Who Left Open the Cookie Jar?
A Comprehensive Evaluation of Third-Party Cookie Policies

Tom Van Goethem, Gertjan Franken, Wouter Joosen

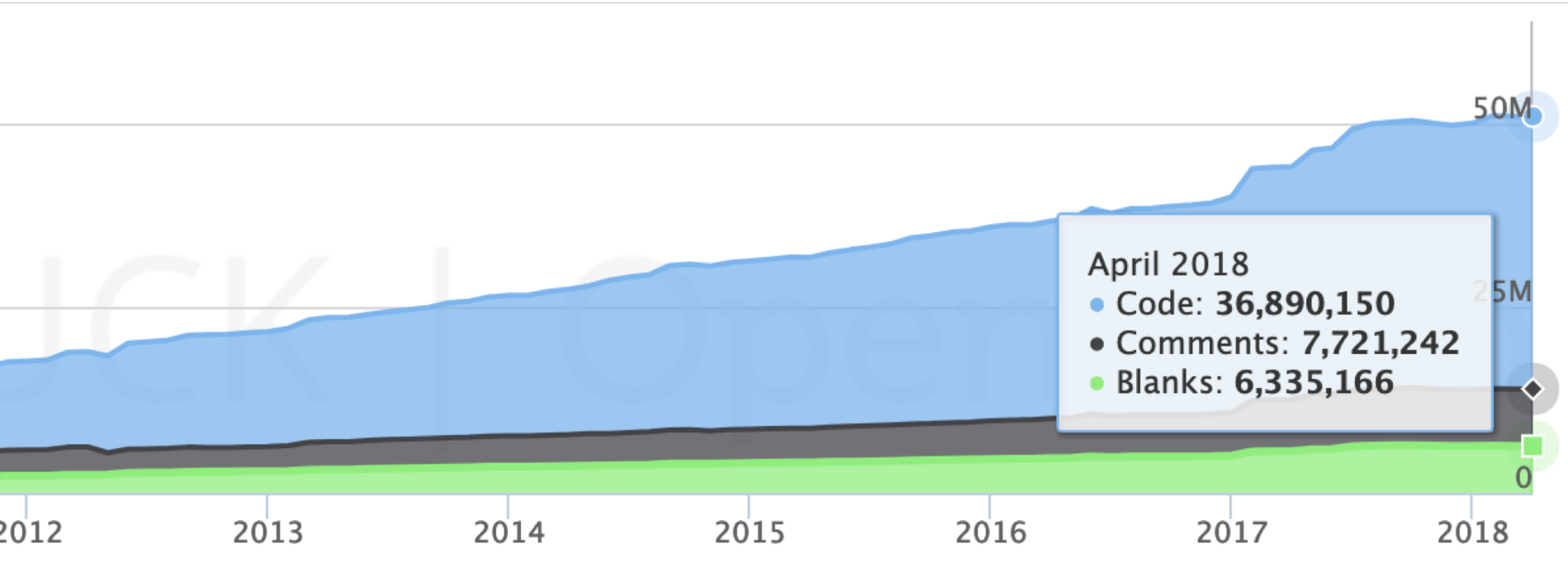
28 March 2019

KU LEUVEN DistriNet

When the web was designed, security was a high priority.

