OWASP
Open Web Application Security Project

I know what you did last summer: New persistent tracking mechanisms in the wild

Stefano Belloro & Dr Alexios Mylonas

$whoami

Currently:

- Lecturer, Cyber Security @BU

Previously:

- PhD in Cyber Security & BSc @AUEB
- MSc Information Security @RHUL
- Security Consultant

$id belloro

Currently:

- Software Engineering Manager @BBC

Previously:

- M.Sc. in software engineering and Internet architecture

Web

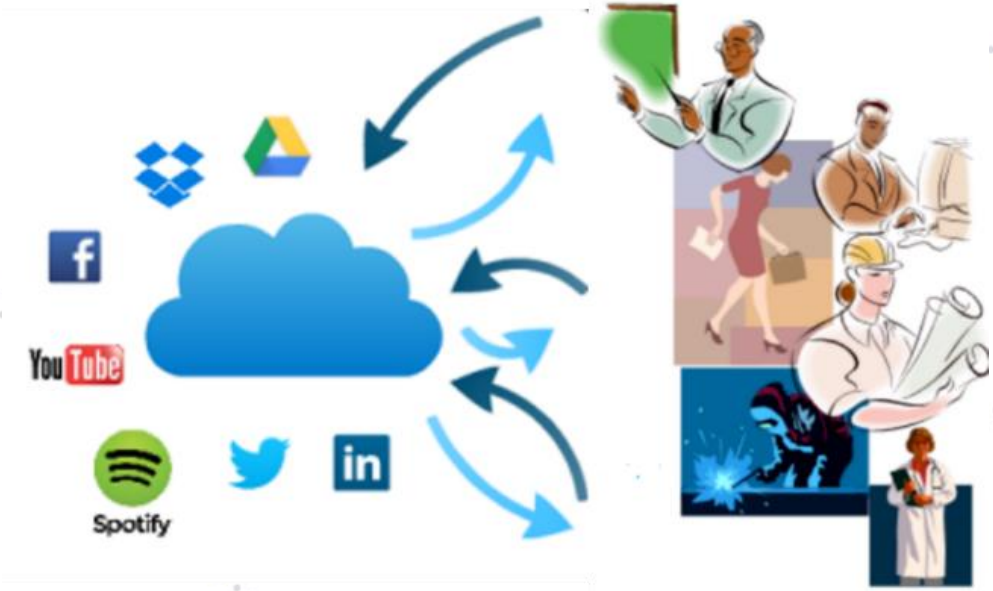
- The world wide web (www) has changed our lives

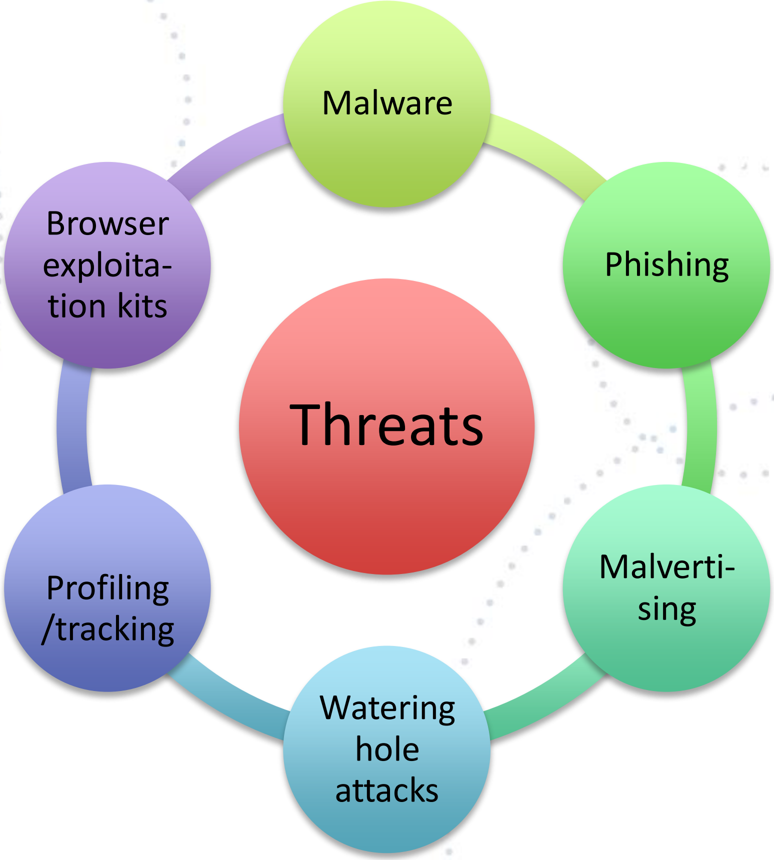
- We spend more than 34h per week accessing online content

Web

- Mobile devices are the primary means used to access the web

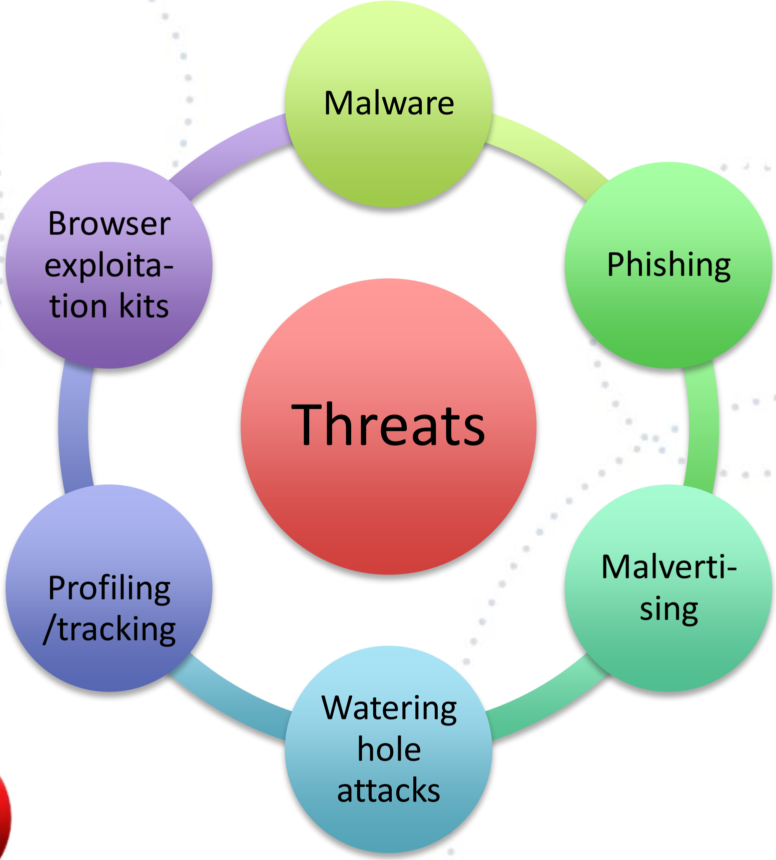
Web Threats?


