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

Tom Van Goethem (joint work with Gertjan Franken & Wouter Joosen)

22 February 2019

KU LEUVEN DistriNet

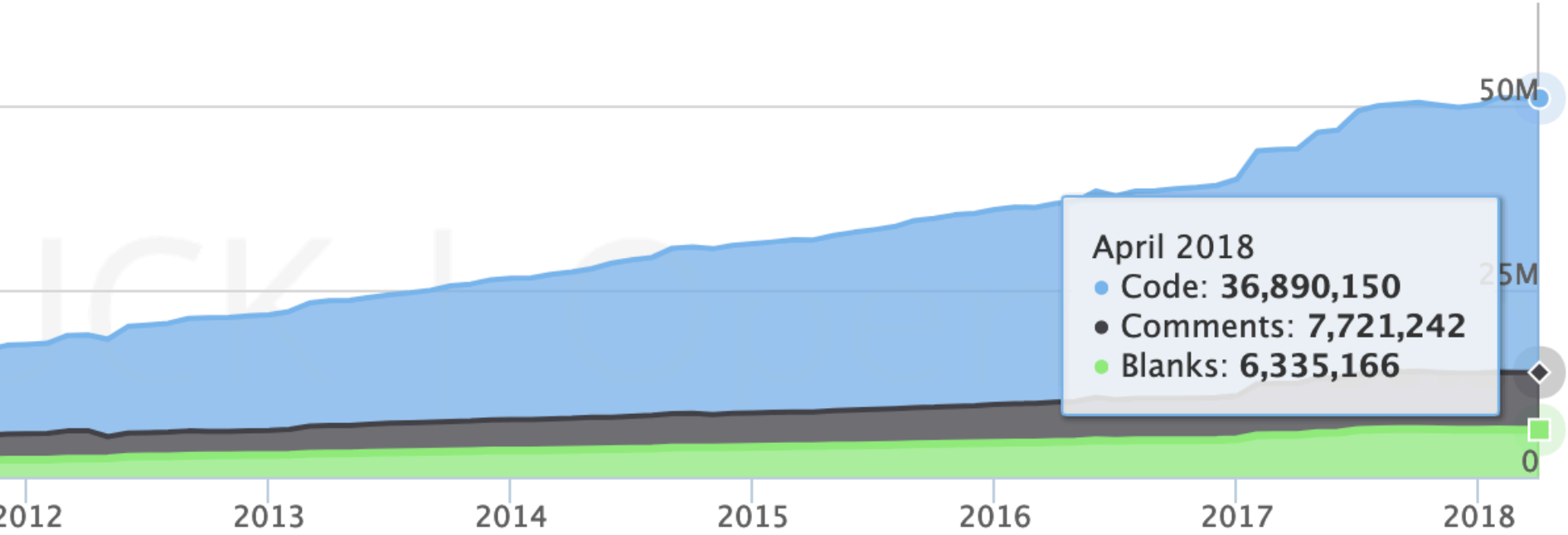
When the web was designed, security was a high priority.

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

Do you trust your browser?

How many lines of code does Firefox have?

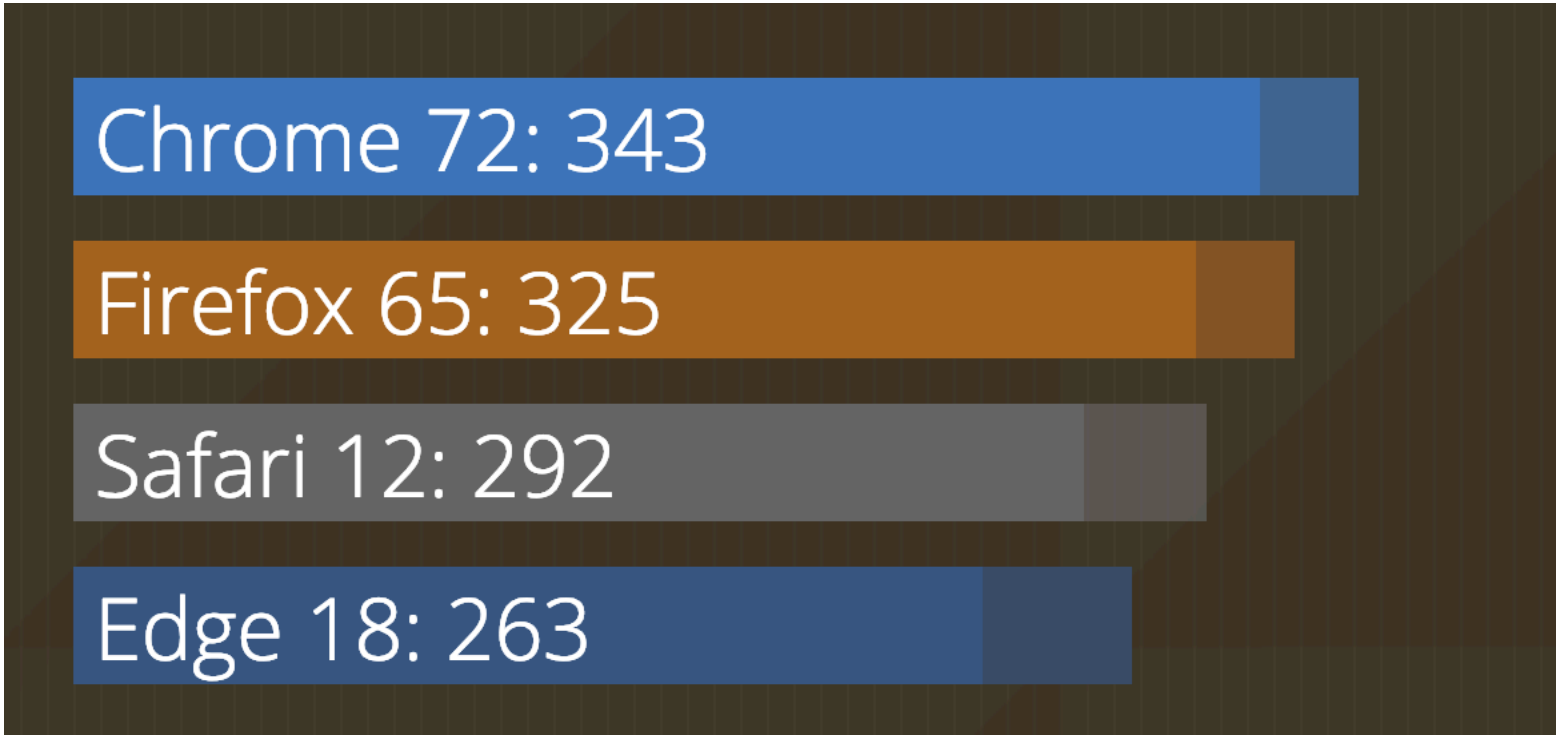
Lines of code for Firefox



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

KU LEUVEN DistriNet

How many different features do modern browser 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

