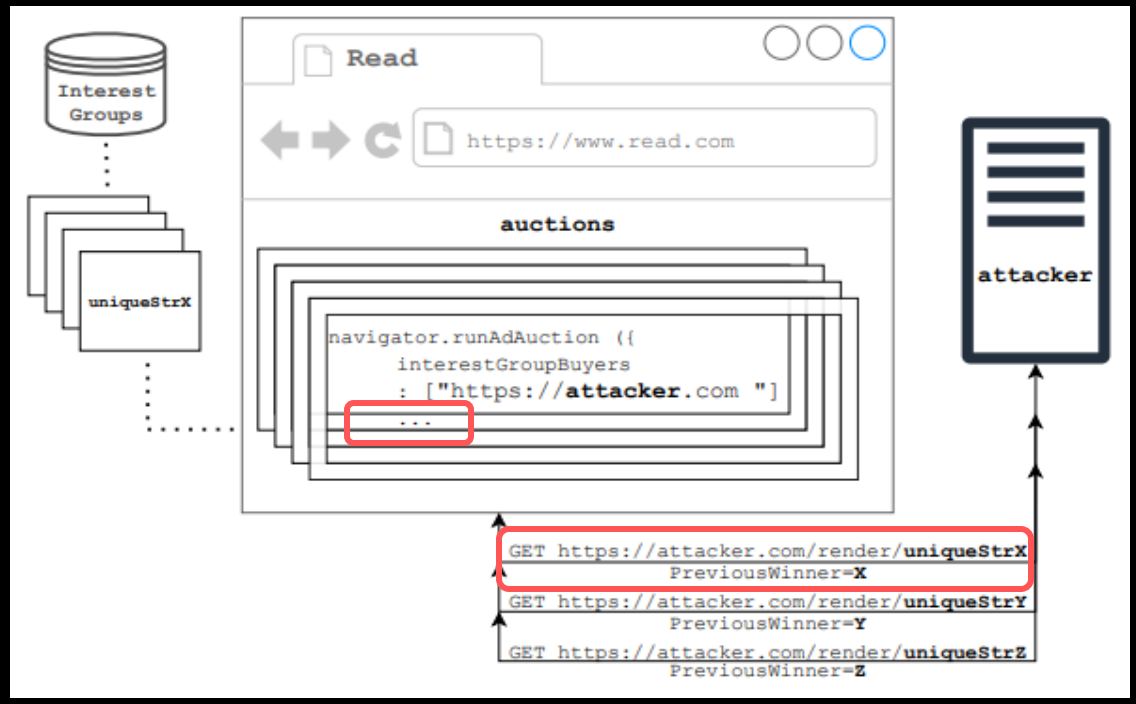


Ad Rendering Attack Overview



Ad Rendering Attack Overview





What I see

Severe attacks

- Stronger threat model
- TEEs "required no sooner than Q3 2025"
- All fundamental privacy violations

Table 3: Summary of our attacks, the mechanism they misuse, privacy advancements they violate, and planned mitigations.

Type	Mechanism	Field	Attacker Role	Future Mitigation	Violation
Tracking	Bidding Helpers	biddingWasmHelperUrl	Advertiser & Seller	Not Planned	PA2
Tracking	Real-time Rendering of Winning Bids	biddingLogicUrl	Advertiser & Seller	Fenced Frames	PA2
Tracking	Bidding Logic	ads	Advertiser & Seller	Not Planned	PA2, PA3
Tracking	Trusted Bidding Signals	trustedBiddingSignals	Advertiser & Seller	Trusted Server	PA1, PA2
Tracking	Non-aggregated Win Reporting	reportWin	Advertiser & Seller	Private Aggregation	PA2, PA3
Tracking	Non-aggregated Win Reporting	sendReportTo	Advertiser & Seller	Private Aggregation	PA2
Tracking	Non-aggregated Event-level Reporting	reportEvent	Advertiser & Seller	Fenced Frames	PA2, PA3
Cross-site Leak	Gathering Interest Group Owners	decisionLogicUrl	Advertiser (Run Auctions)	Not Planned	PA2, PA3
Cross-site Leak	Interest Group Leaks	trustedScoringSignal	Advertiser (Run Auctions)	Trusted Server	PA1, PA2, PA3
DoS	Browser Crash	trustedBiddingSignals	Advertiser & Seller	Fixed	Other
DoS	Blocking Ad Auctions	interestGroups.sqlite3	Advertiser (Join Groups)	Not Planned	Other
Pollution	Polluting Doubleclick Interest Groups	Interest Group size limit	Other (Add iframes)	Not Planned	Other