You Tube
Spotify

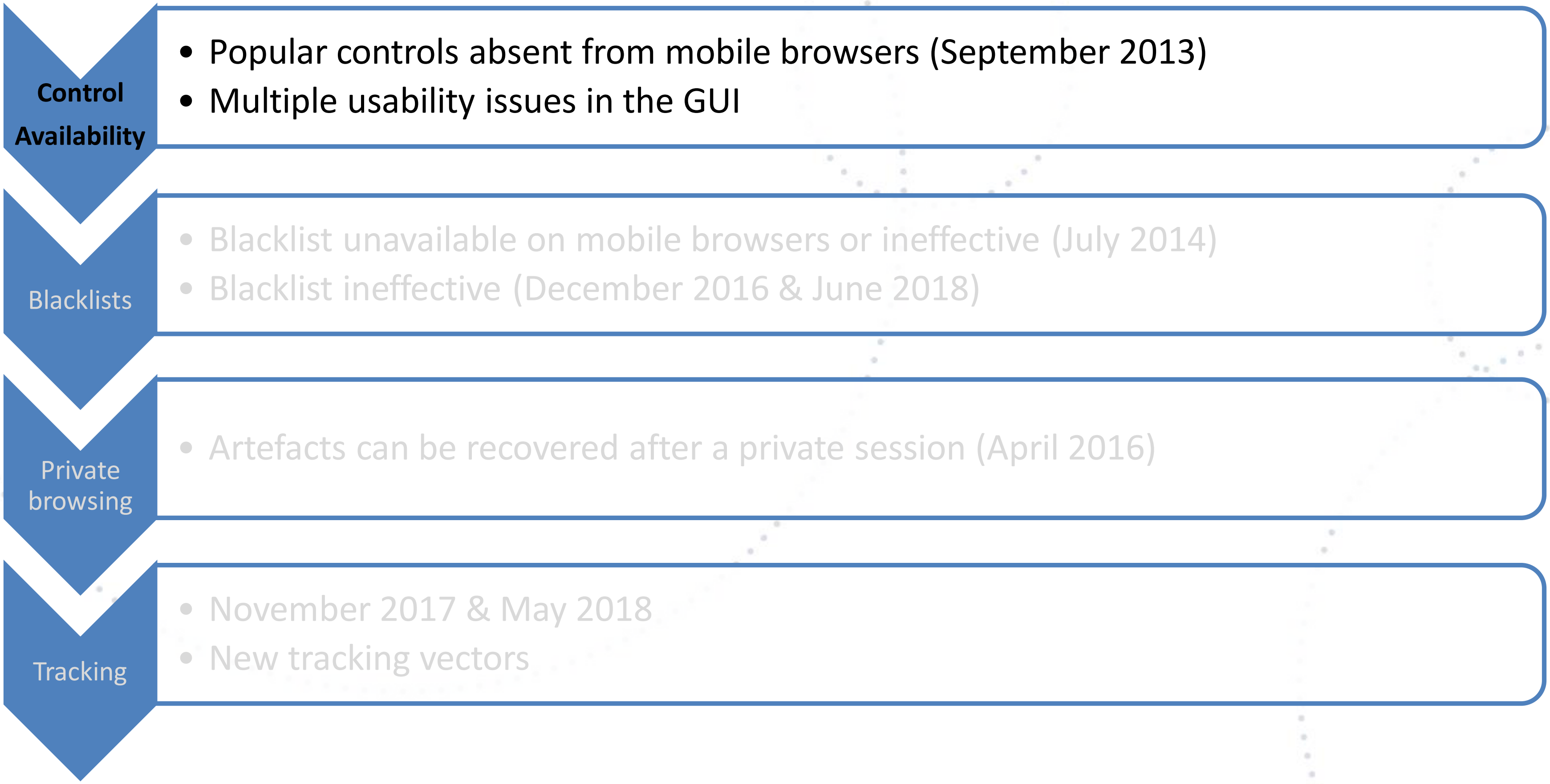

Threats
Malware
Phishing
Malverti-sing
Watering hole attacks
Profiling /tracking
Browser exploita-tion kits

Protection from web threats?

Can (mobile|desktop) browsers protect us from web threats?



Protection from web threats?



Control Availability

- Popular controls absent from mobile browsers (September 2013)
- Multiple usability issues in the GUI

Blacklists

- Blacklist unavailable on mobile browsers or ineffective (July 2014)
- Blacklist ineffective (December 2016 & June 2018)