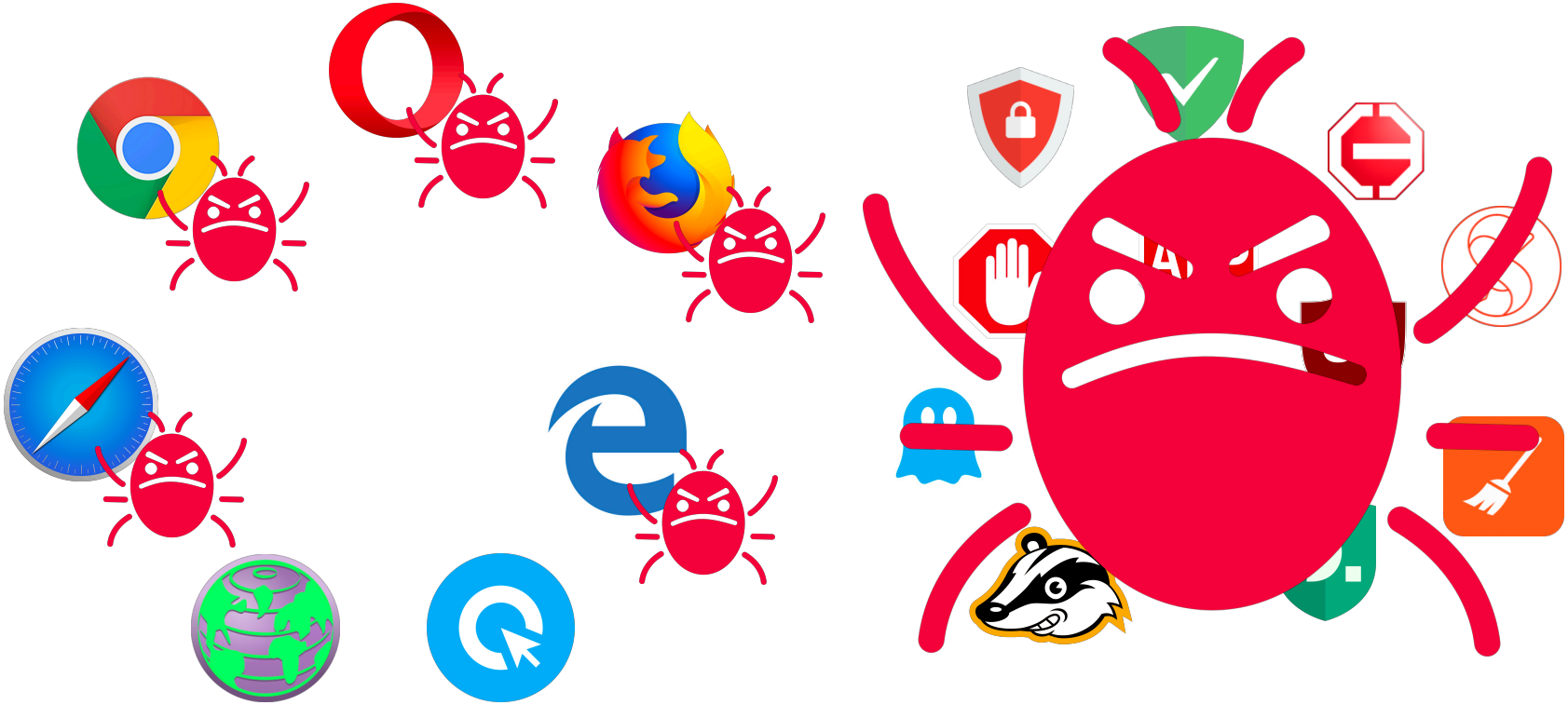
- AbortController & AbortSignal
- Accelerometer

Source: https://caniuse.com

Do you trust your browser?

Do you use an ad-blocker or anti-tracking extension?

Do you trust your privacy extension to block all trackers/ads?