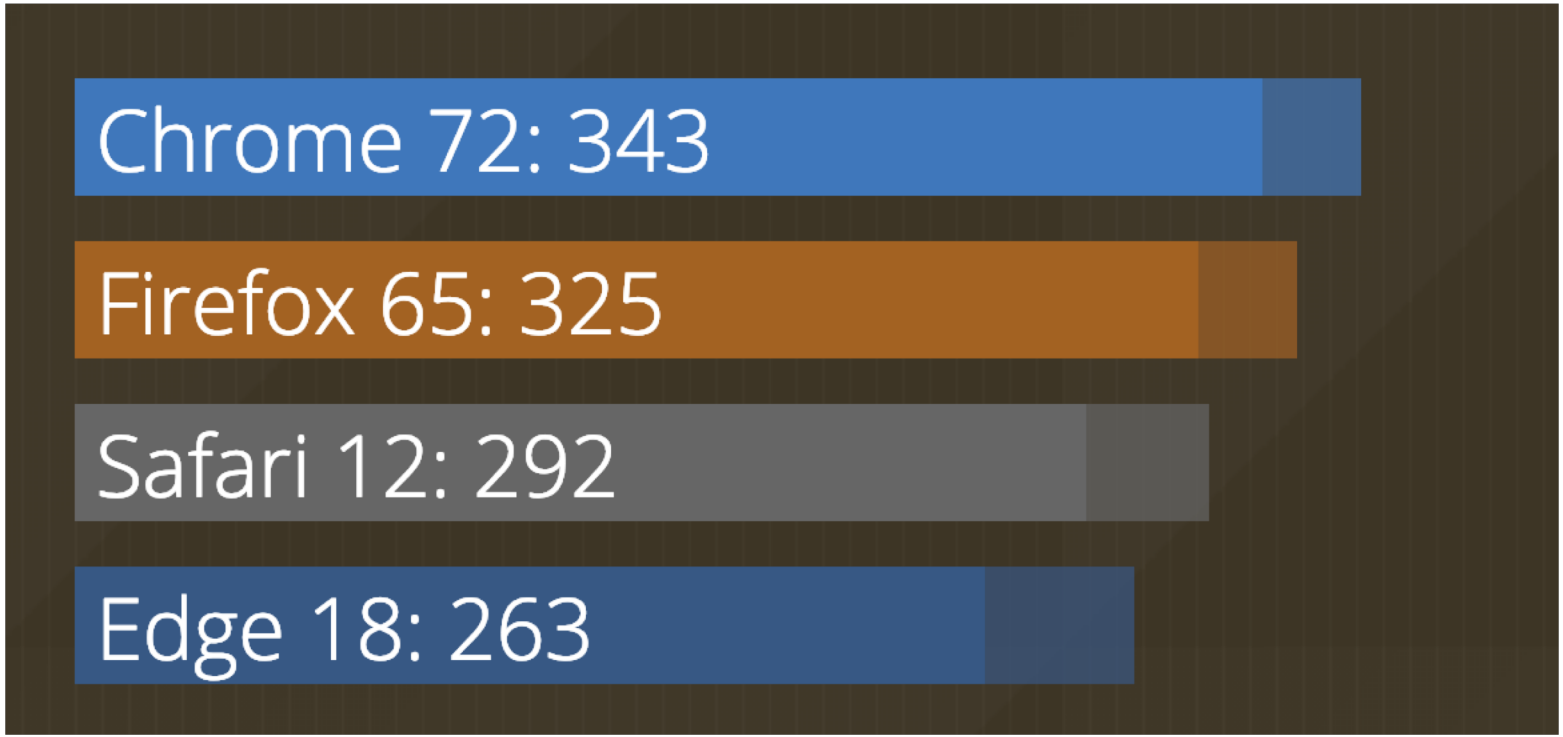
Do you trust your browser?

Lines of code for Firefox



Source: https://www.openhub.net/p/firefox/analyses/latest/languages_summary

How many different features do modern browsers support?



Source: https://caniuse.com

CSS

- ::first-letter CSS pseudo-element selector
- ::placeholder CSS pseudo-element
- ::selection CSS pseudo-element
- :dir() CSS pseudo-class
- :has() CSS relational pseudo-class
- :in-range and :out-of-range CSS pseudo-classes
- :matches() CSS pseudo-class
- :placeholder-shown CSS pseudo-class
- @font-face Web fonts
- Blending of HTML/SVG elements
- calc() as CSS unit value
- Case-insensitive CSS attribute selectors
- ch (character) unit
- 2.1 selectors
- ::marker pseudo-element
- :read-only and :read-write selectors

HTML5

- accept attribute for file input
- Attributes for form submission
- Audio element
- Audio Tracks
- Autofocus attribute
- Canvas (basic support)
- Canvas blend modes
- classList (DOMTokenList)
- Color input type
- contenteditable attribute (basic support)
- Custom Elements (V1)
- Custom protocol handling
- Datalist element
- dataset & data-* attributes
- Date and time input types
- Details & Summary elements