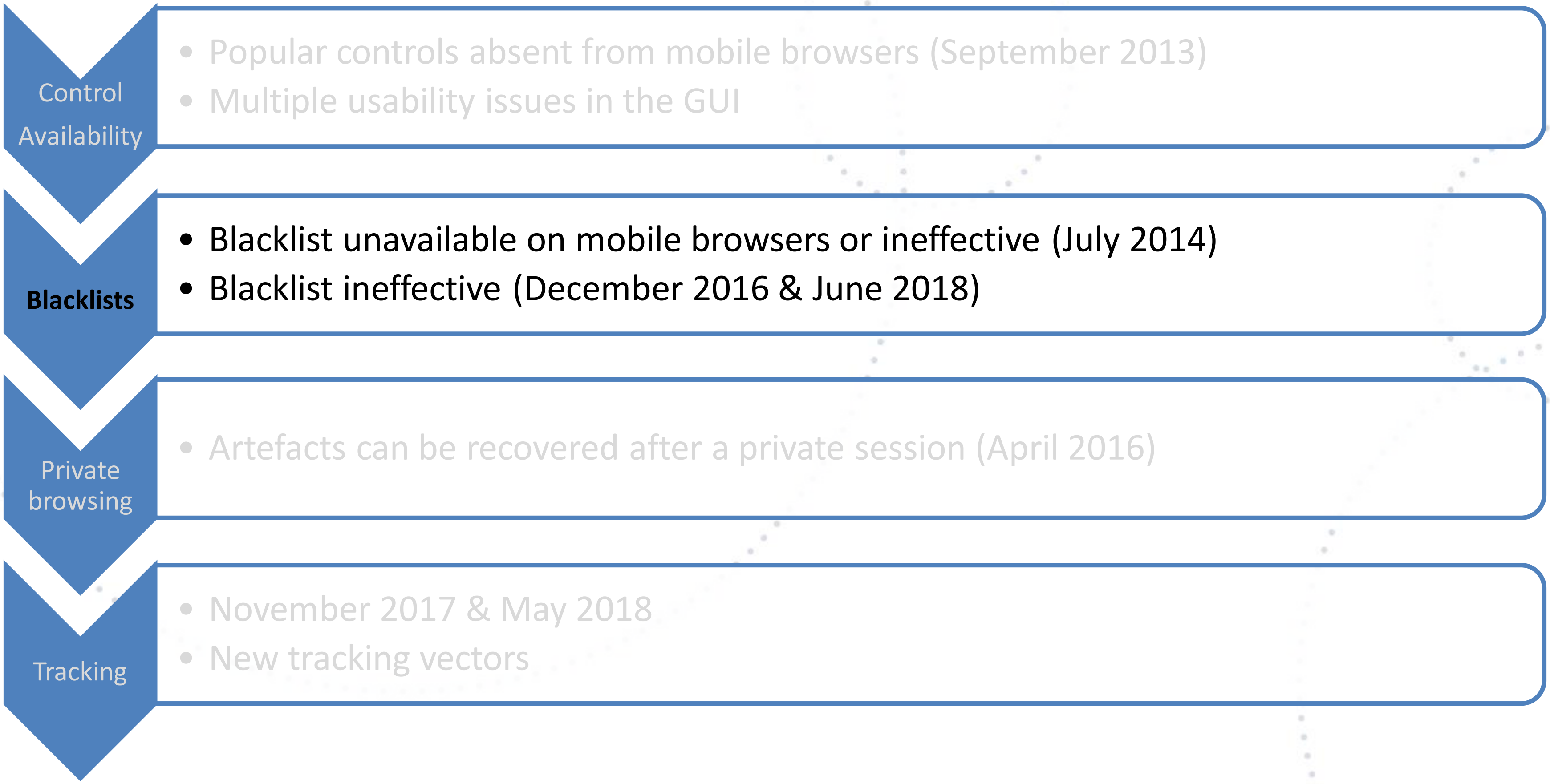
Private browsing

- Artefacts can be recovered after a private session (April 2016)

Tracking

- November 2017 & May 2018
- New tracking vectors

Protection from web threats?



Control Availability

- Popular controls absent from mobile browsers (September 2013)
- Multiple usability issues in the GUI

Blacklists

- Blacklist unavailable on mobile browsers or ineffective (July 2014)
- Blacklist ineffective (December 2016 & June 2018)

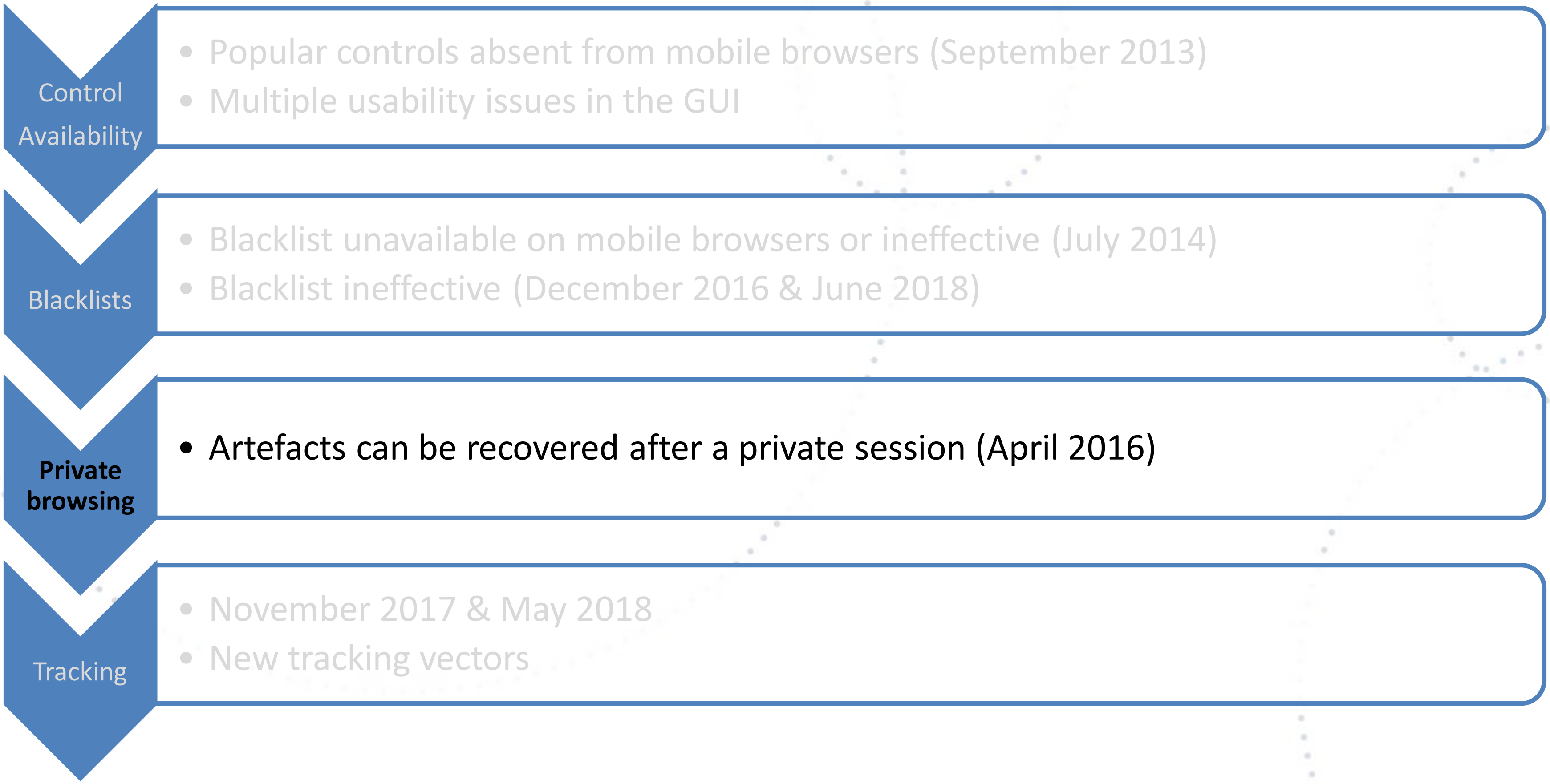
Private browsing

- Artefacts can be recovered after a private session (April 2016)

Tracking

- November 2017 & May 2018
- New tracking vectors

Protection from web threats?



