

Tales from the trenches:

# Fingerprints on the Web

@igortolivei

WHOAMI



Why to track users?

- Analytics
- Target Ads
- Personalization
- Fraud detection
- Deanonymization

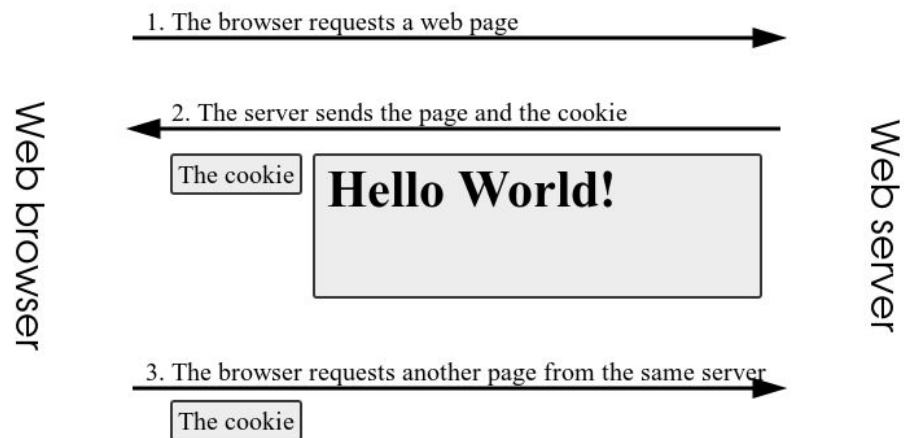
Reminiscences Of The Past

# Cookies

**Cookies** are nuggets of data that can be stored on your PC (Browser) by a Web site and then accessed every time you go back to that site.

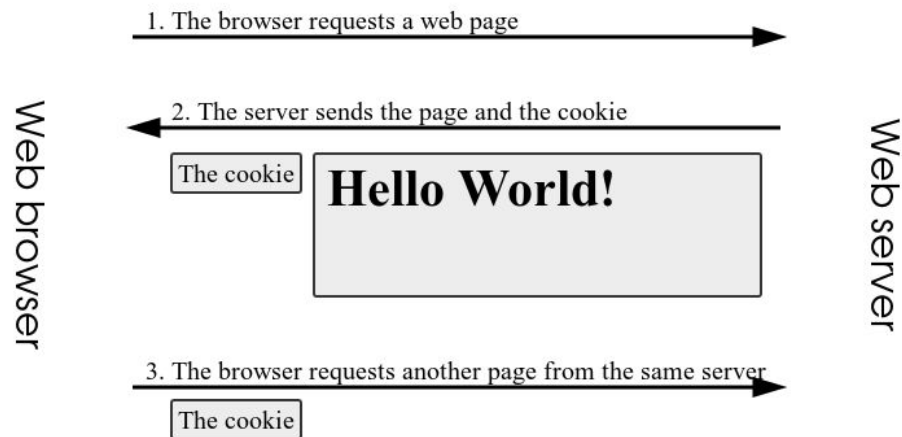
## Reminiscences Of The Past - Cookies

- Browser Requests a web page



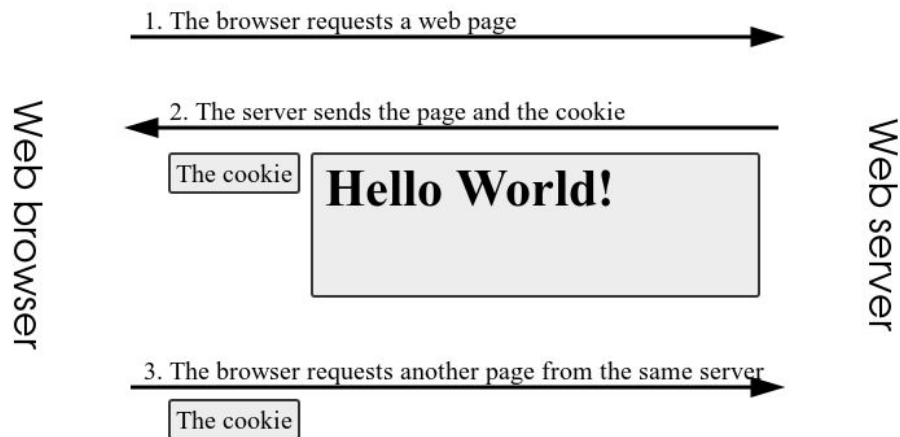
## Reminiscences Of The Past - Cookies

- Browser Requests a web page
- The server sends the page and the cookie (Set-Cookie HTTP Header)