SVG

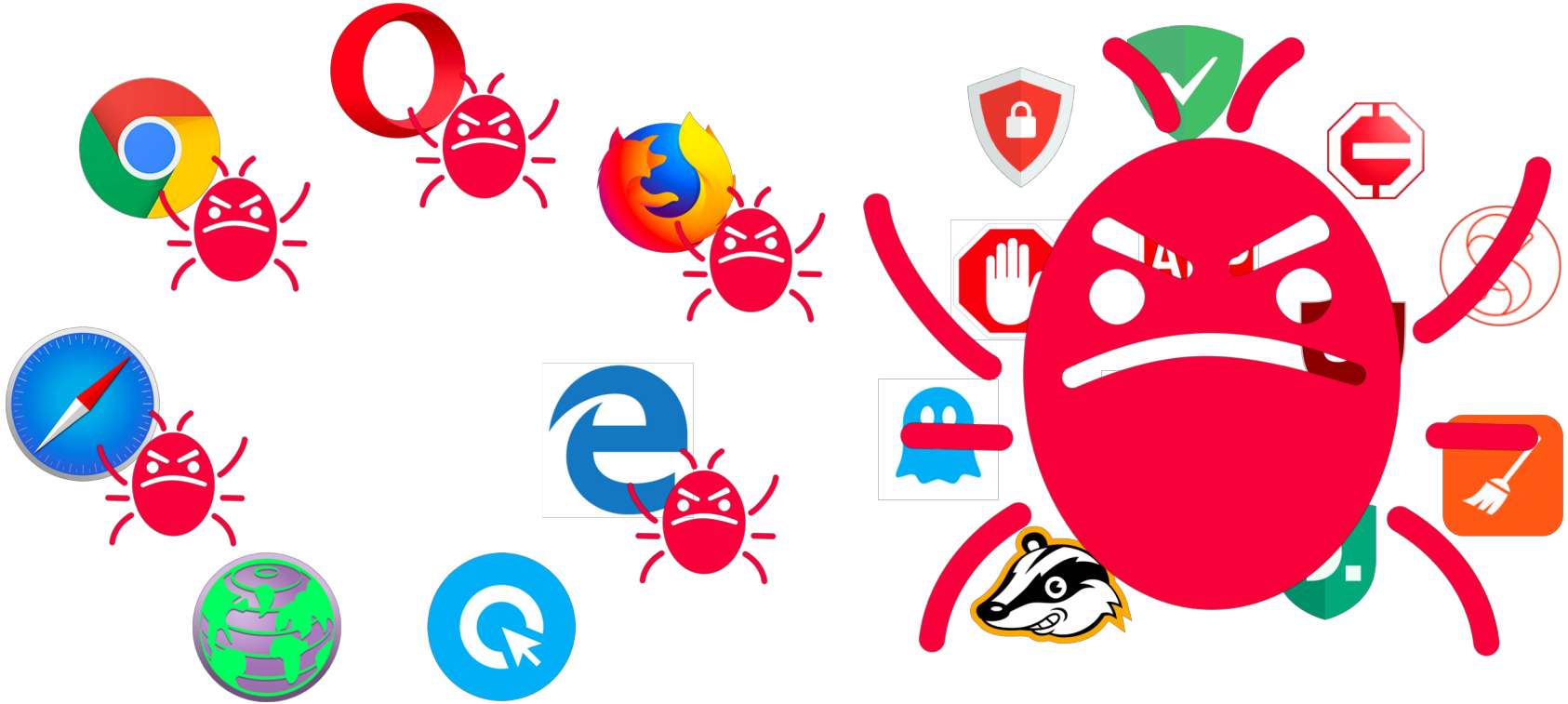
- Inline SVG in HTML5
- SVG (basic support)
- SVG effects for HTML
- SVG favicons
- SVG filters
- SVG fragment identifiers
- SVG in CSS backgrounds
- SVG in HTML img element
- SVG SMIL animation
- SVG fonts
- **All SVG features**

JS API

- AbortController & AbortSignal
- Accelerometer

Source: https://caniuse.com

Do you trust your browser?