Control Availability

- Popular controls absent from mobile browsers (September 2013)
- Multiple usability issues in the GUI

Blacklists

- Blacklist unavailable on mobile browsers or ineffective (July 2014)
- Blacklist ineffective (December 2016 & June 2018)

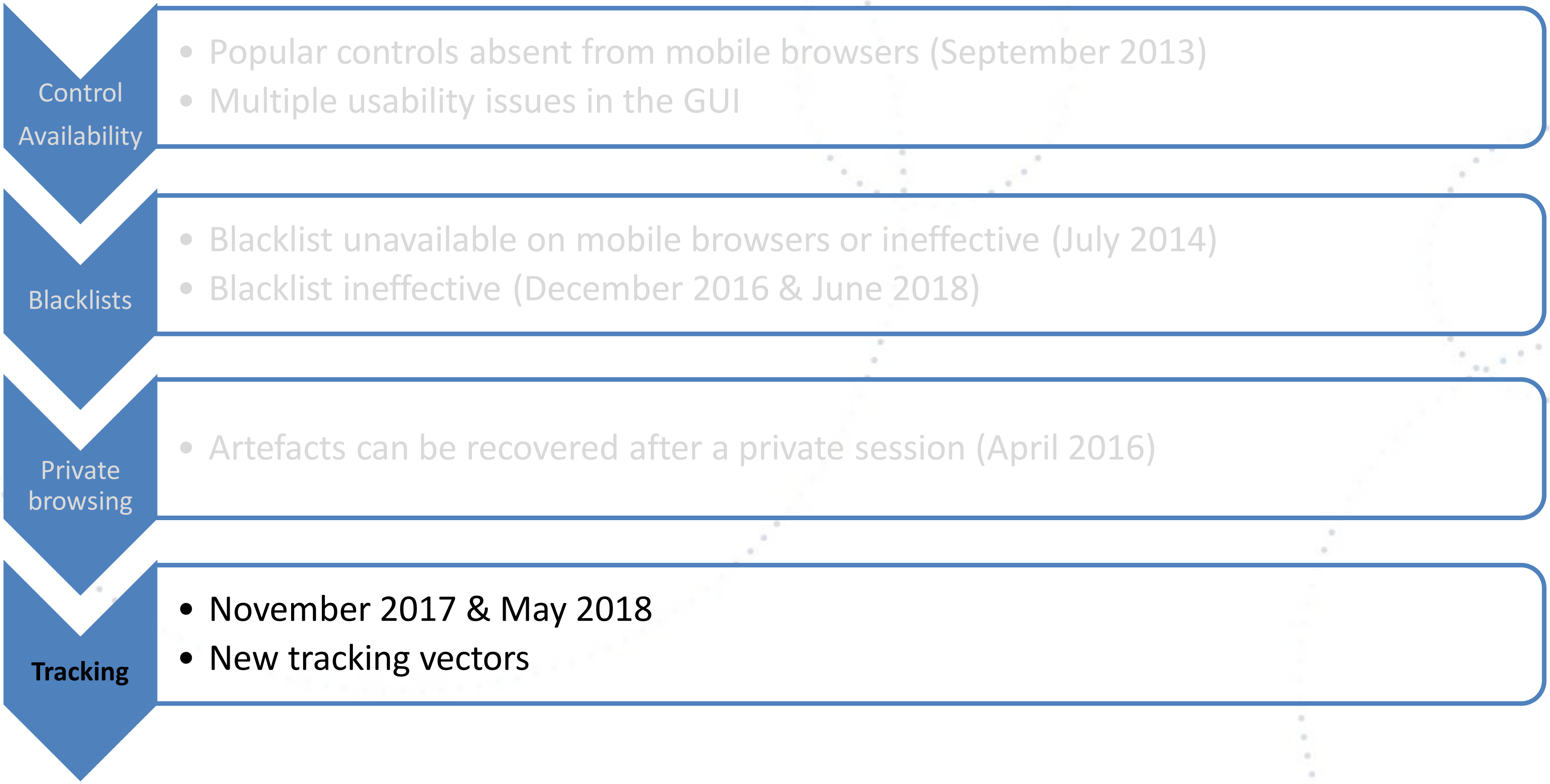
Private browsing

- Artefacts can be recovered after a private session (April 2016)

Tracking

- November 2017 & May 2018
- New tracking vectors

Protection from web threats?



Control Availability

- Popular controls absent from mobile browsers (September 2013)
- Multiple usability issues in the GUI

Blacklists

- Blacklist unavailable on mobile browsers or ineffective (July 2014)
- Blacklist ineffective (December 2016 & June 2018)

Private browsing

- Artefacts can be recovered after a private session (April 2016)

