Sandboxing Trackers with Resource Blocking Lists

Steven Englehardt
@s_englehardt
Joint work with Tanvi Vyas and Eric Rescorla at Mozilla
Tracking Protection
Manchester City 2-1 Sunderland: Former Manchester United defender Paddy McNair scores late own goal to gift first Premier League victory to Pep Guardiola

- Late Paddy McNair own goal handed Manchester City a win in Pep Guardiola's first match in charge
- An equaliser from Jermain Defoe had looked like denying Guardiola in the Premier League opener
- Sub McNair, signed from Manchester United this week, headed into his own net after 87 minutes
- New City boss had made an immediate impact at City by dropping Joe Hart and Yaya Toure

By ROB DRAFTER FOR THE MAIL ON SUNDAY
PUBLISHED: 19:21 EDT, 13 August 2016 | UPDATED: 15:01 EDT, 13 August 2016

At the end, the Etihad Stadium roared with the kind of enthusiasm you might expect when greeting one of the world's finest and most iconic coaches. Poor Paddy McNair, brought on to safeguard the score, had just headed into his own goal within four minutes of his debut, and City finally had their breakthrough.

Jesus Navas crossed the ball, Vito Mannone flicked it away from the feet of Kelechi Iheanacho and McNair simply could not react quick enough to avoid nodding home from close range. The clock read 87 minutes and City fans sang with gusto, as though they finally believed a Messianic figure was about to lead them to the promised land. And so it will be recorded that the Pep Guardiola era began with a win.

And, after the years of anticipation, it was really Guardiola on the touchline, finally overseeing a Premier League match. There was the familiar expensive, well-cut suit and the distinctive bald head, bobbing up and down as he waved his arms in excitement and exasperation in equal measure. On the pitch, the look was not quite so good.
Manchester City 2-1 Sunderland: Former Manchester United defender Paddy McNair scores late own goal to gift first Premier League victory to Pep Guardiola

- Late Paddy McNair own goal handed Manchester City a win in Pep Guardiola's first match in charge
- An equaliser from Jermain Defoe had looked like denying Guardiola in the Premier League opener
- Sub McNair, signed from Manchester United this week, headed into his own net after 87 minutes
- New City boss had made an immediate impact at City by dropping Joe Hart and Yaya Toure

By ROB DRAPER FOR THE MAIL ON SUNDAY

At the end, the Etihad Stadium roared with the kind of enthusiasm you might expect when greeting one of the world's finest and most iconic coaches. Poor Paddy McNair, brought on to safeguard the score, had just headed into his own goal within four minutes of his debut, and City finally had their breakthrough.

Jesus Navas crossed the ball, Vito Mannone flicked it away from the feet of Kelechi Iheanacho and McNair simply could not react quick enough to avoid nodding home from close range. The clock read 87 minutes and City fans sang with gusto, as though they finally believed a Messianic figure was about to lead them to the promised land. And so it will be recorded that the Pep Guardiola era began with a win.

And, after the years of anticipation, it was really Guardiola on the touchline, finally overseeing a Premier League game as a manager. He was calm, collected and in full control, even if he breathed a sigh of relief to have seen off a spirited late rally from the Black Cats.
Here’s The Thing With Ad Blockers

We get it: Ads aren’t what you’re here for. But ads help us keep the lights on. So, add us to your ad blocker’s whitelist or pay $1 per week for an ad-free version of WIRED. Either way, you are supporting our journalism. We’d really appreciate it.
Can we sandbox trackers instead of block them?
Can we sandbox trackers instead of block them?

Not completely :(
Stateful Tracking  Stateless Tracking
Stateful Tracking

Stateless Tracking

ben174 / hsts-cookie

Creates a HSTS Supercookie to fingerprint a browser
Stateful Tracking

Stuff that requires cross-domain storage access

Stateless Tracking
Stateful Tracking

Stuff that requires cross-domain storage access

Stateless Tracking

Canvas

Audio

Font

Image source: http://www.lalit.org/lab/javascript-css-font-detect/

stuff that requires cross-domain storage access
Stateful Tracking

Stuff that requires cross-domain storage access

Stateless Tracking

Canvas

Stuff that requires Javascript access

Audio

Font
<table>
<thead>
<tr>
<th>Stateful</th>
<th>Stateless</th>
</tr>
</thead>
<tbody>
<tr>
<td>First-party Context</td>
<td>Third-party Context (iframes)</td>
</tr>
</tbody>
</table>
First-party Context

Stateful

SOP already provides protection

Third-party Context (iframes)

Stateless
1. Make a new third-party cookie blocking mode
1. Make a new third-party cookie blocking mode

+ No stateful tracking in 3rd party iframes
1. Make a new third-party cookie blocking mode