XS Leak Attacks Overview

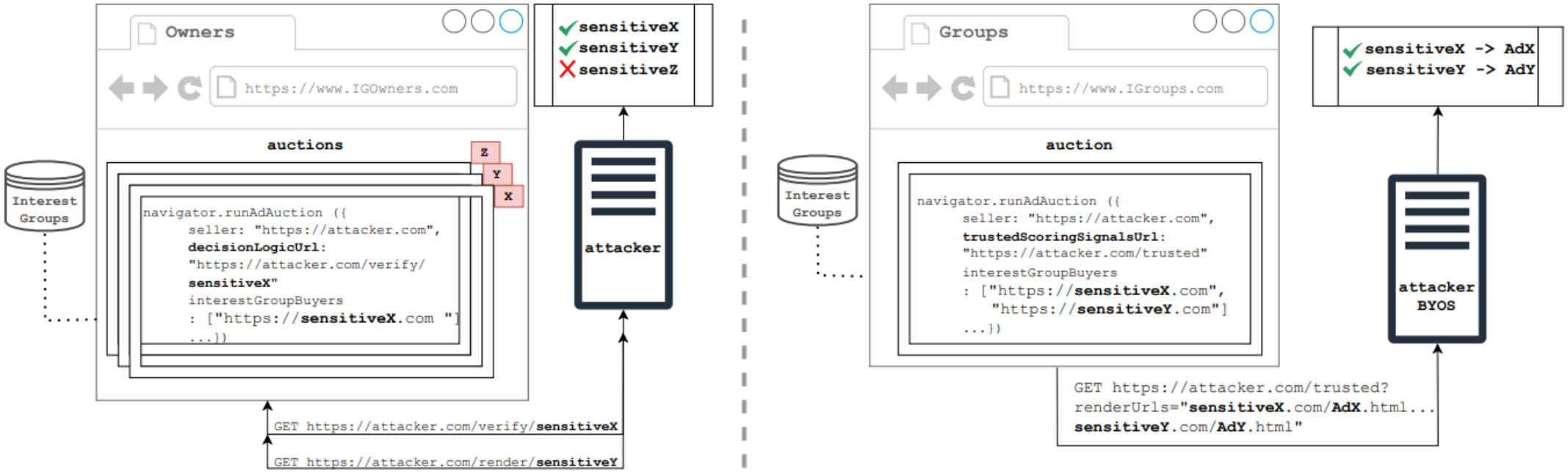


Figure 6: Cross-site leaks of owners (left) and interest group contents (right).

What I see

Serious attack

- No planned mitigations
- Usability violation

Table 3: Summary of our attacks, the mechanism they misuse, privacy advancements they violate, and planned mitigations.

Type	Mechanism	Field	Attacker Role	Future Mitigation	Violation
Tracking	Bidding Helpers	biddingWasmHelperUrl	Advertiser & Seller	Not Planned	PA2
Tracking	Real-time Rendering of Winning Bids	biddingLogicUrl	Advertiser & Seller	Fenced Frames	PA2
Tracking	Bidding Logic	ads	Advertiser & Seller	Not Planned	PA2, PA3
Tracking	Trusted Bidding Signals	trustedBiddingSignals	Advertiser & Seller	Trusted Server	PA1, PA2
Tracking	Non-aggregated Win Reporting	reportWin	Advertiser & Seller	Private Aggregation	PA2, PA3
Tracking	Non-aggregated Win Reporting	sendReportTo	Advertiser & Seller	Private Aggregation	PA2
Tracking	Non-aggregated Event-level Reporting	reportEvent	Advertiser & Seller	Fenced Frames	PA2, PA3
Cross-site Leak	Gathering Interest Group Owners	decisionLogicUrl	Advertiser (Run Auctions)	Not Planned	PA2, PA3
Cross-site Leak	Interest Group Leaks	trustedScoringSignal	Advertiser (Run Auctions)	Trusted Server	PA1, PA2, PA3
DoS	Browser Crash	trustedBiddingSignals	Advertiser & Seller	Fixed	Other
DoS	Blocking Ad Auctions	interestGroups.sqlite3	Advertiser (Join Groups)	Not Planned	Other
Pollution	Polluting Doubleclick Interest Groups	Interest Group size limit	Other (Add iframes)	Not Planned	Other