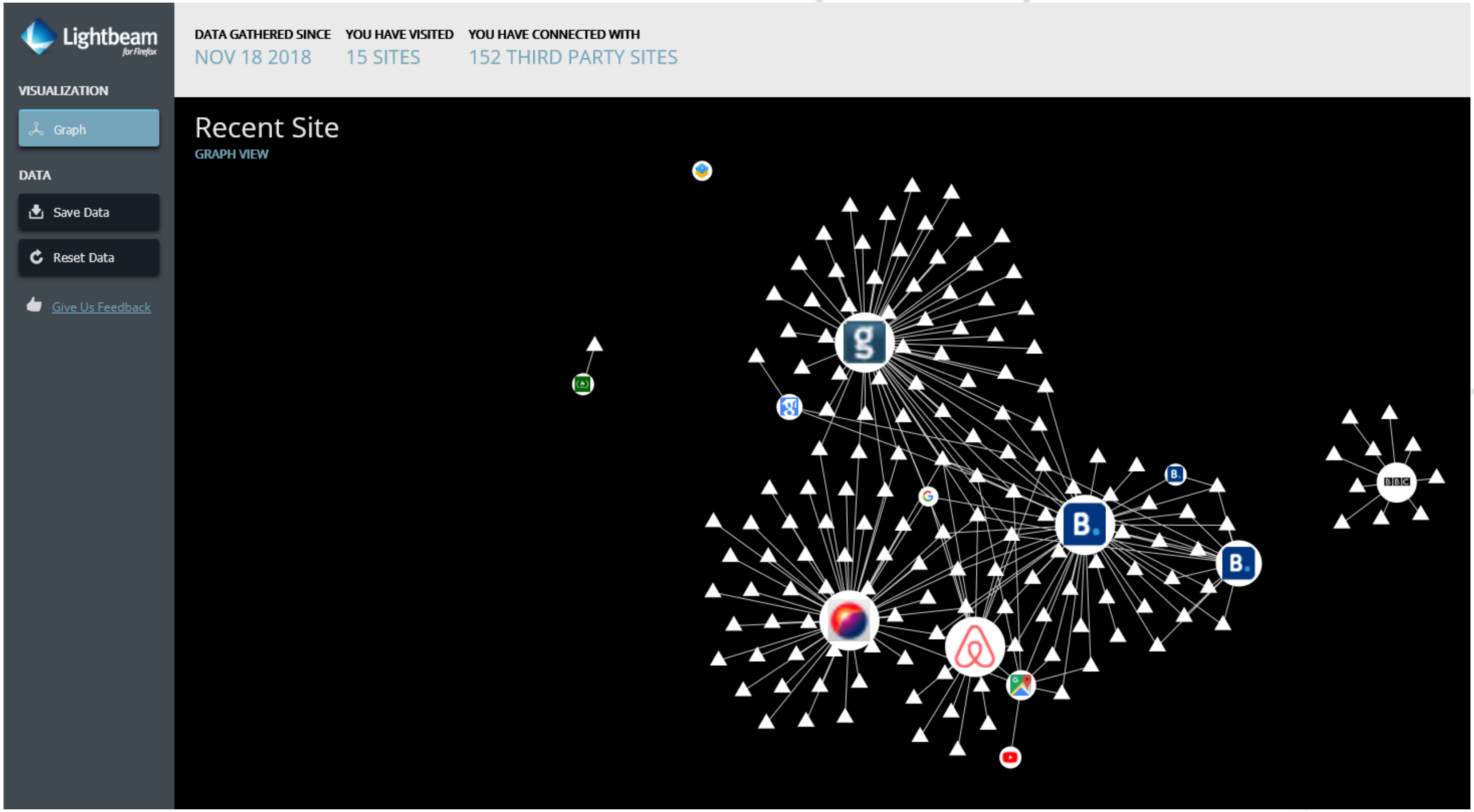
Tracking

- November 2017 & May 2018
- New tracking vectors

Tracking

- Web tracking is not new
  - – Madrigal. I'm Being Followed: How Google—and 104 Other Companies—Are Tracking Me on the Web, link
- Today?

Tracking



DATA GATHERED SINCE
NOV 18 2018

YOU HAVE VISITED
15 SITES

YOU HAVE CONNECTED WITH
152 THIRD PARTY SITES

Recent Site
GRAPH VIEW

Tracking

- Client-side tracking is not new
  - Madrigal. I'm Being Followed: How Google—and 104 Other Companies—Are Tracking Me on the Web, link
- Different tracking vectors
  - Cookies, Flash cookies, Silverlight, …
  - HTML 5.0 storage

HTML 5.0 client-side technologies

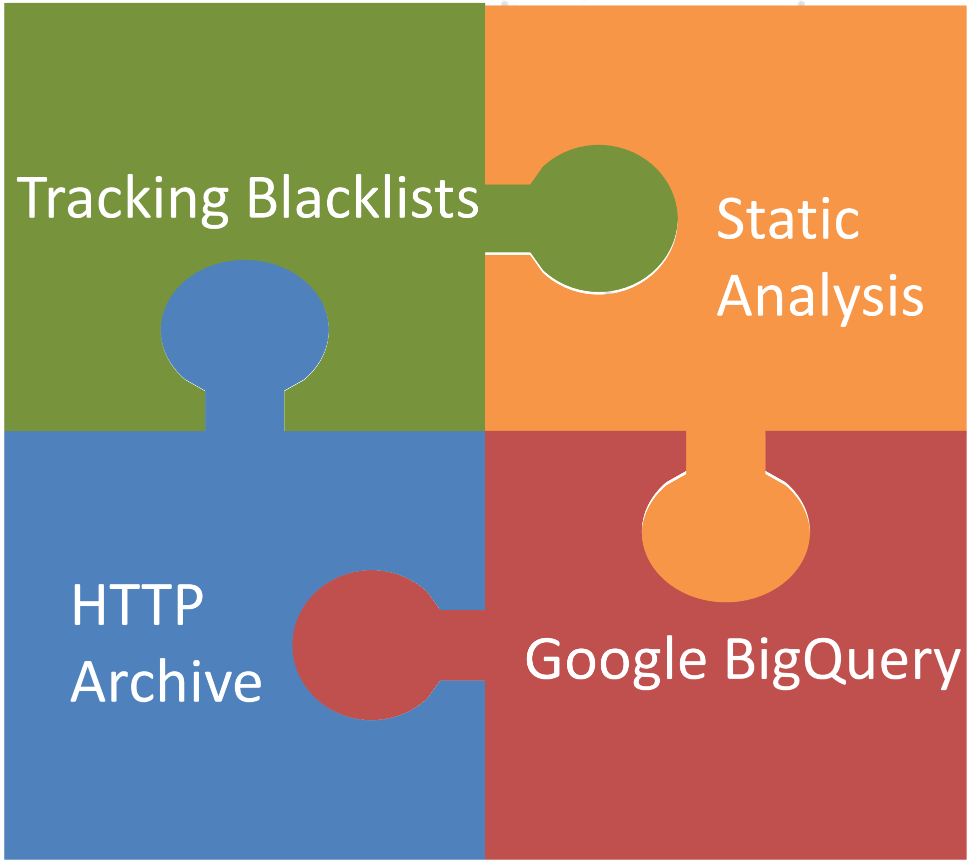
- Focus
  - Web Storage, Web SQL Database, Indexed Database API
- Have not received the same level of attention
  - Infrequent use or no use as tracking vector
  - Should be treated as cookies

Used for tracking?