Overview

Cookies & SOP 101

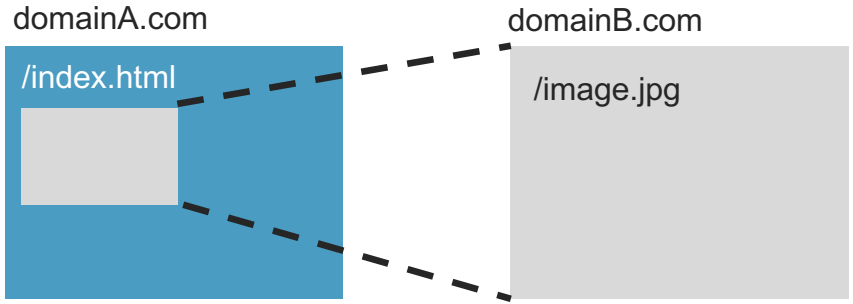
Cross-site attacks and tracking

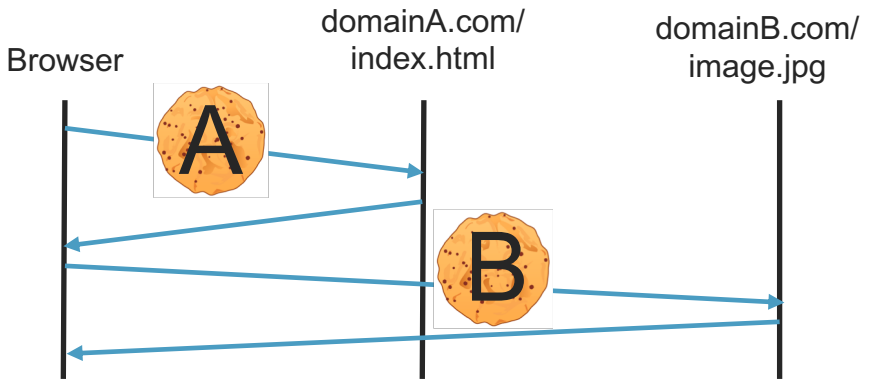
Third-party cookie policies

Comprehensive evaluation

Conclusion

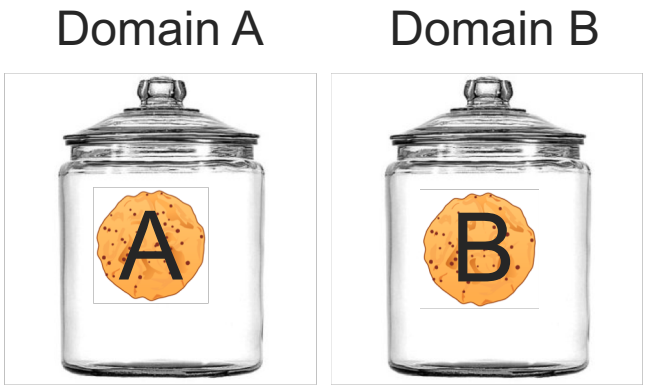
Cookie inclusion





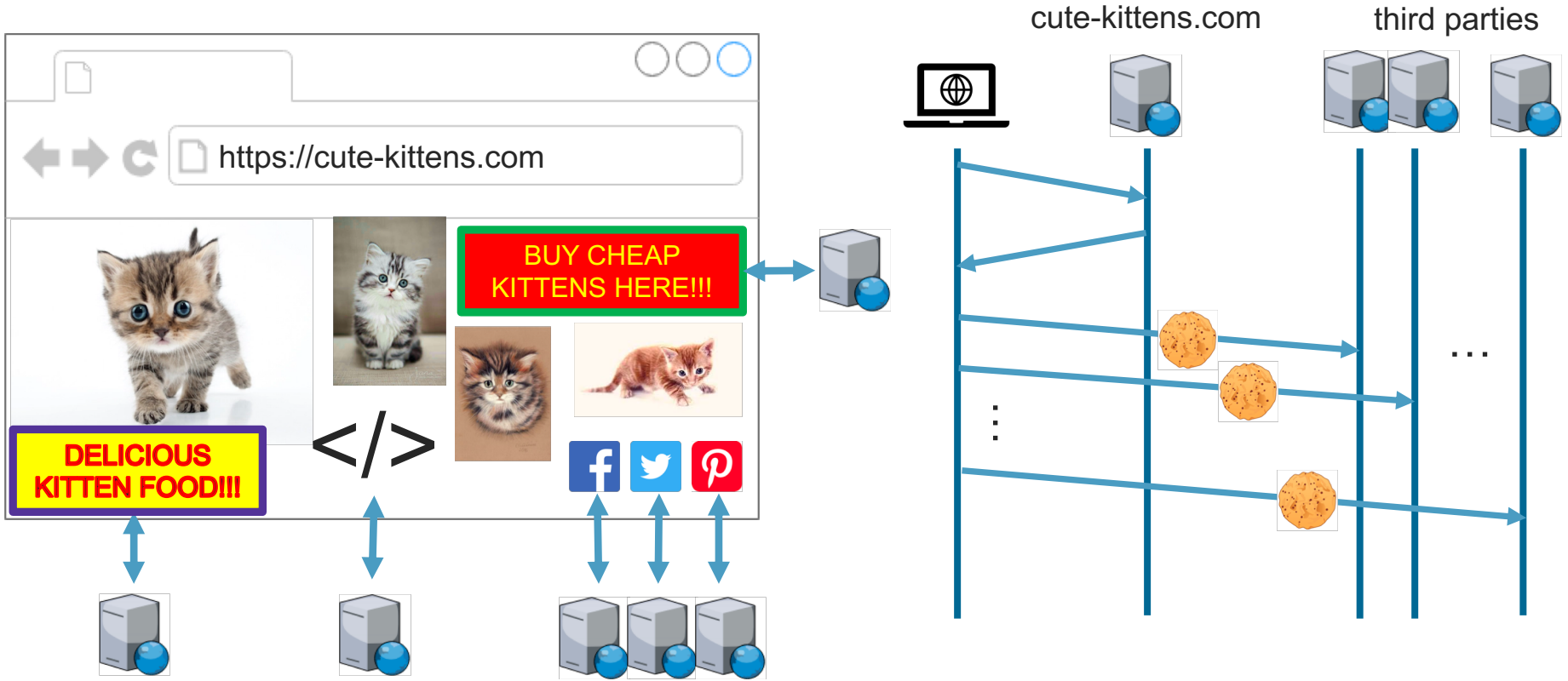
HTTP cookies [1]

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



[1] Barth, A., "HTTP State Management Mechanism", RFC 6265, DOI 10.17487/RFC6265, April 2011.

Third-party requests: implicit and ubiquitous

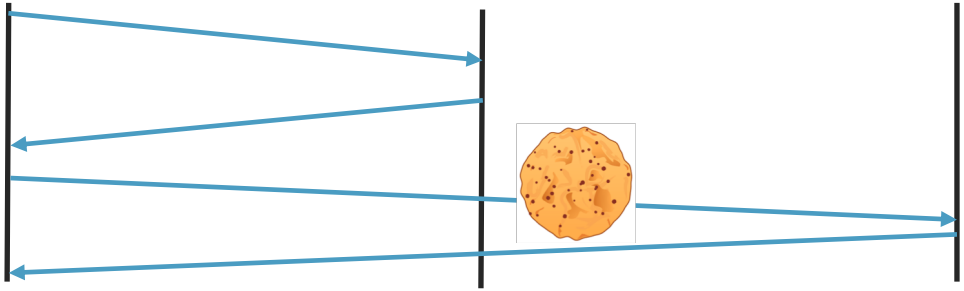


Cross-site attacks

Cross-site Request Forgery (CSRF)

victim cute-kittens.com doggo-bank.com

- Authenticated state-changing request



```
<img src="https://doggo-bank.com/transfer.php
    ?amount=999999&recipient=catboss">
```

Cross-site Request Forgery

- OWASP Top 10

2010
5th place

2013
8th place

2017
dropped

- Why?
  - Framework-integrated server-side defenses
  - Awareness

ZDNet

CENTRAL EUROPE

MUST READ: Meet the new Microsoft Phone, powered by Android (No Windows

could have

News Reviews How To's

APPUALS
FROM THE EXPERTS!