Auction Blocking Attack Overview

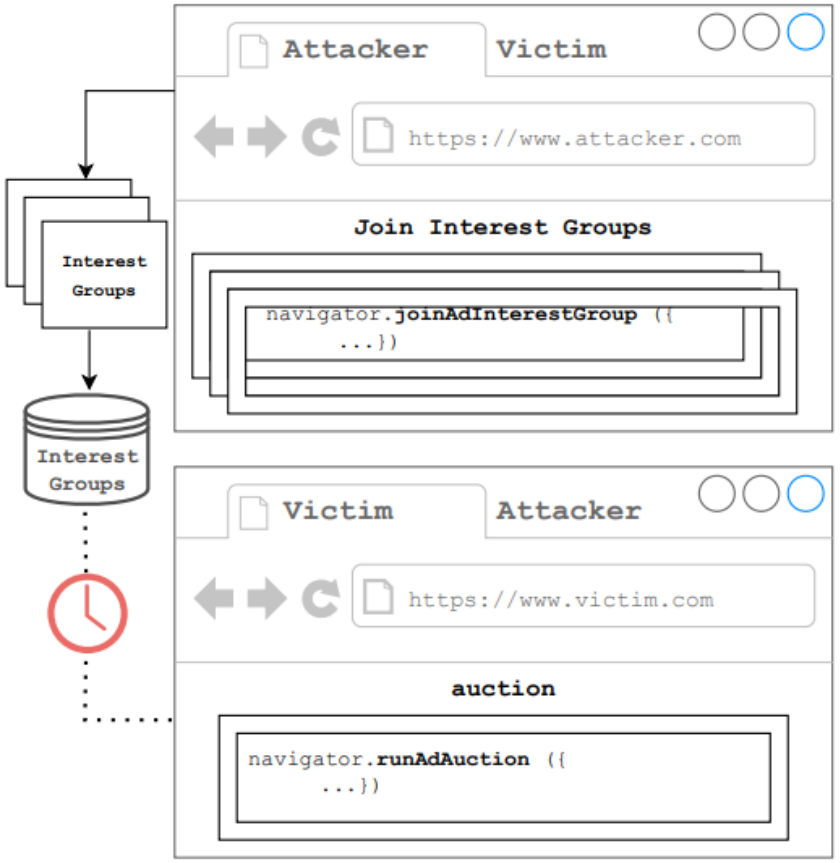
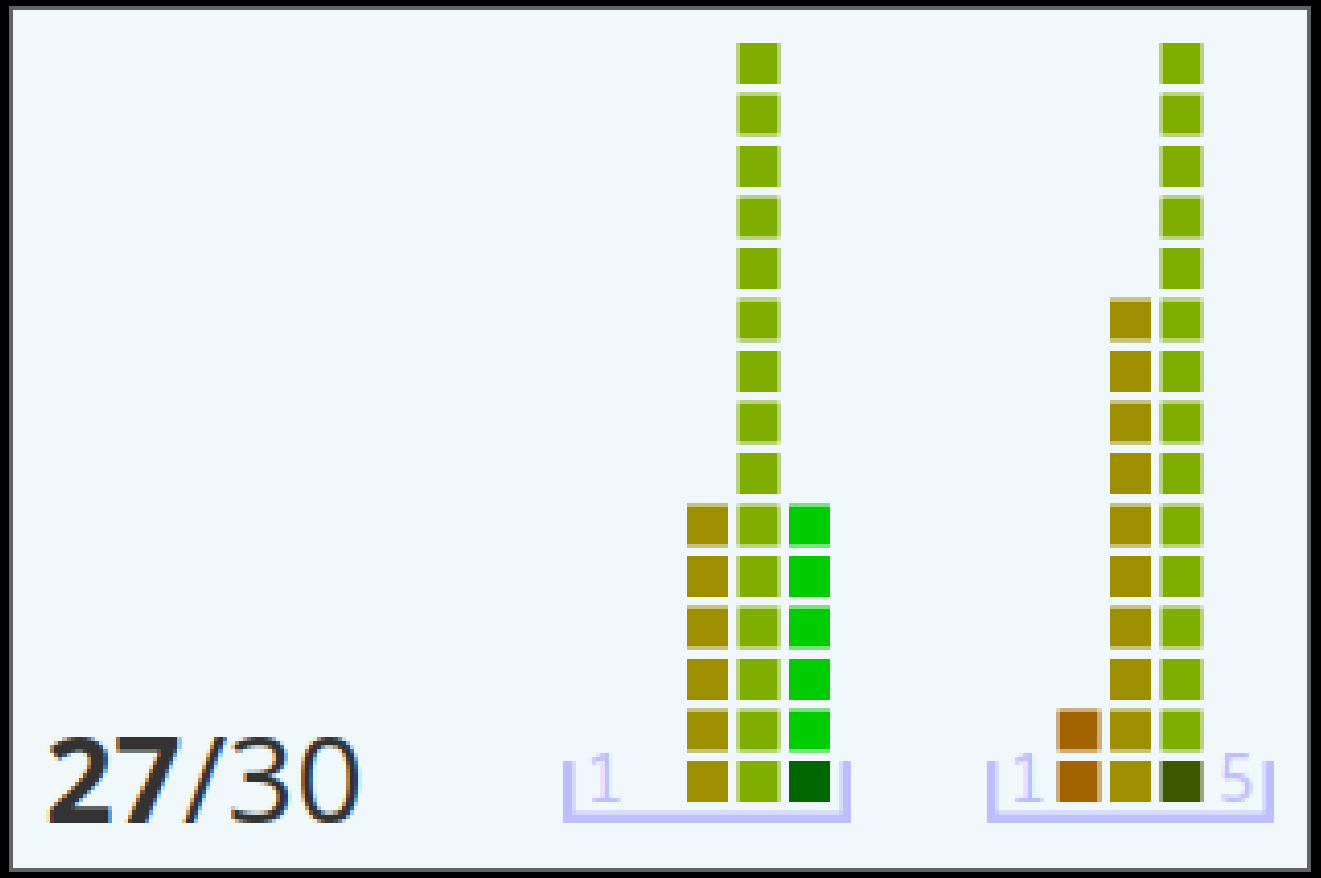