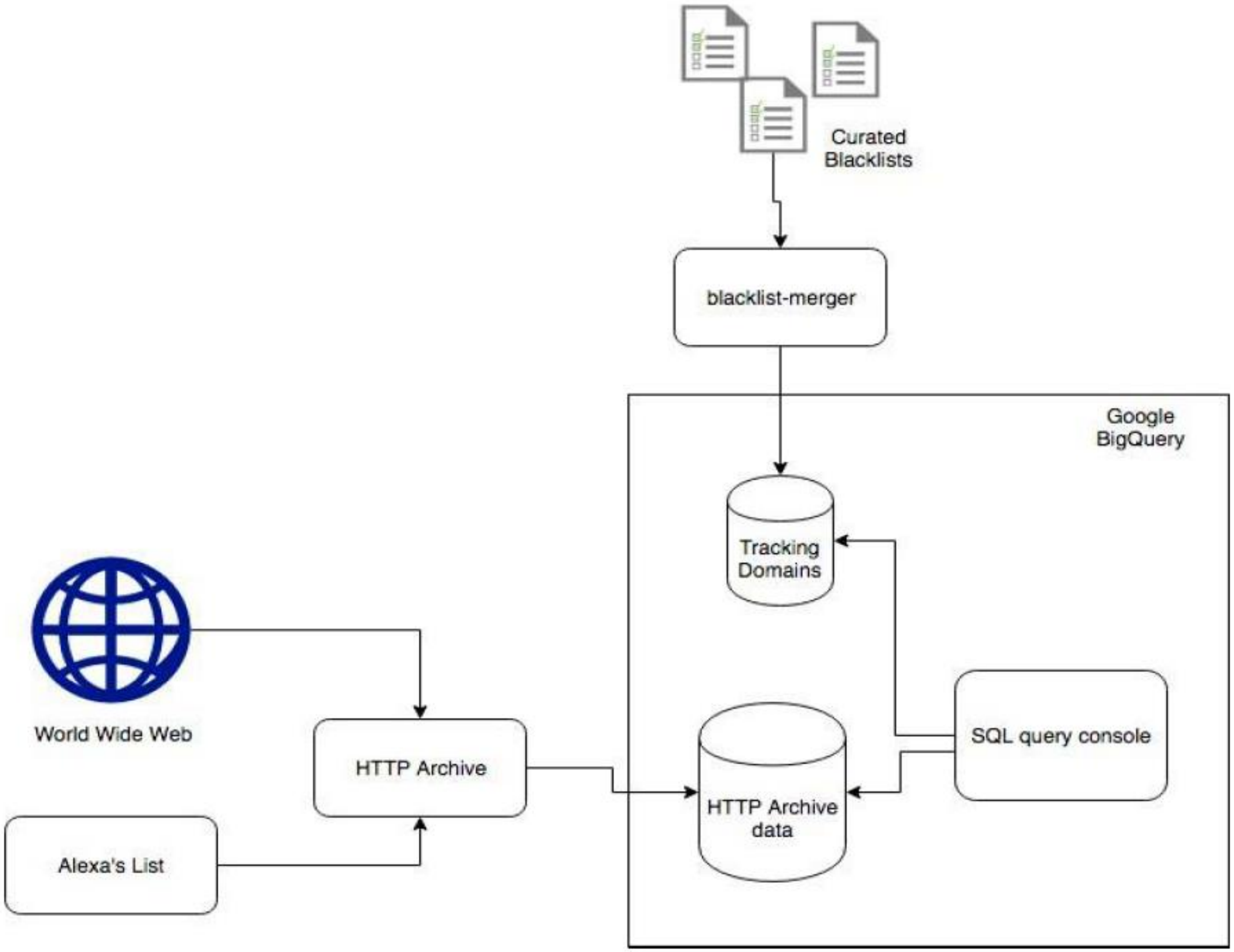
1. Frequency of their use?

2. How often used for tracking?

Methodology

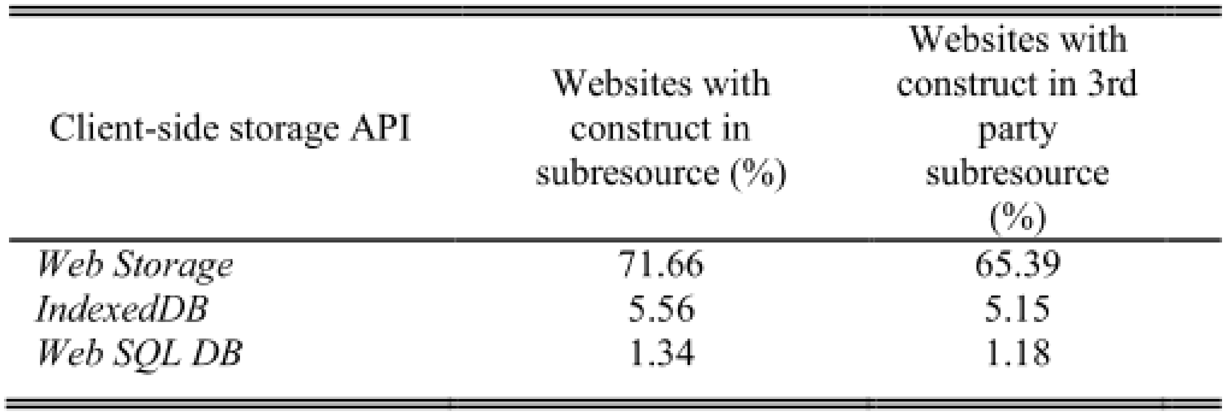


Methodology: Architecture



Frequency of use

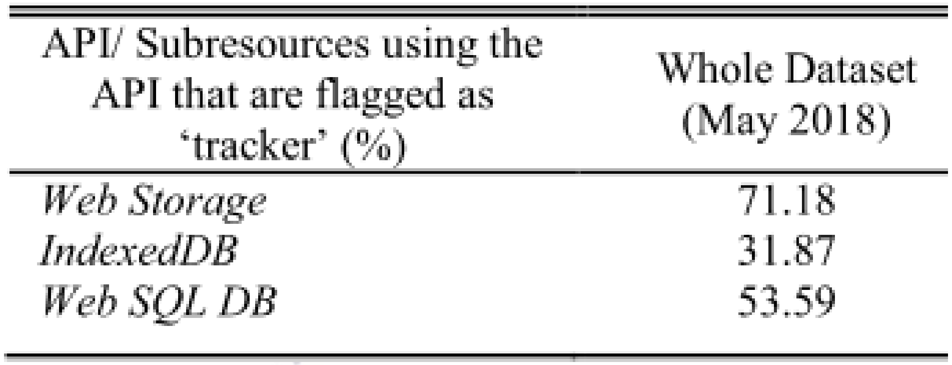
APIs often found as 3rd party subresource (*N*=460K)