## Reminiscences Of The Past - Cookies

- Browser Requests a web page
- The server sends the page and the cookie (Set-Cookie HTTP Header)
- The browser requests a new page from the same server





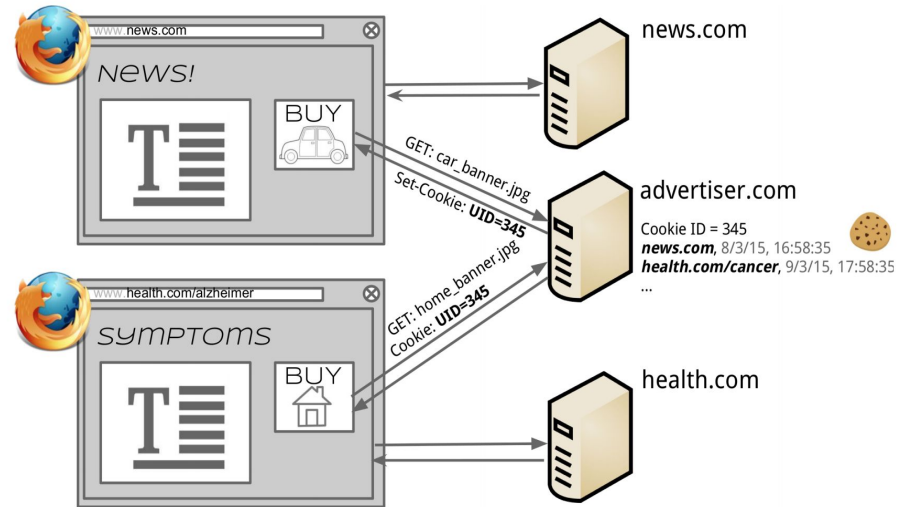
Reminiscences Of The Past

# Cookie Apocalypse

In 1996 **Third Party Cookies** where being used in the wild.

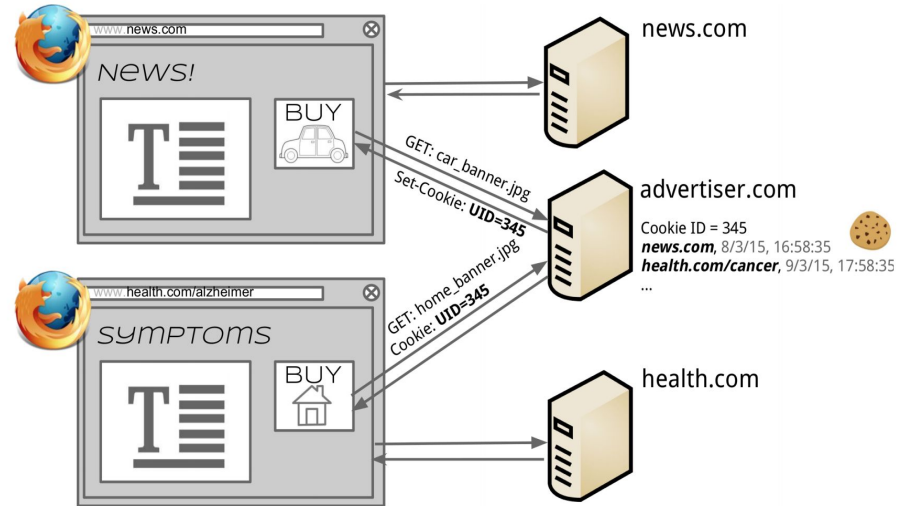
## Reminiscences Of The Past - Cookie Apocalypse

- Browser requests the Web Page



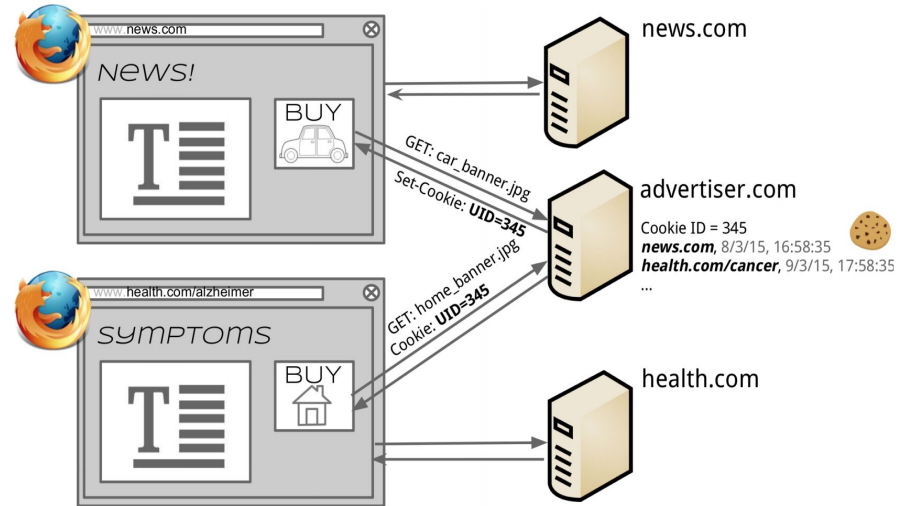
## Reminiscences Of The Past - Cookie Apocalypse