Overview

Cookies & SOP 101

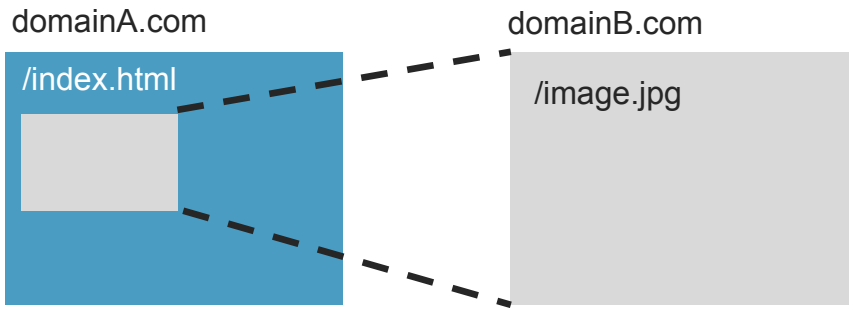
Cross-site attacks and tracking

Third-party cookie policies

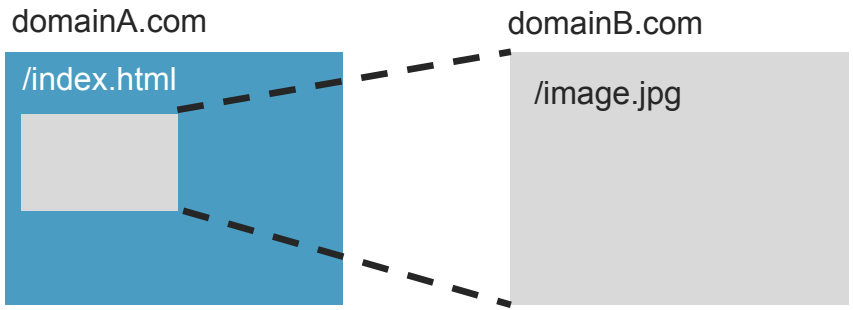
Comprehensive evaluation

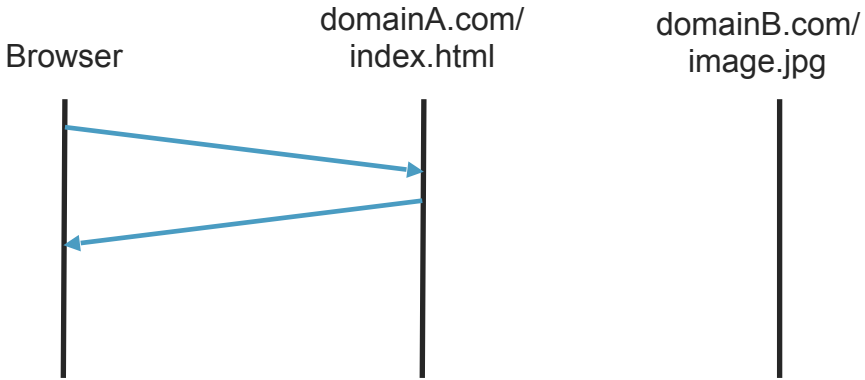
Conclusion

Cookie inclusion

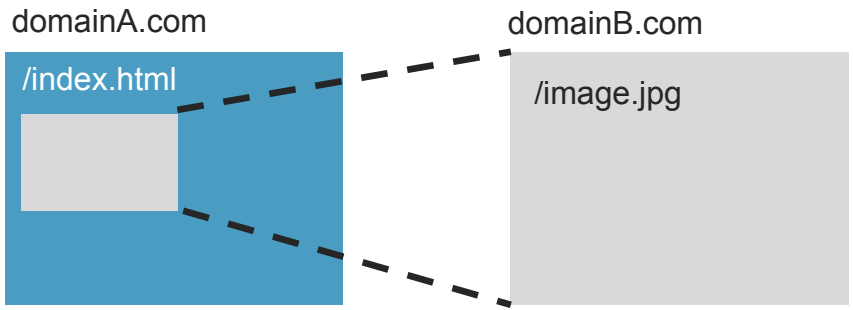


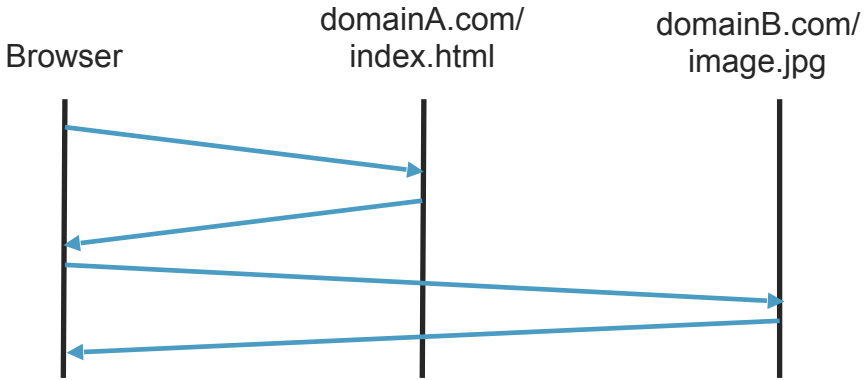
Cookie inclusion



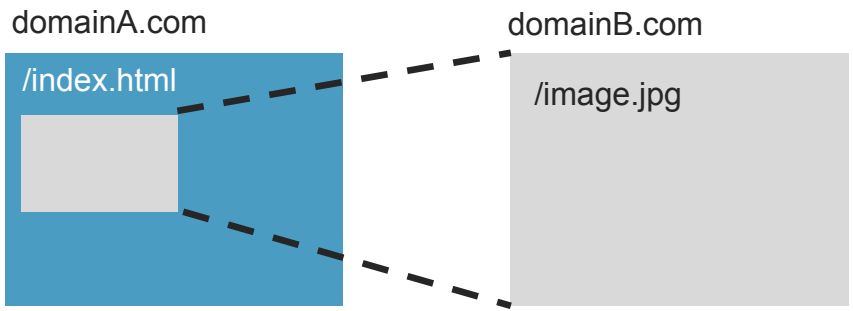


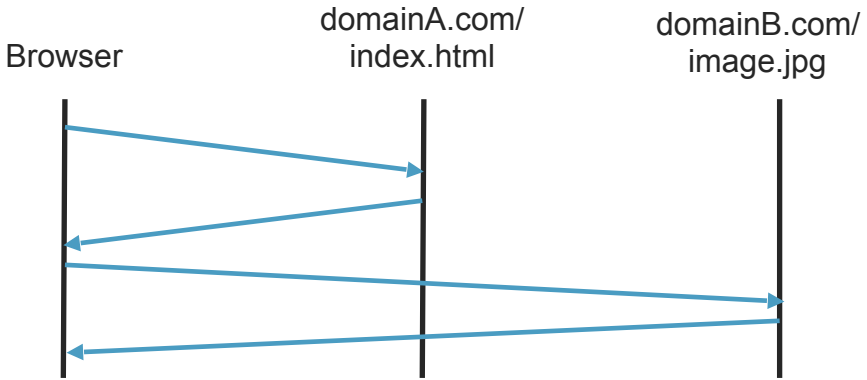
Cookie inclusion





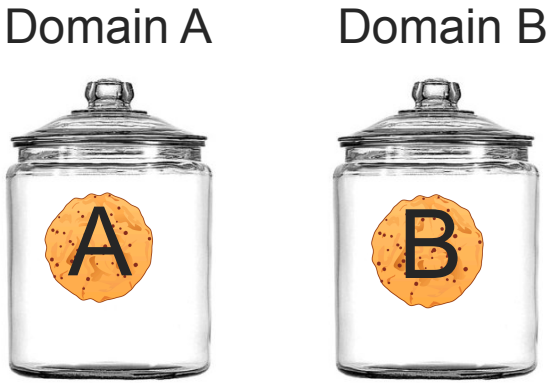
Cookie inclusion





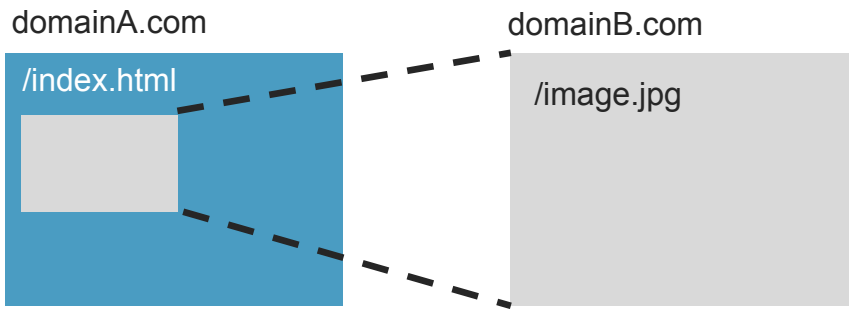
HTTP cookies [1]

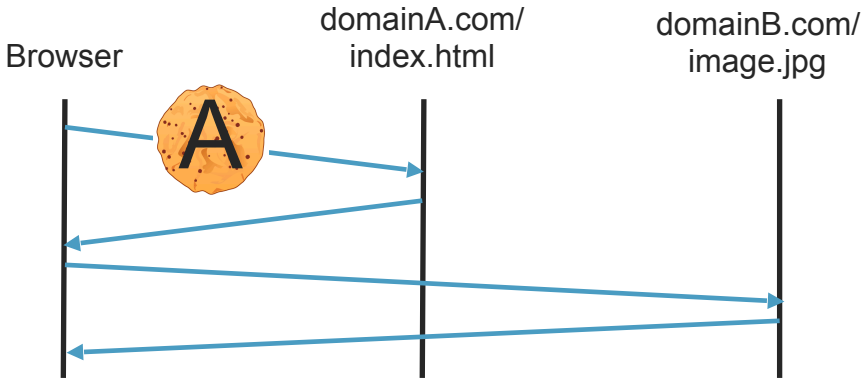
- Implicit inclusion
- Authentication / identification
- Same-Origin Policy