Client-side storage API	Websites with construct in subresource (%)	Websites with construct in 3rd party subresource (%)
Web Storage	71.66	65.39
IndexedDB	5.56	5.15
Web SQL DB	1.34	1.18

Tracking?

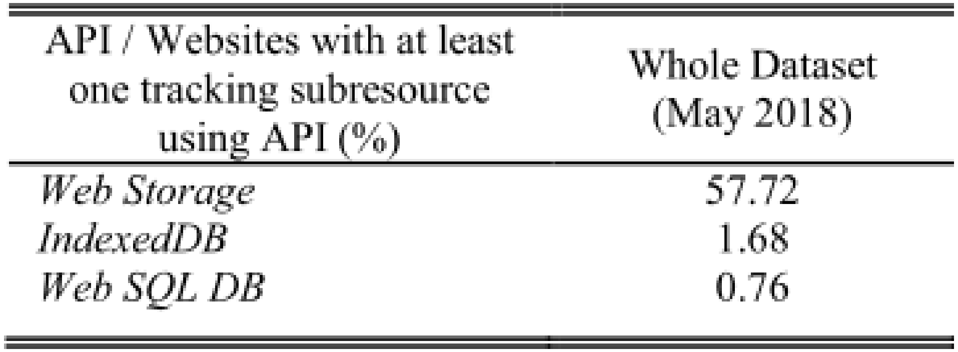
Tracking is their main use case



API/ Subresources using the API that are flagged as 'tracker' (%)	Whole Dataset (May 2018)
Web Storage	71.18
IndexedDB	31.87
Web SQL DB	53.59

Pervasiveness?

High percentage of websites containing at least one tracking subresource (*N*=460K)



API / Websites with at least one tracking subresource using API (%)	Whole Dataset (May 2018)
Web Storage	57.72
IndexedDB	1.68
Web SQL DB	0.76

Browser Protection

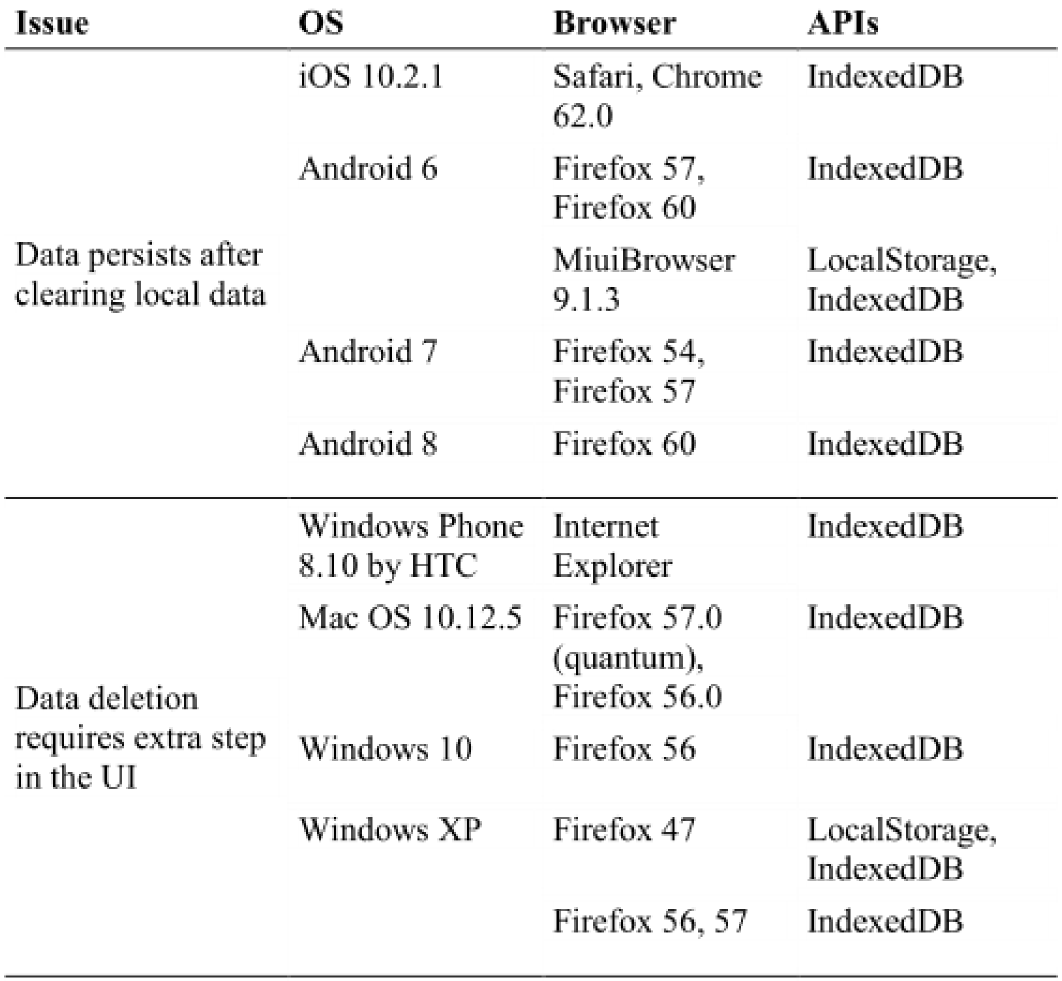
- Can I erase them like cookies?
  - Tested all popular desktop and mobile browsers
  - Windows, Mac OS
  - Android, iOS, Windows Phone