Follow Us

5,715 Fans

2,490 Subscribers

HELPNETSECURITY News Features Expert Analysis Reviews Events Whitepapers Industry news Newsletters

Featured news

- UK citizens fear identity theft over other security concerns such as national security
- How science can fight insider threats
- The risk to OT networks is real, and it's dangerous for business leaders to ignore
- 66% UK SMBs believe they are being aggressively targeted by fraudsters
- Phishing attacks becoming more targeted, phishers

Zeljka Zorz, Managing Editor
October 3, 2018

Share this article

Popular TP-Link wireless home router open to remote hijacking

By concatenating a known improper authentication flaw with a newly discovered CSRF vulnerability, remote unauthenticated control over TP-Link TL-WR841N worldwide

How science can fight insider threats

How to make the CFO your best cybersecurity friend

Safeguarding hybrid-cloud infrastructures through identity privilege management

Why you should take an operational approach to risk management

Cross-site Request Forgery

- Why is this still a problem?
  - Defense (e.g. random token in request parameters) needs to be applied ubiquitously
  - Insecure by default
- How to move on from here?
  - SameSite cookies -> secure by default (if enforced correctly by the browser)

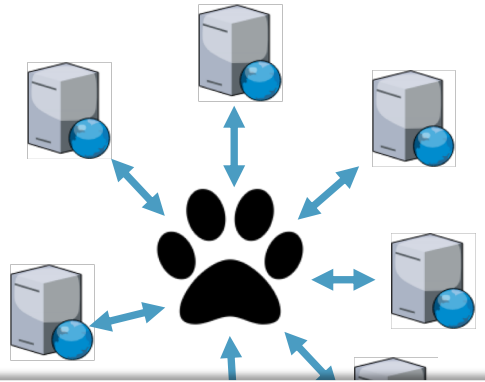

CROSS-SITE ATTACKS
LIGHTYEAR
CROSS-SITE ATTACKS EVERYWHERE

Cross-site attacks everywhere

- HEIST (HTTP Encrypted Information can be Stolen through TCP-windows)
- Cache API abuse
- Quota management API abuse
- Storage API abuse
- Cross-site size exposing
- Cross-site search
- Cross-site script inclusion / JSON hijacking
- Cross-site timing attacks

Third-party tracking

Third-party Tracking



victim

cat-news.com

paw-book.com

Tracking the Trackers

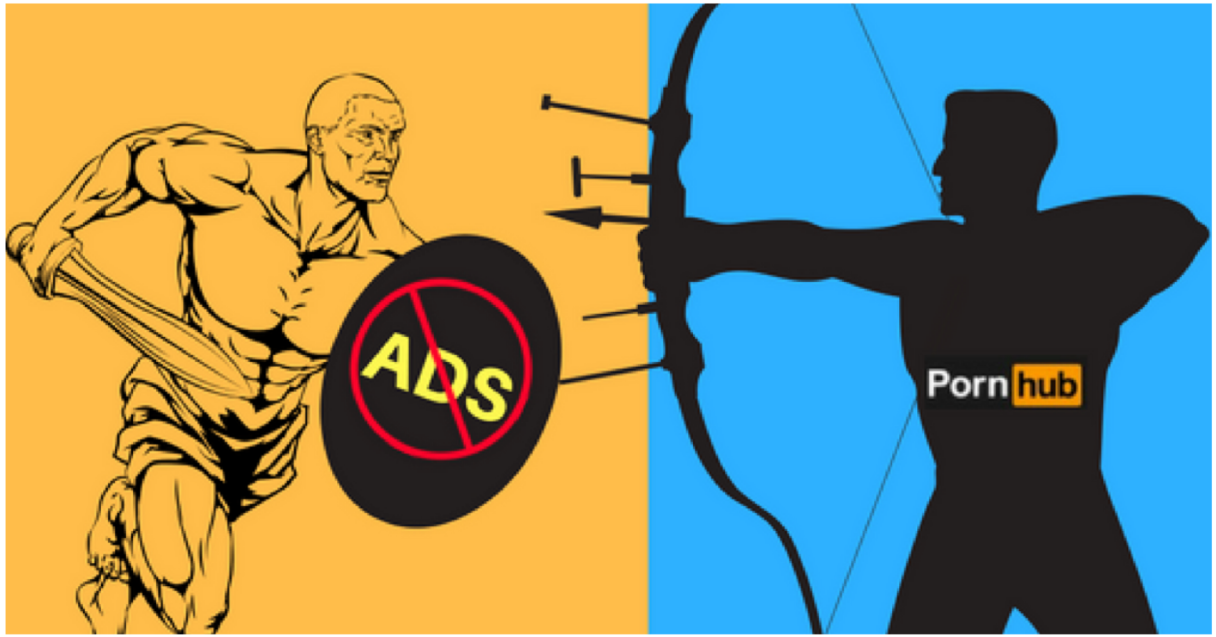
Zhonghao Yu Sam Macbeth Konark Modi

"95% of the pages visited contain 3rd party requests to potential trackers
78% attempt to transfer unsafe data"