- Browser requests the Web Page
- The server sends the page and the cookie (Set-Cookie HTTP Header)



## Reminiscences Of The Past - Cookie Apocalypse

- Browser requests the Web Page
- The server sends the page and the cookie (Set-Cookie HTTP Header)
- When the user visits either of the websites, the Browser will send the cookies to the advertiser



# The Rage of the Ad Blockers

## The Rage of the Ad Blockers



# Browser Fingerprinting



- Request Behavior
- JavaScript
- CSS
- Plugins

- Request Behavior
- JavaScript
- CSS
- ~~Plugins~~

- Accept-\* Headers

Accept-Language: en-US,en;q=0.5

Accept-Encoding: deflate, gzip;q=1.0

- User Agent

Mozilla/5.0 (Windows NT 6.1; rv:52.0) Gecko/20100101 Firefox/52

# . Behavior of JS Objects - Navigator

```
< ▼ Navigator {vendorSub: "", productSub: "20030107", vendor: "Google Inc.", maxTouchPoints: 0, hardwareConcurrency: 8, ...} ⓘ
  appCodeName: "Mozilla"
  appName: "Netscape"
  appVersion: "5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.186 Safari/537.36"
  ▶ bluetooth: Bluetooth {}
  ▶ budget: BudgetService {}
  ▶ connection: NetworkInformation {downlink: 4.3, effectiveType: "4g", onchange: null, rtt: 200}
  cookieEnabled: true
  ▶ credentials: CredentialsContainer {}
    deviceMemory: 8
    doNotTrack: null
  ▼ geolocation: Geolocation
    ▶ __proto__: Geolocation
    hardwareConcurrency: 8
    language: "en-US"
  ▶ languages: (4) ["en-US", "en", "pt", "ja"]
    maxTouchPoints: 0
  ▶ mediaDevices: MediaDevices {ondevicechange: null}
  ▶ mimeType: MimeTypeArray {0: MimeType, 1: MimeType, 2: MimeType, 3: MimeType, 4: MimeType, application/pdf: MimeType, application/x-google-chrome-pdf: MimeType, application/x-nacl: MimeType, applica
    online: true
  ▶ permissions: Permissions {}
    platform: "MacIntel"
  ▶ plugins: PluginArray {0: Plugin, 1: Plugin, 2: Plugin, 3: Plugin, Chrome PDF Plugin: Plugin, Chrome PDF Viewer: Plugin, Native Client: Plugin, Widevine Content Decryption Module: Plugin, length: 4}
  ▶ presentation: Presentation {defaultRequest: null, receiver: null}
    product: "Gecko"
    productSub: "20030107"
  ▶ serviceWorker: ServiceWorkerContainer {controller: null, ready: Promise, oncontrollerchange: null, onmessage: null}
  ▶ storage: StorageManager {}
    userAgent: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.186 Safari/537.36"
    vendor: "Google Inc."
    vendorSub: ""
  ▶ webkitPersistentStorage: DeprecatedStorageQuota {}
  ▶ webkitTemporaryStorage: DeprecatedStorageQuota {}
  ▶ __proto__: Navigator
```

## . Behavior of JS Objects - Screen

```
▼ Screen {availWidth: 1440, availHeight: 873, width: 1440, height: 900, colorDepth: 24, ...} ⓘ  
  availHeight: 873  
  availLeft: 0  
  availTop: 23  
  availWidth: 1440  
  colorDepth: 24  
  height: 900  
  ▼ orientation: ScreenOrientation  
    angle: 0  
    onchange: null  
    type: "landscape-primary"  
    ► __proto__: ScreenOrientation  
  pixelDepth: 24  
  width: 1440  
  ► __proto__: Screen
```

## . Mitigation

- We make the values uniform
- Locales, Dates, vendors ...