Methodology

https://github.com/stefano-belloro/storage-watcher

Clearing browsing data might not be enough

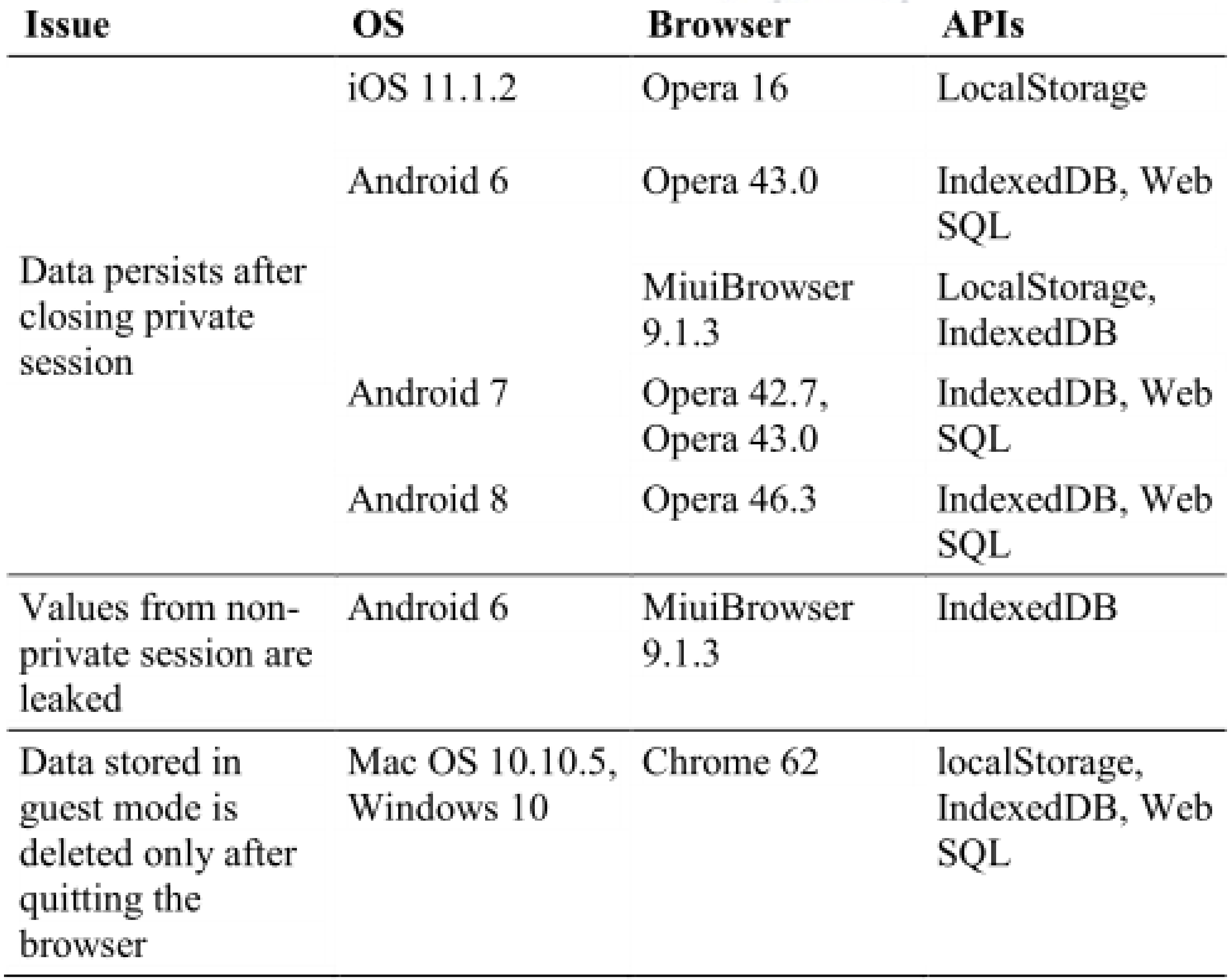
1. Data from these APIs might not be removed
2. Extra step in the GUI is required



Issue	OS	Browser	APIs
Data persists after clearing local data	iOS 10.2.1	Safari, Chrome 62.0	IndexedDB
	Android 6	Firefox 57, Firefox 60	IndexedDB
		MiuiBrowser 9.1.3	LocalStorage, IndexedDB
	Android 7	Firefox 54, Firefox 57	IndexedDB
	Android 8	Firefox 60	IndexedDB
Data deletion requires extra step in the UI	Windows Phone 8.10 by HTC	Internet Explorer	IndexedDB
	Mac OS 10.12.5	Firefox 57.0 (quantum), Firefox 56.0	IndexedDB
	Windows 10	Firefox 56	IndexedDB
	Windows XP	Firefox 47	LocalStorage, IndexedDB
		Firefox 56, 57	IndexedDB

Private session might not be enough

1. Data persists after closing private mode or guest mode
2. Data from a private session leaked to normal session



Issue	OS	Browser	APIs
Data persists after closing private session	iOS 11.1.2	Opera 16	LocalStorage
	Android 6	Opera 43.0	IndexedDB, Web SQL
		MiuiBrowser 9.1.3	LocalStorage, IndexedDB
	Android 7	Opera 42.7, Opera 43.0	IndexedDB, Web SQL
	Android 8	Opera 46.3	IndexedDB, Web SQL
Values from non-private session are leaked	Android 6	MiuiBrowser 9.1.3	IndexedDB
Data stored in guest mode is deleted only after quitting the browser	Mac OS 10.10.5, Windows 10	Chrome 62	localStorage, IndexedDB, Web SQL

Submitted bugs…

- Most of the bugs that we found have been patched ☺
  - Users might not update their OS or app ☹

- Newer versions of the browser introduce other bugs ☹
  - Noticed this in our experiments
  - Bugs appear and disappear in newer versions! ☹

Demo

Android 8

- Firefox 63.0.2
- Opera 48.2

More info

Belloro, S., & Mylonas, A. (2018). I know what you did last summer: New persistent tracking mechanisms in the wild. *IEEE Access*, *6*, 52779-52792. Link (open access)

Questions

Now!

Later:

- Alexios Mylonas, amylonas@bournemouth.ac.uk, alexios.mylonas@gmail.com
- Steafano Belloro, stefano.belloro@gmail.com