Cliqz
Arabellastraße 23

Pornhub Bypasses Ad Blockers With WebSockets

BugReplay Follow
Nov 1, 2016 · 4 min read



Third-party cookie policies

Cookie policies for privacy

- Built-in browser options
  - Block third-party cookies
  - Firefox Tracking Protection
  - Opera Ad Blocker
  - Safari Intelligent Tracking Prevention
- Extensions
  - Ad blocking
  - Privacy protection

Client-side defense mechanisms

Same-site cookie [1]

In-depth defense against cross-site attacks

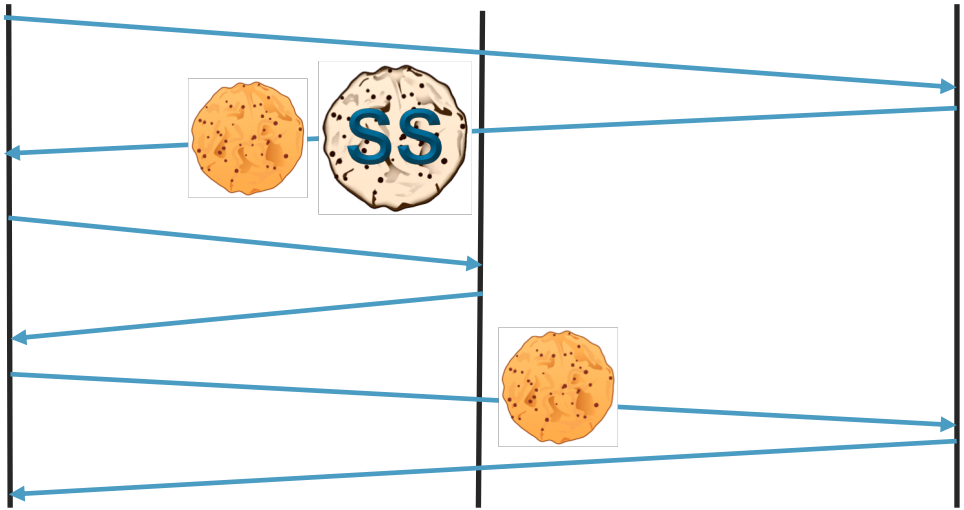
- Cookie with extra attribute ‘SameSite’
  - SameSite=strict → NO CROSS-SITE REQUESTS!
  - SameSite=lax → exceptions: top-level GET, prerender
- Adoption by websites is rather slow
  - Interesting blog: Dropbox’s use case [2]

[1] West, M., Goodwin, M. Same-site cookies. Internet- Draft draft-ietf-httpbis-cookie-same-site-00, IETF Secretariat, June 2016.
[2] https://blogs.dropbox.com/tech/2017/03/preventing-cross-site-attacks-using-same-site-cookies/