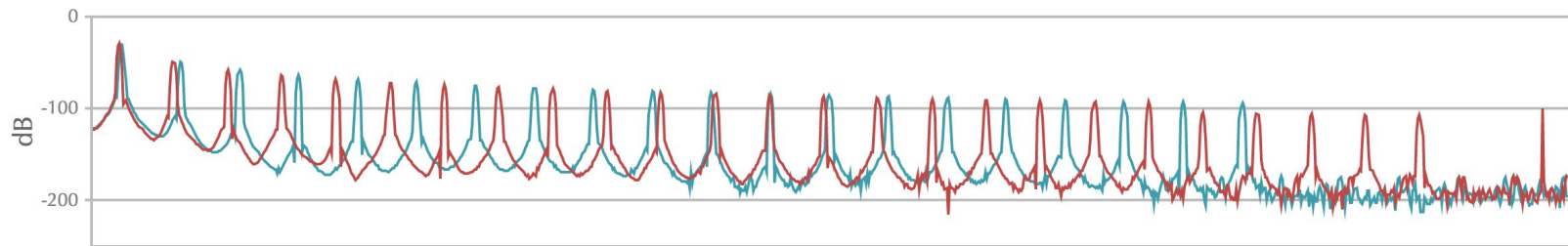
## Browser Fingerprinting - JavaScript

# . WebAudio

```
▼ AudioContext {baseLatency: 0.005804988662131519, destination: AudioDestinationNode, currentTime: 0, sampleRate: 44100, listener: AudioListener, ...} ⓘ
  baseLatency: 0.005804988662131519
  currentTime: 1.8285714285714285
  ▼ destination: AudioDestinationNode
    channelCount: 2
    channelCountMode: "explicit"
    channelInterpretation: "speakers"
    ► context: AudioContext {baseLatency: 0.005804988662131519, destination: AudioDestinationNode, currentTime: 7.668390022675737, sampleRate: 44100, listener: AudioListener, ...}
    maxChannelCount: 2
    numberOfInputs: 1
    numberOfOutputs: 0
    ► __proto__: AudioDestinationNode
  ▼ listener: AudioListener
    ► forwardX: AudioParam {value: 0, defaultValue: 0, minValue: -3.4028234663852886e+38, maxValue: 3.4028234663852886e+38}
    ► forwardY: AudioParam {value: 0, defaultValue: 0, minValue: -3.4028234663852886e+38, maxValue: 3.4028234663852886e+38}
    ► forwardZ: AudioParam {value: -1, defaultValue: -1, minValue: -3.4028234663852886e+38, maxValue: 3.4028234663852886e+38}
    ► positionX: AudioParam {value: 0, defaultValue: 0, minValue: -3.4028234663852886e+38, maxValue: 3.4028234663852886e+38}
    ► positionY: AudioParam {value: 0, defaultValue: 0, minValue: -3.4028234663852886e+38, maxValue: 3.4028234663852886e+38}
    ► positionZ: AudioParam {value: 0, defaultValue: 0, minValue: -3.4028234663852886e+38, maxValue: 3.4028234663852886e+38}
    ► upX: AudioParam {value: 0, defaultValue: 0, minValue: -3.4028234663852886e+38, maxValue: 3.4028234663852886e+38}
    ► upY: AudioParam {value: 1, defaultValue: 1, minValue: -3.4028234663852886e+38, maxValue: 3.4028234663852886e+38}
    ► upZ: AudioParam {value: 0, defaultValue: 0, minValue: -3.4028234663852886e+38, maxValue: 3.4028234663852886e+38}
    ► __proto__: AudioListener
    onstatechange: null
    sampleRate: 44100
    state: "running"
    ► __proto__: AudioContext
```

Online tracking: A 1-million-site measurement and analysis. Steven Englehardt and Arvind Narayanan. 2016.

# . WebAudio





## Browser Fingerprinting - JavaScript

```
1 let cc_output = [];  
2 let audioCtx = new window.AudioContext(),  
3   oscillator = audioCtx.createOscillator(),  
4   analyser = audioCtx.createAnalyser(),  
5   gain = audioCtx.createGain(),  
6   scriptProcessor = audioCtx.createScriptProcessor(4096, 1, 1);  
7  
8  
9 gain.gain.value = 0; // Disable volume  
10 oscillator.type = "triangle"; // Set oscillator to output triangle wave  
11 oscillator.connect(analyser); // Connect oscillator output to analyser input  
12 analyser.connect(scriptProcessor); // Connect analyser output to scriptProcessor input  
13 scriptProcessor.connect(gain); // Connect scriptProcessor output to gain input  
14 gain.connect(audioCtx.destination); // Connect gain output to audiocontext destination  
15  
16 scriptProcessor.onaudioprocess = function () {  
17   let bins = new Float32Array(analyser.frequencyBinCount);  
18   analyser.getFloatFrequencyData(bins);  
19   for (var i = 0; i < bins.length; i = i + 1) {  
20     cc_output.push(bins[i]);  
21   }  
22   //cc_output.extend(bins);  
23   analyser.disconnect();  
24   scriptProcessor.disconnect();  
25   gain.disconnect();  
26  
27   console.log(cc_output)  
28 };  
29  
30 oscillator.start(0);
```