Figure 8: Blocking Ad Auctions.

Denial of Service

Discussion


27/30
1
1
5

Personal Points

OPINIONS

- Authors...
  - Performed non-comprehensive measurement
  - Found creative attacks with serious implications
  - Produced an award-quality paper
- Attack surface of FLEDGE likely still vulnerable

QUESTIONS

- What was your "favorite" attack?
- What is more privacy-invasive: 3rd party cookies or FLEDGE?
- Can 3rd party cookies and the Google Privacy Sandbox coexist?
  - *Google walked back its announcement to deprecate 3rd party cookies.*

Class Points

OPINIONS

- Attacks...
  - Should have been tested on real users (?!)
  - Have a strong/narrow threat model
  - Are too limited in scope
    - "test other APIs"
  - Are already achievable with 1st party cookies
  - Are hard to understand
  - Are clever
  - Are alarming
    - "So many attacks, why haven't we moved to other browsers?"

    => *we have* ***;)***

QUESTIONS

- Is private advertising possible?
- How does the privacy level of FLEDGE compare to traditional RTB?
- Should Google disable FLEDGE? Should users turn it off?
- How would FLEDGE do in other browsers?
- How does FLEDGE affect Google's business model? What about small advertisers?

Class Points

OPINIONS

- The Google Privacy Sandbox...
  - is good for user privacy
  - requires further investigation
- We should investigate...
  - new Sandbox proposals
  - browser side-channels
  - further measurements on FLEDGE adoption
  - economic implications

QUESTIONS

- What is the right balance of utility and privacy?
  - Ad revenue vs privacy?
  - Rapid development vs security/privacy?
- To what extent does Google care about user privacy? Can we trust them?
  - Google *still* hasn't responded to 10/12 disclosures
- How can we nerf Google's role in the ad ecosystem?

Class Points

OPINIONS

- Proposed mitigations...
  - Lack specificity
  - Are not well-enough thought out
- There should be a FLEDGE usability study

QUESTIONS

- Should the researchers have published with the flaws still present?
- How can we regulate the advertising industry?
  - Remove targeted ads (i.e., contextual ads only)?

Thank you! :)