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

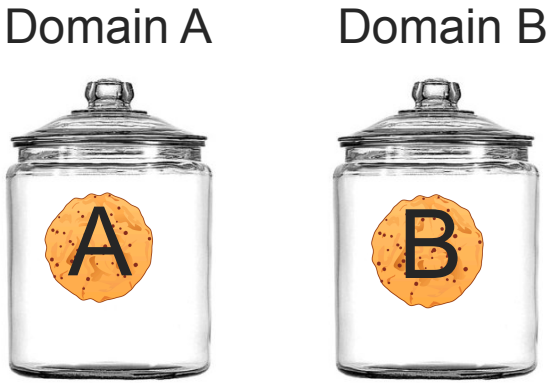
Cookie inclusion





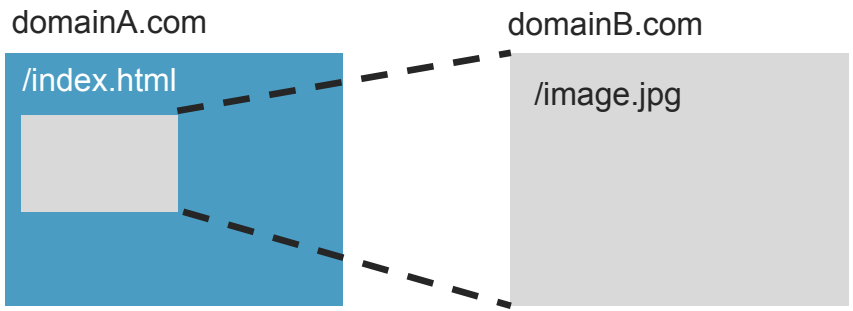
HTTP cookies [1]

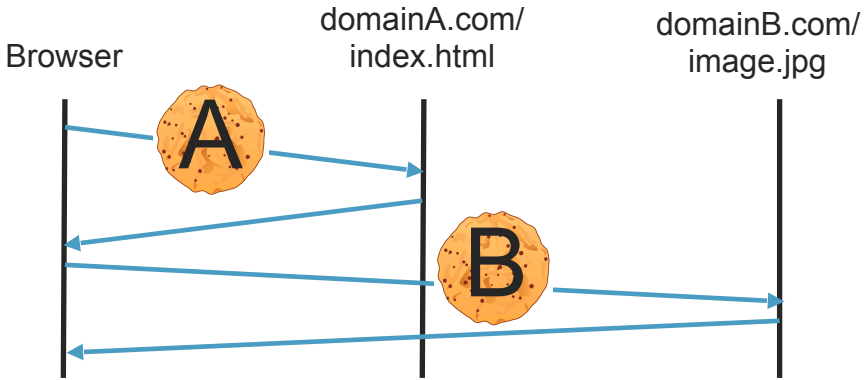
- Implicit inclusion
- Authentication / identification
- Same-Origin Policy



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

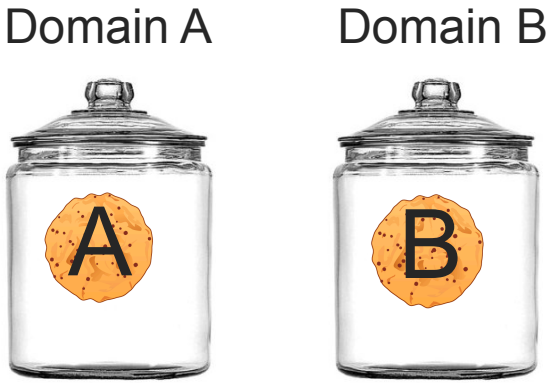
Cookie inclusion





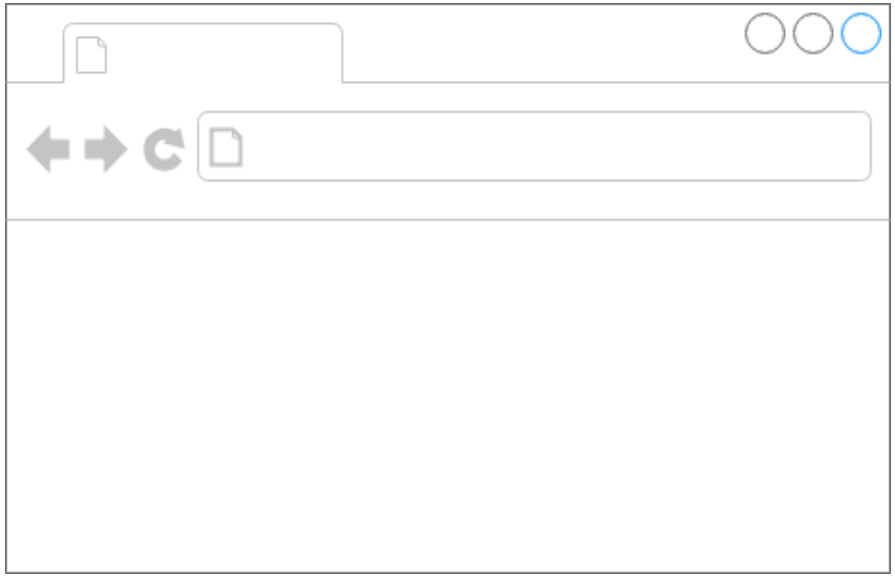
HTTP cookies [1]