Use of same-site cookies

against cross-site attacks

doggo-bank.com victim cute-kittens.com doggo-bank.com



```
Set-Cookie: auth=ekSd2lksq090pQDs; 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
- Saturated market of extensions
  - No clear quantification of quality

Automated evaluation of effectiveness

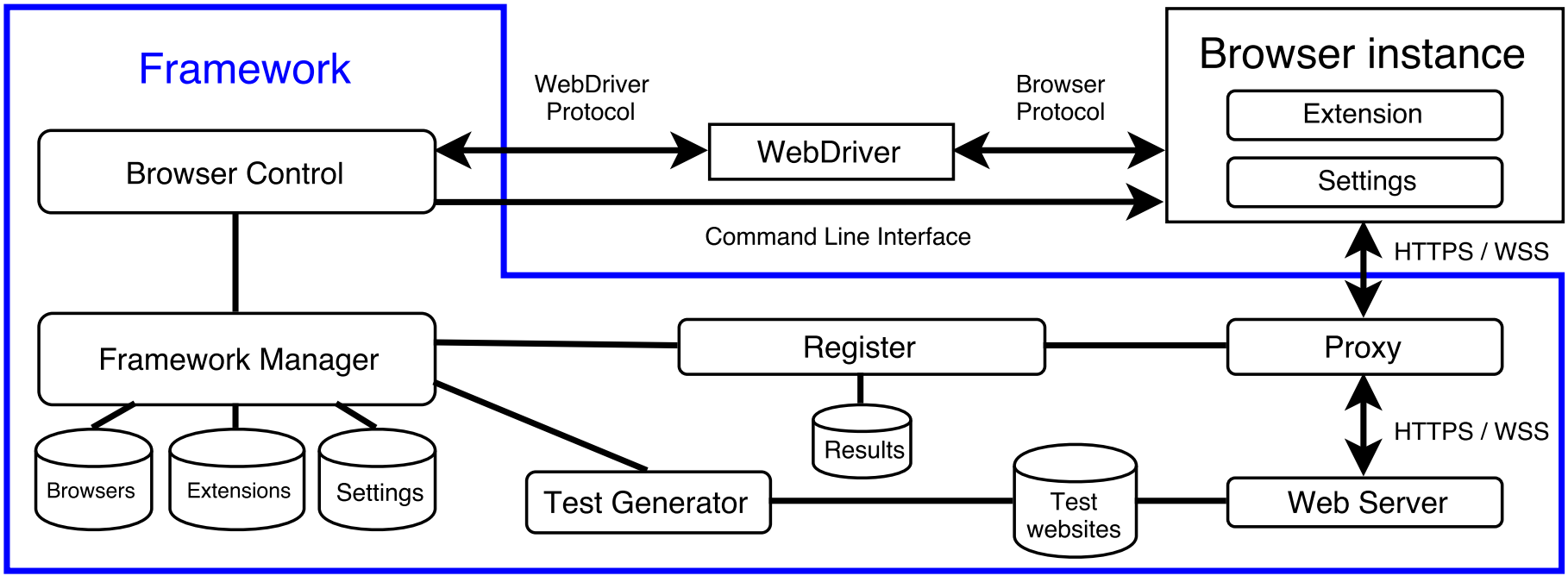
Comprehensive evaluation

Black box approach

- Browsers consist of millions of lines of code
  - Source code not always available
- Many extensions

Framework

Design



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

Overview

- Browsers
  - Chrome SameSite
  - Opera SameSite
  - Firefox SameSite
  - Safari SameSite
  - Edge SameSite
  - Tor Browser
  - Cliqz
- Extensions
  - Ad blocking (31)

...

  - Tracking protection (15)

...

	AppCache	HTML	Headers	Redirects	PDF JS	JavaScript	SW
Chrome 63	●	●	●	●	●	●	●
- Block third-party cookies	◐	◐	◐	●	●	◐	◐
Opera 51	●	●	●	●	●	●	●
- Block third-party cookies*	◐	◐	◐	●	●	◐	◐
- Ad Blocker	●	●	○	●	○	●	●
Firefox 57	●	●	●	●	○	●	●
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
- Tracking Protection	●	●	●	●	○	●	●
Safari 11	○†	◐	○	●	○	◐	N/A
- No Intelligent Tracking Prevention	●†	●	○	●	○	●	N/A
- Block third-party cookies‡	●†	●	◐	●	○	●	N/A
Edge 40	●	●	◐	●	○	●	N/A
- Block third-party cookies	●	●	◐	●	○	●	N/A
Cliqz 1.17*	◐	●	◐	●	○	◐	◐
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
Tor Browser 7	○	◐	◐	●	○	◐	N/A

●: 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

	AppCache	HTML	Headers	Redirects	PDF JS	JavaScript	SW
Chrome 63	●	●	●	●	●	●	●
- Block third-party cookies	◐	◐	◐	●	●	◐	◐
Opera 51	●	●	●	●	●	●	●
- Block third-party cookies*	◐	◐	◐	●	●	◐	◐
- Ad Blocker	●	●	○	●	○	●	●
Firefox 57	●	●	●	●	○	●	●
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
- Tracking Protection	●	●	●	●	○	●	●
Safari 11	○†	◐	○	●	○	◐	N/A
- No Intelligent Tracking Prevention	●†	●	○	●	○	●	N/A
- Block third-party cookies‡	●†	●	◐	●	○	●	N/A
Edge 40	●	●	◐	●	○	●	N/A
- Block third-party cookies	●	●	◐	●	○	●	N/A
Cliqz 1.17*	◐	●	◐	●	○	◐	◐
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
Tor Browser 7	○	◐	◐	●	○	◐	N/A

●: 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

	AppCache	HTML	Headers	Redirects	PDF JS	JavaScript	SW
Chrome 63	●	●	●	●	●	●	●
- Block third-party cookies	◐	◐	◐	●	●	◐	◐
Opera 51	●	●	●	●	●	●	●
- Block third-party cookies*	◐	◐	◐	●	●	◐	◐
- Ad Blocker	●	●	○	●	○	●	●
Firefox 57	●	●	●	●	○	●	●
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
- Tracking Protection	●	●	●	●	○	●	●
Safari 10	○†	◐	○	●	○	◐	N/A
- No Intelligent Tracking Prevention	●†	●	○	●	○	●	N/A
- Block third-party cookies‡	●†	●	◐	●	○	●	N/A
Edge 40	●	●	◐	●	○	●	N/A
- Block third-party cookies	●	●	◐	●	○	●	N/A
Cliqz 1.17*	◐	●	◐	●	○	◐	◐
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
Tor Browser 7	○	◐	◐	●	○	◐	N/A

●: 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

	AppCache	HTML	Headers	Redirects	PDF JS	JavaScript	SW
Chrome 63	●	●	●	●	●	●	●
- Block third-party cookies	◐	◐	◐	●	●	◐	◐
Opera 51	●	●	●	●	●	●	●
- Block third-party cookies*	◐	◐	◐	●	●	◐	◐
- Ad Blocker	●	●	○	●	○	●	●
Firefox 57	●	●	●	●	○	●	●
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
- Tracking Protection	●	●	●	●	○	●	●
Safari 11	○†	◐	○	●	○	◐	N/A
- No Intelligent Tracking Prevention	●‡	●	○	●	○	●	N/A
- Block third-party cookies‡	●‡	●	◐	●	○	●	N/A
Edge 40	●	●	◐	●	○	●	N/A
- Block third-party cookies	●	●	◐	●	○	●	N/A
Cliqz 1.17*	◐	●	◐	●	○	◐	◐
- Block third-party cookies	◐	◐	◐	●	○	◐	◐
Tor Browser 7	○	◐	◐	●	○	◐	N/A

●: 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

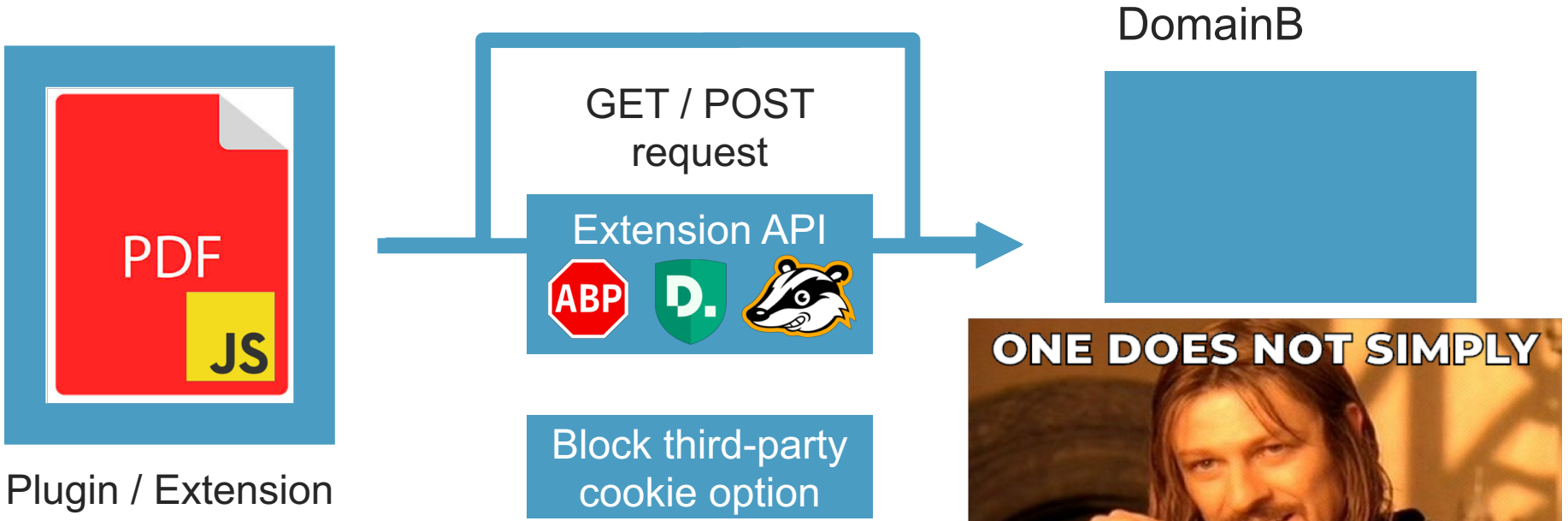
Extensions

Tested in Chrome, Firefox, Opera and Edge

- 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



Unclear WebExtension API

AppCache API

