Who left open the cookie jar?

A comprehensive evaluation of third-party cookie policies

Gertjan Franken, Tom Van Goethem, Wouter Joosen

August 15th 2018
Third-party policies are highly relevant today

OpenEMR security flaws could have exposed millions of patient records

Over 20 severe bugs were found using only manual methods by a single cybersecurity group.

- Online tracking study (200,000 users) [2]
  - 95% of visited pages initiated cross-site request to potential trackers
  - Of which 78% attempted to transfer potentially identifying data

Outline

› Why you should keep an eye on your cookies

› The comprehensive evaluation

› What’s wrong with your browser’s third-party cookie policies

› Conclusion
Why you should keep an eye on your cookies
Web Fundamentals

HTTP cookies [1]

› Implicit inclusion
› Authentication / identification
› Same-Origin Policy

Exploitation of implicit authentication

Cross-site attacks

› CSRF

› XSSI

› Cross-site timing attacks

victim
cute-kittens.com
doggo-bank.com

Exploitation of implicit authentication

Cross-site attacks

THIRD-PARTY COOKIE POLICIES

victim	cute-kittens.com
doggo-bank.com

Exploitation of implicit identification

Tracking

› Advertising
› Social media
› Web analytics

victim
cat-news.com
paw-book.com

Exploitation of implicit identification

Tracking

THIRD-PARTY COOKIE POLICIES

victim  cat-news.com  paw-book.com

Existing third-party cookie policies

› Built-in browser options
  › Block third-party cookies
  › Firefox Tracking Protection
  › Opera Ad Blocker
  › Safari Intelligent Tracking Prevention

› Extensions
  › Ad blocking
  › Privacy protection

› Same-site cookies
Same-site cookie [1]

- Cookie with extra attribute ‘SameSite’
  - `SameSite=strict` → NO CROSS-SITE REQUESTS!
  - `SameSite=lax` → exceptions: top-level GET, prerender

Use of same-site cookies against cross-site attacks

Set-Cookie: auth=ekSdq090pQDs; SameSite=strict
Why evaluate third-party cookie policies?

› Browsers are known to exhibit inconsistent behavior
  › Interference from different standards
  › Unintended side-effects by code modification

› Extensions have been actively bypassed in the past [1]

Comprehensive evaluation of effectiveness

The comprehensive evaluation
Black box approach

- No code review!
  - Browsers consist of millions of lines of code
    - Source code not always available
  - Many interesting extensions

Browser instance
- Browser
- Extension
- Configuration

Framework

Bypass detection data
Framework

Design

Framework

Browser Control

Framework Manager

Browsers
Extensions
Settings

WebDriver

Browser Protocol

Command Line Interface

Register

Results

Test Generator

Test websites

Browser instance

Extension
Settings

Proxy

Web Server

HTTPS / WSS

HTTPS / WSS
Framework

Design

Framework

Browser Control

Framework Manager
  Browsers
  Extensions
  Settings

WebDriver
  Command Line Interface

Browser instance
  Extension
  Settings

Proxy

Test Generator

Test websites

Results

Web Server

WebDriver Protocol
Browser Protocol
HTTPS / WSS
Framework Design

Framework

Browser Control

Framework Manager

Browsers
Extensions
Settings

Test Generator

WebDriver

Browser Protocol

Command Line Interface

Register

Results

Test websites

Browser instance

Extension
Settings

Proxy

Web Server

HTTPS / WSS

HTTPS / WSS
Inside the framework

» Browser control
  » Selenium / Command line interface

» Web server
  » Initiate cross-site requests to blacklisted domain
  » Proxy intercepts all requests
Initiating cross-site requests

› AppCache API
   » Caching cross-site pages

› HTML-tags
   » <script>, <img>, <link>, etc.

› Headers
   » Link, CSP headers

› Redirects

› JavaScript
   » Fetch, EventSource API, etc.

› PDF JS
   » sendForm()

› ServiceWorker API
What’s wrong with your browser’s third-party cookie policies
Overview

› Browsers

› Chrome
› Opera
› Firefox
› Safari
› Edge
› Tor Browser
› Cliqz

› Extensions

› Ad blocking (31)
› Tracking protection (15)
<table>
<thead>
<tr>
<th></th>
<th>AppCache</th>
<th>HTML</th>
<th>Headers</th>
<th>Redirects</th>
<th>PDF JS</th>
<th>JavaScript</th>
<th>SW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome 63</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Opera 51</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>- Block third-party cookies*</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>- Ad Blocker</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Firefox 57</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>- Tracking Protection</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
</tr>
<tr>
<td>Safari 11</td>
<td>○†</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>- No Intelligent Tracking Prevention</td>
<td>●†</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>N/A</td>
</tr>
<tr>
<td>- Block third-party cookies‡</td>
<td>●†</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>N/A</td>
</tr>
<tr>
<td>Edge 40</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>N/A</td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>N/A</td>
</tr>
<tr>
<td>Cliqz 1.17*</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Tor Browser 7</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- ●: request with cookies
- ○: request without cookies
- ○: no request

* Secure cookies were omitted in all requests.
† Safari does not permit cross-domain caching over https (only over http).
‡ Safari 10.1.2
<table>
<thead>
<tr>
<th>Browser</th>
<th>AppCache</th>
<th>HTML</th>
<th>Headers</th>
<th>Redirects</th>
<th>PDF JS</th>
<th>JavaScript</th>
<th>SW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome 63</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Opera 51</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Firefox 57</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Safari 11</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Edge 40</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Cliqz 1.17*</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>○</td>
</tr>
<tr>
<td>Tor Browser 7</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>N/A</td>
</tr>
<tr>
<td></td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
</tbody>
</table>