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

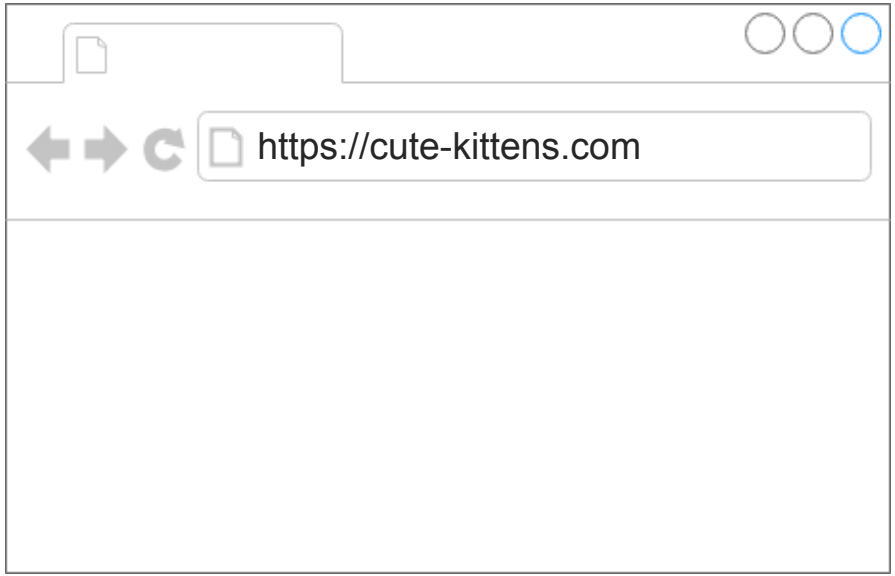


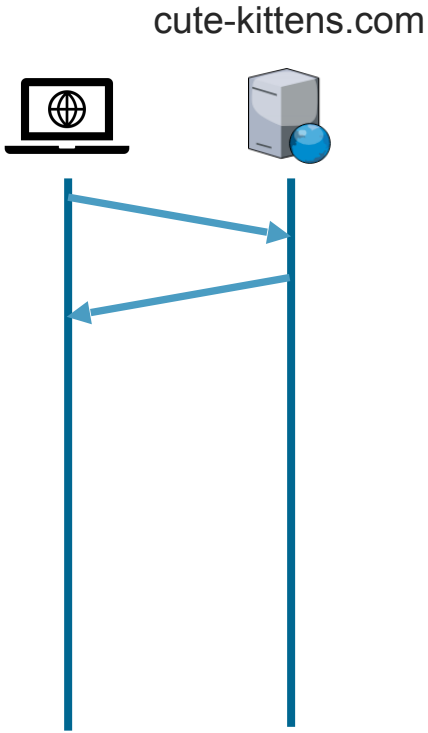
[1] Barth, A., "HTTP State Management Mechanism", RFC 6265, DOI 10.17487/RFC6265, April 2011.

Third-party requests: implicit and ubiquitous

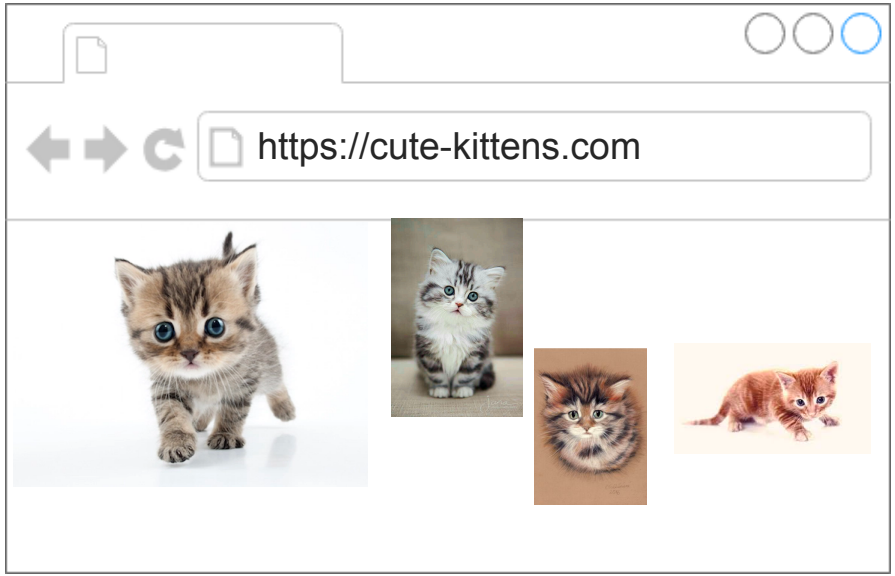


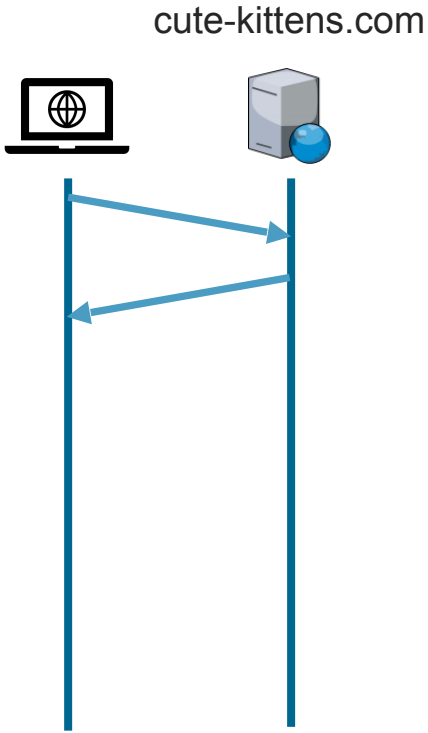
Third-party requests: implicit and ubiquitous



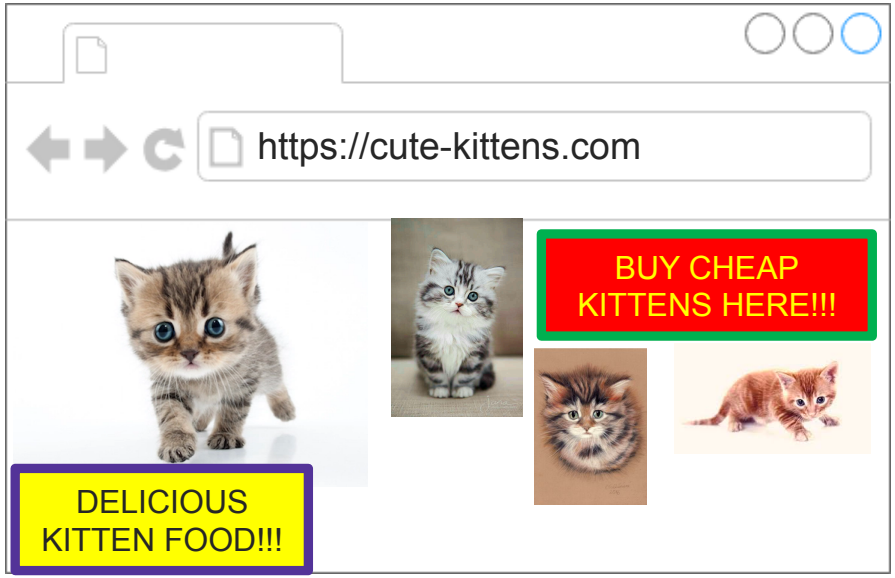


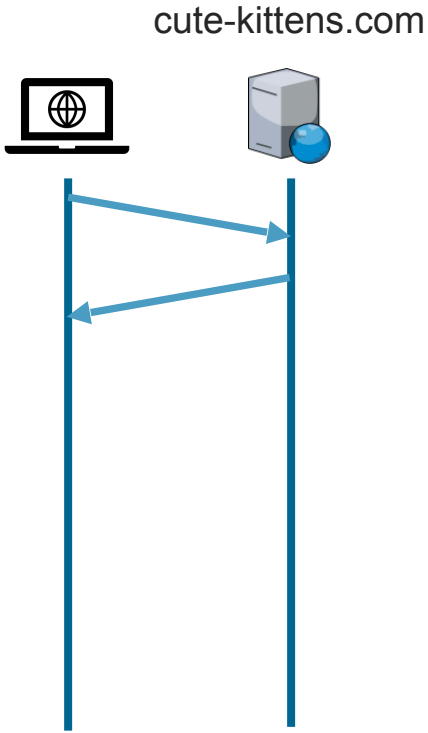
Third-party requests: implicit and ubiquitous