```
<html manifest='/manifest.appcache'>
```

```
CACHE MANIFEST
# ...

CACHE:
https://tracker.com/report/?leak=appcache-cache
```

-1	chrome.tabs.TAB_ID_NONE	Since Chrome 46. An ID that represents the absence of a browser tab.

tabs.TAB_ID_NONE

A special ID value given to tabs that are not browser tabs (for example, tabs in devtools windows).

Affected browsers:

Unclear WebExtension API

ServiceWorker API

- Firefox
  - Assign tab id of tab that initiated ServiceWorker
  - Blocked by <u>all</u> extensions

Affected browsers:

Common mistakes by extension developers

- Requesting insufficient permissions
- Catch: WebSockets use ws:// and wss://
- Solution: use “<all_urls>”

Extension manifest

```
{
    "name": "My extension",
    ...
    "permissions": [
        "webRequest",
        “http://*/*”,
        “https://*/*
    ],
    ...
}
```

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
- Firefox and Safari: no bugs detected

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 websites
  - Up to 20 pages on each website
  - 160,059 pages visited

Conclusion

Conclusion

Initial findings

- 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 cookie policy bypass)

- Originally reported for Chrome 57
- Present in: 58 59 60 61
- Fixed in: 62 63 64 65
- Reintroduced in: 66 67 68 69 70 71

- Shows importance of a comprehensive evaluation of implemented policies

Key takeaways

- Virtually every built-in third-party cookie policy, and every adblocking and privacy extension can be bypassed

- The current state of browser policy testing is inadequate

- Browser evaluation results available at WhoLeftOpenTheCookieJar.com

Thank you!

WhoLeftOpenTheCookieJar.com

@tomvangoethem @gjfr_ @wlotcj