●: request with cookies  ○: request without cookies  ○: no request

* Secure cookies were omitted in all requests.
† Safari does not permit cross-domain caching over https (only over http).  26
‡ Safari 10.1.2
<table>
<thead>
<tr>
<th>Browser</th>
<th>AppCache</th>
<th>HTML</th>
<th>Headers</th>
<th>Redirects</th>
<th>PDF JS</th>
<th>JavaScript</th>
<th>SW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome 63</td>
<td>⬤</td>
<td>⬤</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>⬤</td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>⬤</td>
</tr>
<tr>
<td>Opera 51</td>
<td>❌</td>
<td>⬤</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>- Block third-party cookies*</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>- Ad Blocker</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Firefox 57</td>
<td>❌</td>
<td>⬤</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>- Tracking Protection</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>Safari 10</td>
<td>⬤</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>N/A</td>
</tr>
<tr>
<td>- No Intelligent Tracking Prevention</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
</tr>
<tr>
<td>- Block third-party cookies‡</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>N/A</td>
</tr>
<tr>
<td>Edge 40</td>
<td>❌</td>
<td>⬤</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>N/A</td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>N/A</td>
</tr>
<tr>
<td>Cliqz 1.17*</td>
<td>❌</td>
<td>⬤</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>⬤</td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>⬤</td>
</tr>
<tr>
<td>Tor Browser 7</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>❌</td>
<td>N/A</td>
</tr>
</tbody>
</table>

- ○: request with cookies
- ○: request without cookies
- ○: no request

* Secure cookies were omitted in all requests.
‡ Safari does not permit cross-domain caching over https (only over http).
§ Safari 10.1.2
<table>
<thead>
<tr>
<th>Browser</th>
<th>AppCache</th>
<th>HTML</th>
<th>Headers</th>
<th>Redirects</th>
<th>PDF JS</th>
<th>JavaScript</th>
<th>SW</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome 63</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Opera 51</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Block third-party cookies*</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>- Ad Blocker</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>Firefox 57</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>- Tracking Protection</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>Safari 11</td>
<td>○†</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>N/A</td>
</tr>
<tr>
<td>- No Intelligent Tracking Prevention</td>
<td>●'</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>○</td>
<td>●</td>
<td>N/A</td>
</tr>
<tr>
<td>- Block third-party cookies†</td>
<td>●'</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>N/A</td>
</tr>
<tr>
<td>Edge 40</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Cliqz 1.17*</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>●</td>
</tr>
<tr>
<td>- Block third-party cookies</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
</tr>
<tr>
<td>Tor Browser 7</td>
<td>○</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>N/A</td>
</tr>
</tbody>
</table>

●: request with cookies  ●: request without cookies  ○: no request

* Secure cookies were omitted in all requests.
† Safari does not permit cross-domain caching over https (only over http).
‡ Safari 10.1.2
Extensions

› No extension managed to block all third-party cookies to blacklisted domains

› Insufficient API
  » PDF JS for Chromium, but also Firefox favicon (HTML tags)

› Unclear API
  » No clear distinction for browser background requests

› Common mistakes
  » Insufficient permissions to intercept certain requests
PDFium design flaw
Chrome and Opera

GET / POST request

DomainB
PDFium design flaw

Chrome and Opera
PDFium design flaw
Chrome and Opera

Plugin / Extension

GET / POST request

Extension API

DomainB
PDFium design flaw
Chrome and Opera

Plugin / Extension

GET / POST request
Extension API

DomainB
PDFium design flaw
Chrome and Opera

Plugin / Extension

GET / POST request
Extension API

Block third-party cookie option

DomainB
Same-site cookie policy

- Chrome and Opera: prerender functionality
  - Both lax and strict included in cross-site request

- Edge
  - Lax bypasses: WebSocket API, `<embed>`, `<object>`
  - Strict bypasses: WebSocket API, redirects
Exploitation of a bypass

Same-site cookies

```
<link rel="prerender" href="https://doggo-bank.com/transfer.php?amount=999999&recipient=catboss" />
```
Evaluation of the framework
Completeness and novelty

› Distributed crawler setup
  » Interception of headless Chrome network traffic (using linux network namespaces)
  » Analysis of intercepted HTTP requests

› Alexa Top 10,000
  » Up to 20 pages on each website
  » 160,059 pages visited
Conclusion
Conclusion

What did we find?

› Built-in browser policies can be bypassed
  › Same-site cookie, third-party cookie policies
  › Advanced options (e.g. Opera AdBlocker, Firefox Tracking Protection)

› All adblocking and privacy extensions can be bypassed
  › Due to extension API provided by browsers
  › Due to common mistakes by extension developers
Future work

What about other policies?

› Expansion of framework

  › Policy-wise → private browsing mode, security (e.g. CSP)
  › Platform-wise → mobile browsers

› Goal: tool for comprehensive, automated analysis of security and privacy policy implementations
Illustration of importance
The prerender bug (same-site policy bypass)

› Originally reported for Chrome 57
› Present in: 58 59 60 61
› Fixed in: 62 63 64 65
› Reintroduced in: 66 67 68

› Shows importance of a comprehensive evaluation of implemented policies
Thank you!

More info and details:

www.WhoLeftOpenTheCookieJar.com