+ No stateful tracking in 3rd party iframes
+ No cookies with `<script src…>` embeds
1. Make a new third-party cookie blocking mode

+ No stateful tracking in 3rd party iframes
+ No cookies with `<script src…>` embeds
+ Less breakage than other cookie blocking mode
<table>
<thead>
<tr>
<th>First-party Context</th>
<th>Third-party Context (iframes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stateful</td>
<td></td>
</tr>
<tr>
<td>SOP already provides protection</td>
<td>Selective 3rd-party cookie blocking</td>
</tr>
<tr>
<td>Stateless</td>
<td></td>
</tr>
</tbody>
</table>
2. Block cookies and use iframe sandbox


2. Block cookies and use iframe sandbox

+ No fingerprinting in iframes
+ Restrict plugin use, modal dialogs, top-level navigation, etc
2. Block cookies and use iframe sandbox

+ No fingerprinting in iframes
+ Restrict plugin use, modal dialogs, top-level navigation, etc

Not enough trackers are embedded in iframes.

71% of third-party scripts on top homepages will still be able to track on 90%+ of pages

10% of third-party scripts on top homepages have a reduction in tracking by 50% or more
<table>
<thead>
<tr>
<th>Stateful</th>
<th>Stateless</th>
</tr>
</thead>
<tbody>
<tr>
<td>First-party Context</td>
<td>SOP already provides protection</td>
</tr>
<tr>
<td>Third-party Context (iframes)</td>
<td>Selective 3rd-party cookie blocking</td>
</tr>
<tr>
<td></td>
<td>Reduced JS feature set (extend iFrame sandbox)</td>
</tr>
</tbody>
</table>
3. Block active content and sandbox iframes

Built a prototype to test this...
3. Block active content and sandbox iframes

Built a prototype to test this...
breakage is still too high!
3. Block scripts and sandbox iframes

- Google, Facebook, Twitter all require or recommend first-party script access
- 2 out of 10,000 sites iframe Doubleclick
- 209 out of 10,000 sites iframe Facebook
15 New iOS 9.3.3 Jailbreak Tweaks Worth Trying On Your iPhone Or iPad
By Oliver Haslam on August 14th, 2016

Here are 15 newly released jailbreak tweaks compatible with iOS 9.3.3, the latest version of firmware to have a jailbreak to its name. If you're running iOS 9.3.3 and are jailbroken, this list is for you.

Enable Android Notifications On Windows 10 Anniversary Update, Here's How
By Paul Morris on August 14th, 2016

Here's a step-by-step guide on how to enable your Android phone to push notifications to a Windows 10 Anniversary Update or even your running PC.

Apple Is Giving Away A $2 Kids-Oriented iPhone And iPad App For Free
By Zayed Rehman on August 14th, 2016

Another week has come to an end, which means we are ready to get our hands on yet another paid iOS app gone free for limited time. As part of Apple's Free App of the Week promotion, this week's app happens to be a game intended for children which usually retails for $1.99 on the App Store.

Blocking with Tracking Protection
Sandboxing with Tracking Protection
Guten Abend!
Ihr Wetter für heute in
Berlin

bis 21°C
leicht bewölkt

Zur Tagesvorhersage

Aussichten
weiterlesen

Empfehlungen der Redaktion

Blocking with Tracking Protection
Sandboxing with Tracking Protection
Stateful

SOP already provides protection

Third-party Context (iframes)

Selective 3rd-party cookie blocking

Stateless

:(

Reduced JS feature set (extend iFrame sandbox)
4. Sandbox active content and sandbox iframes
4. Sandbox active content and sandbox iframes

Define *tracking wrappers* for interactions across the sandbox boundary.
What do Google scripts do?
What do Google scripts do?

<iframe
    onload = ...
    id = "aswift_0"
    width = "300"
    height = "250"
></iframe>
What do Google scripts do?

```javascript
var i = this.id,
    s = window.google_iframe_oncopy,
    h = s & amp; & amp;
    s.handlers, h = h & amp; & amp;
    h[i], w = this.contentwindow, d;
    d = w.document
    if (h & amp; & amp; d & amp; & amp;
        ... 
        w.location.replace(h)
    } 
} 
```
Tracking scripts require inline javascript access

- Google iframes with `onload` -- 10% of sites
- Iframes with `javascript: src urls` -- 20% of sites
- Insert inline scripts into first-party -- 18% of sites
Sandboxing Javascript is infeasible

- Breakage still too high
- Requires support for inline javascript
  - Inline function rewriting
  - Function reflection from sandbox to main page

- Sandbox design will change as scripts change
A Path Forward: Only block first-party context fingerprinting scripts, sandbox everything else.

- How to detect?
  - Blocklist building through crawling
  - Real time classifier in browser

- Crowdsourcer fingerprinting detection in scripts