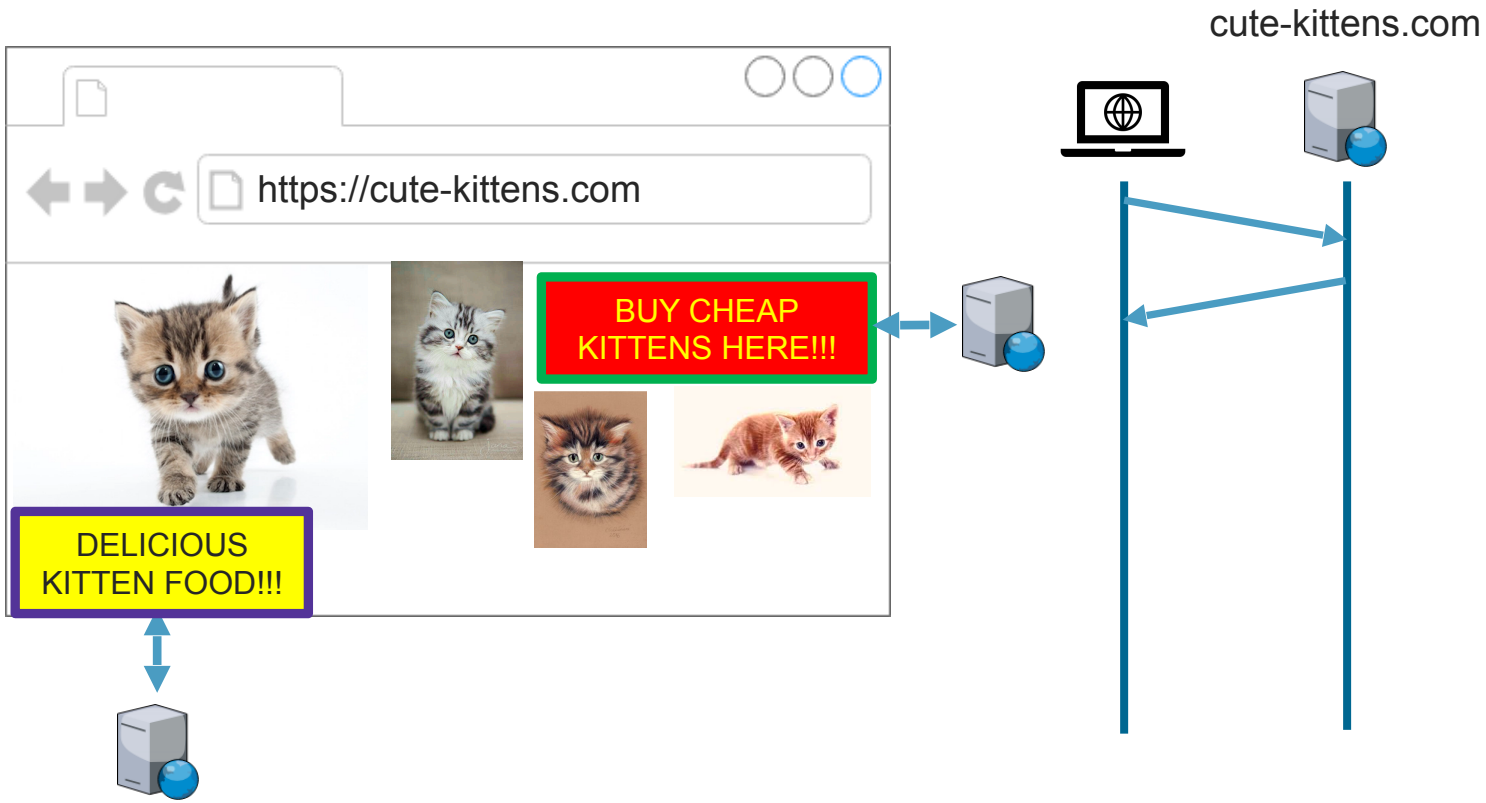
Third-party requests: implicit and ubiquitous