- Mitigation

- Too many things to make uniform
- We disable it :(

- Timing Based Side Channels
  - JavaScript JIT

- Timing Based Side Channels
  - JavaScript JIT
  - CPU

- . Timing Based Side Channels
  - JavaScript JIT
  - CPU
  - **Timing of computation**

## . Timing Based Side Channels

```
performance.now()  
new Date().getTime()  
audioContext.currentTime  
canvasStream.currentTime  
video.currentTime  
audio.currentTime  
new File([], "").lastModified  
new File([], "").lastModifiedDate.getTime()  
animation.startTime  
animation.currentTime  
animation.timeline.currentTime  
document.timeline.currentTime
```

## . Timing Based Side Channels

```
1  <html><body><img id="test" style="display: none">
2  <script>
3      var test = document.getElementById('test');
4      var start = new Date();
5      test.onerror = function() {
6          var end = new Date();
7          alert("Total time: " + (end - start));
8      }
9      test.src = "http://www.example.com/page.html";
10 </script>
11 </body></html>
12
```

- Mitigation

- Remove timers granularity:  
Clamp to 100ms



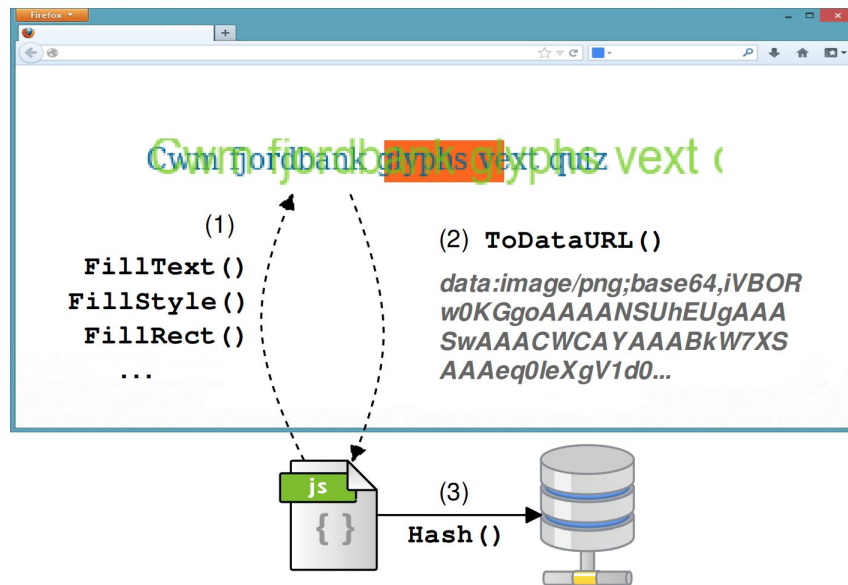
## . Mitigation

- Remove timers granularity:

Clamp to 100ms

- No silver bullet :(

## . Canvas2D



## . Mitigation



This website ([www.html5canvastutorials.com](http://www.html5canvastutorials.com)) attempted to extract HTML5 canvas image data, which may be used to uniquely identify your computer.

Should Tor Browser allow this website to extract HTML5 canvas image data?

Not Now



- Line Height

- Ascender Height + Descender Height + Font size



- Line Height (Firefox)
  - Linux: 19px
  - Mac OS X: 19.5167px
  - Windows: 19.2px or 20px

- Mitigation

- Use a default value of 1.2 (W3C)

## . Media Queries

- device-aspect-ratio
- device-height
- device-width

## . Mitigation

- We make the values uniform
- E.g. aspect ratio = 1.0



And What About Cookies?!?

# **First Party Isolation (FPI) OR Cross Origin Identifier Unlikability**

- First Party (URL based) Isolation of all browser identifier sources

- First Party (URL based) Isolation of all browser identifier sources
  - Cookies
  - Shared Workers
  - Blob
  - Storage

# THANKS!

Use Tor (Browser)  
Protect Your Privacy

@igortolivei (igt0)