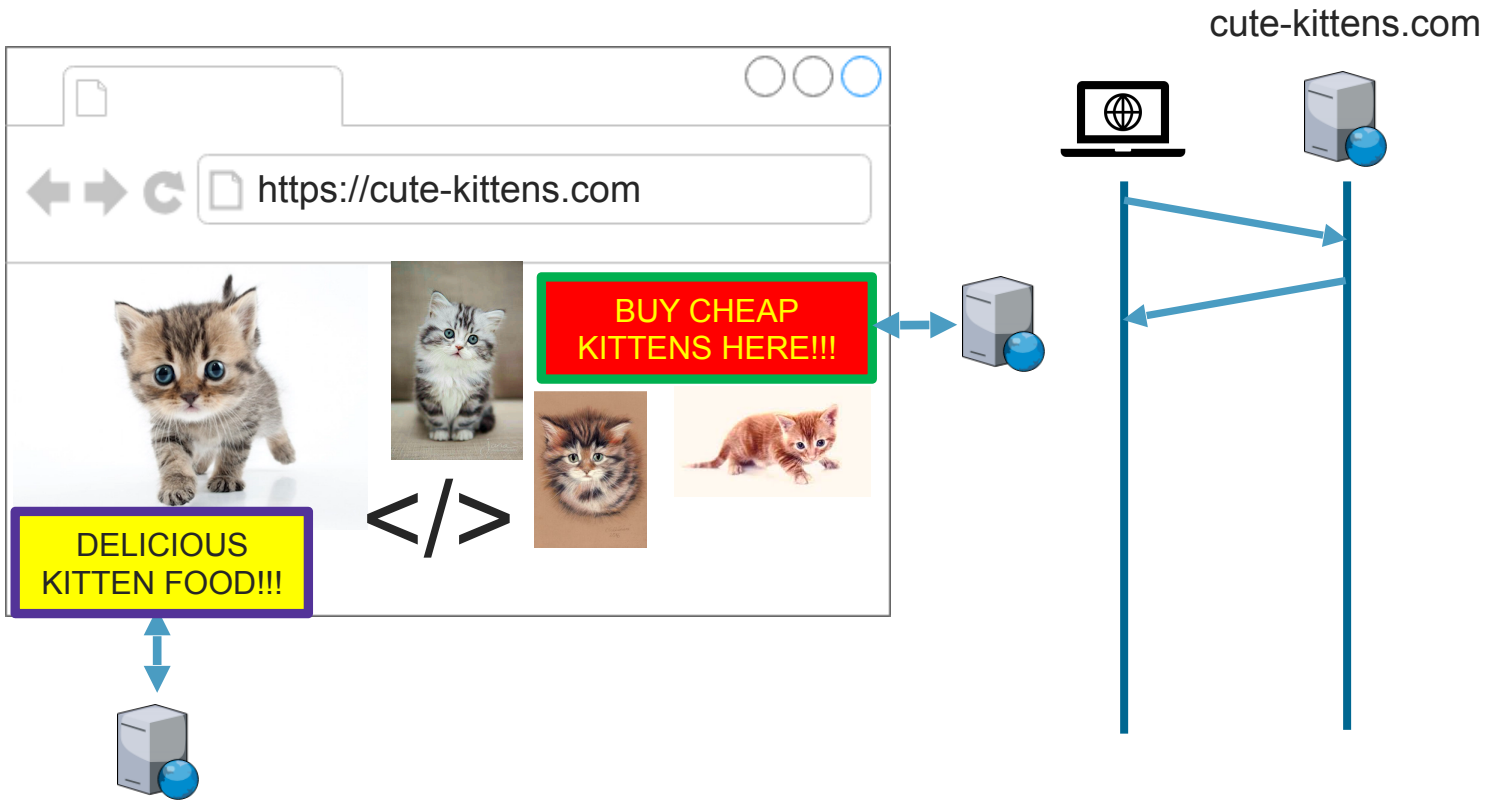


KU LEUVEN DistriNet

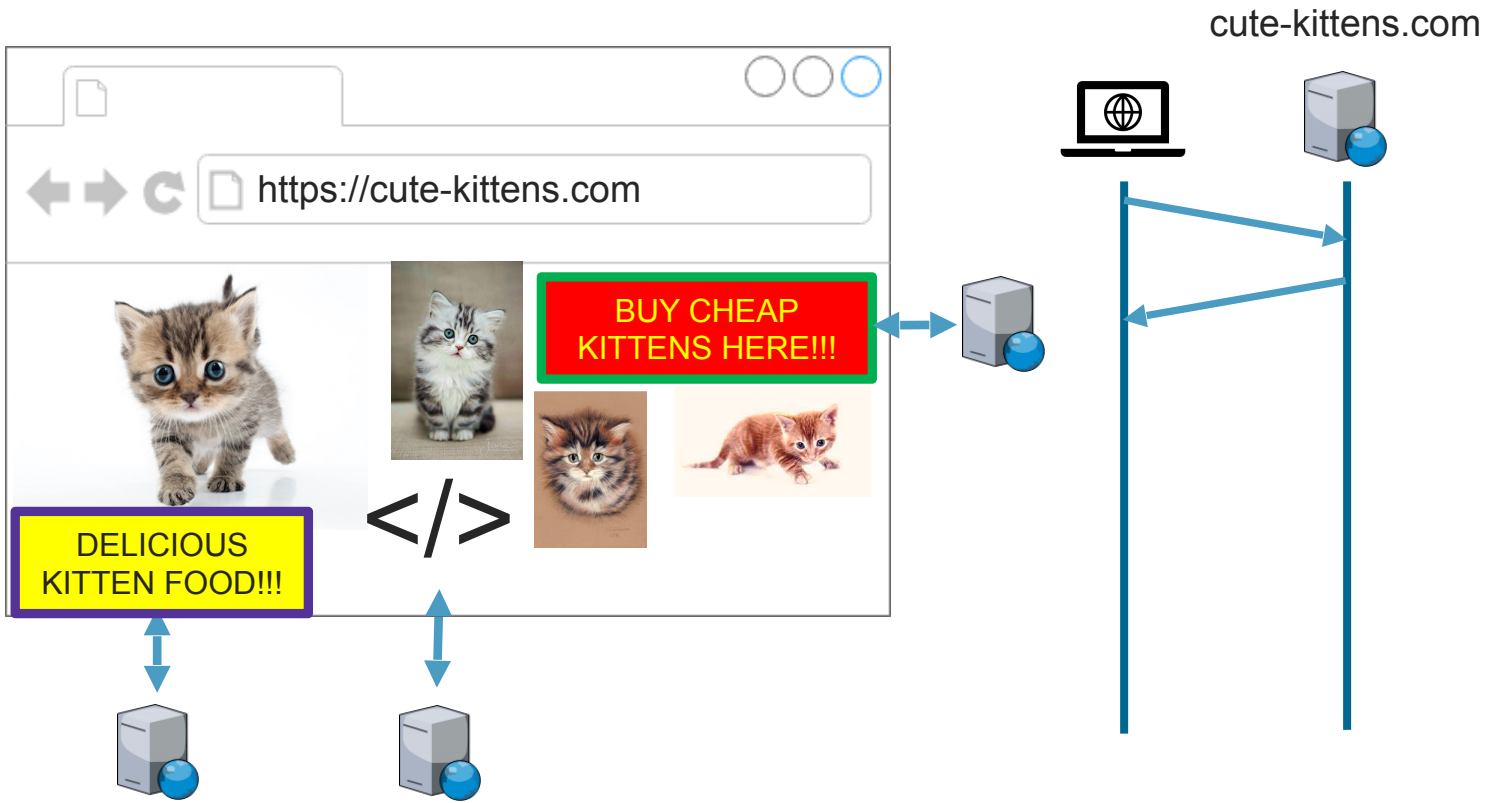
Third-party requests: implicit and ubiquitous



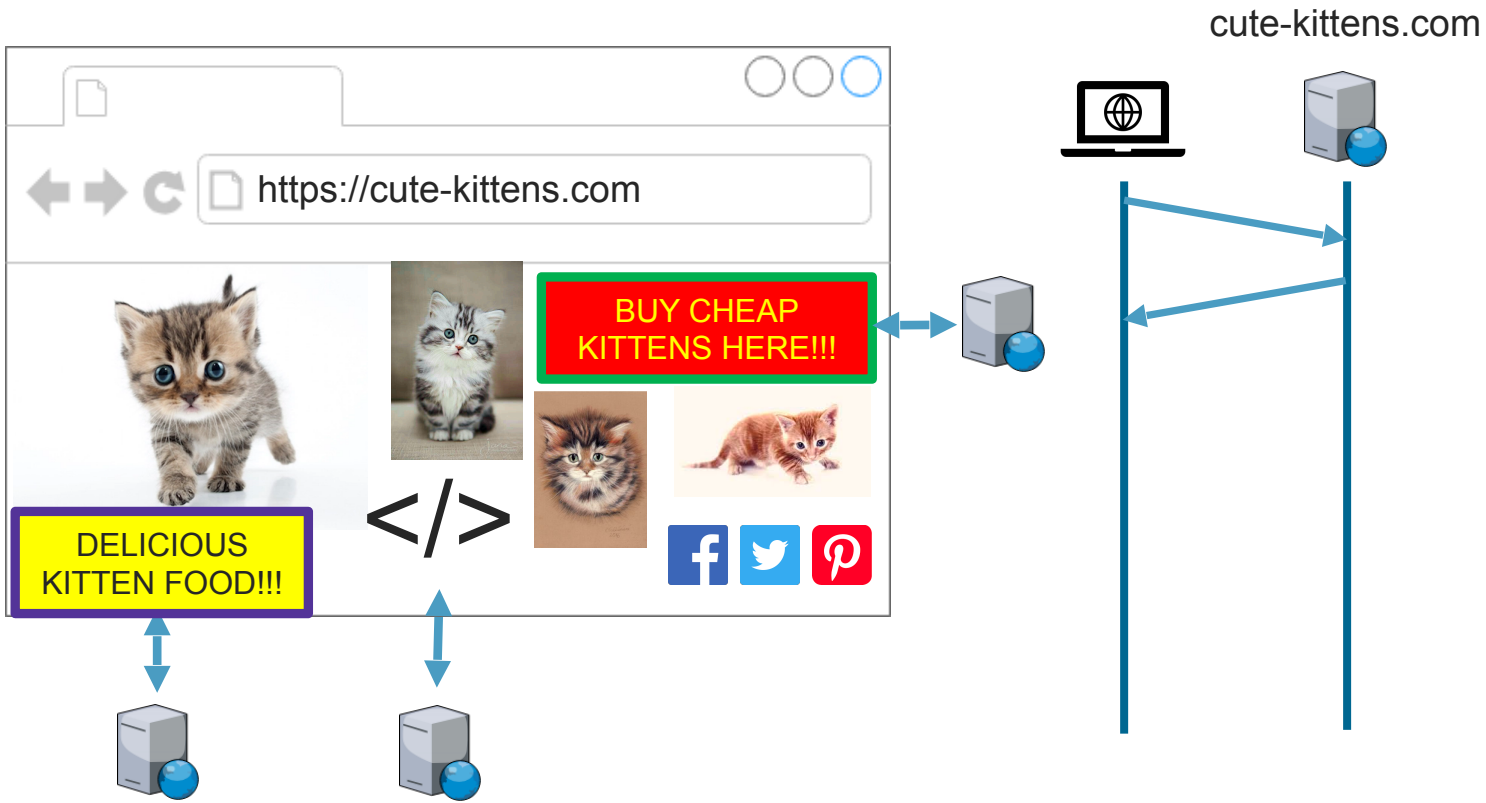
Third-party requests: implicit and ubiquitous



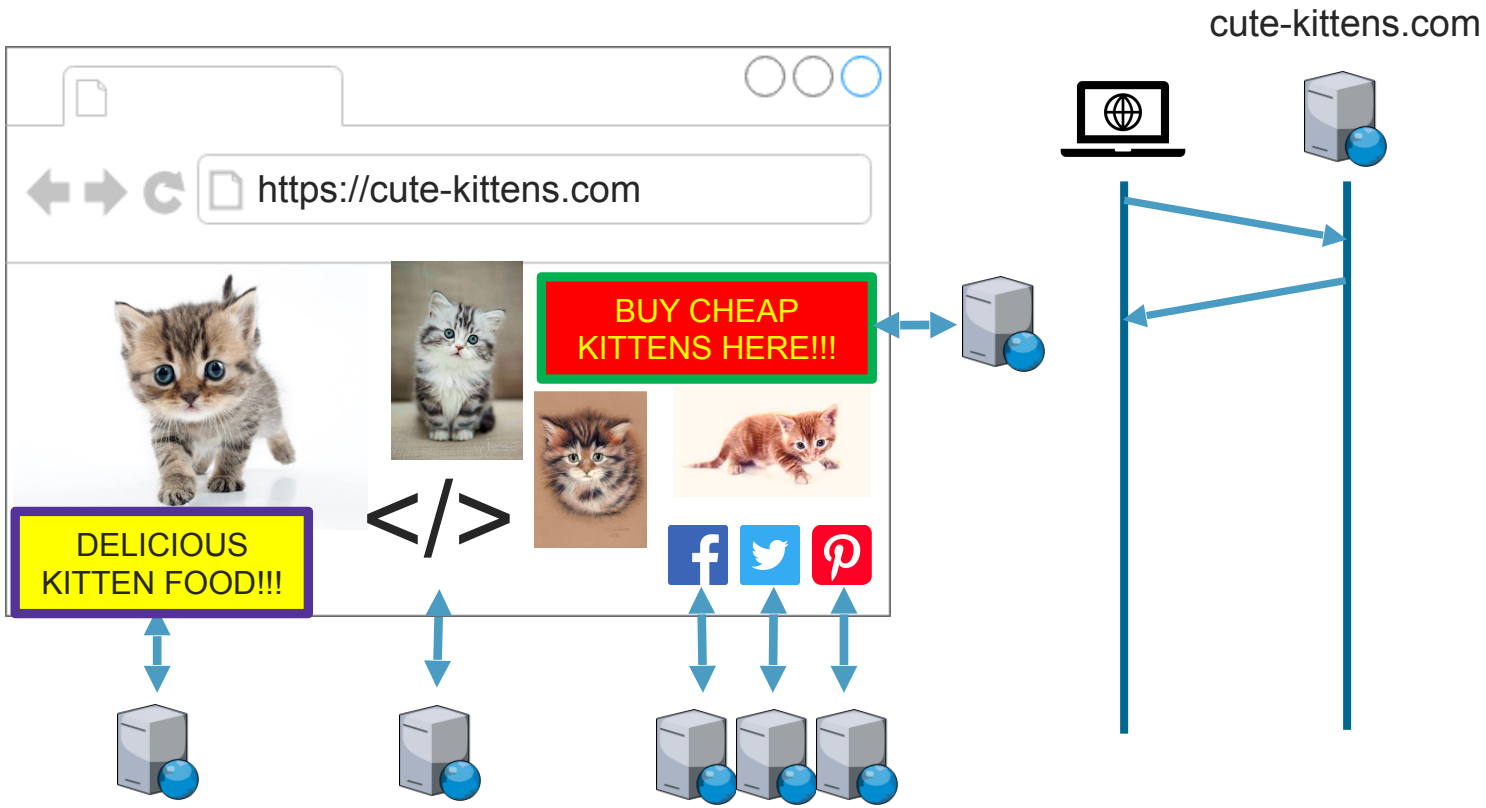
Third-party requests: implicit and ubiquitous



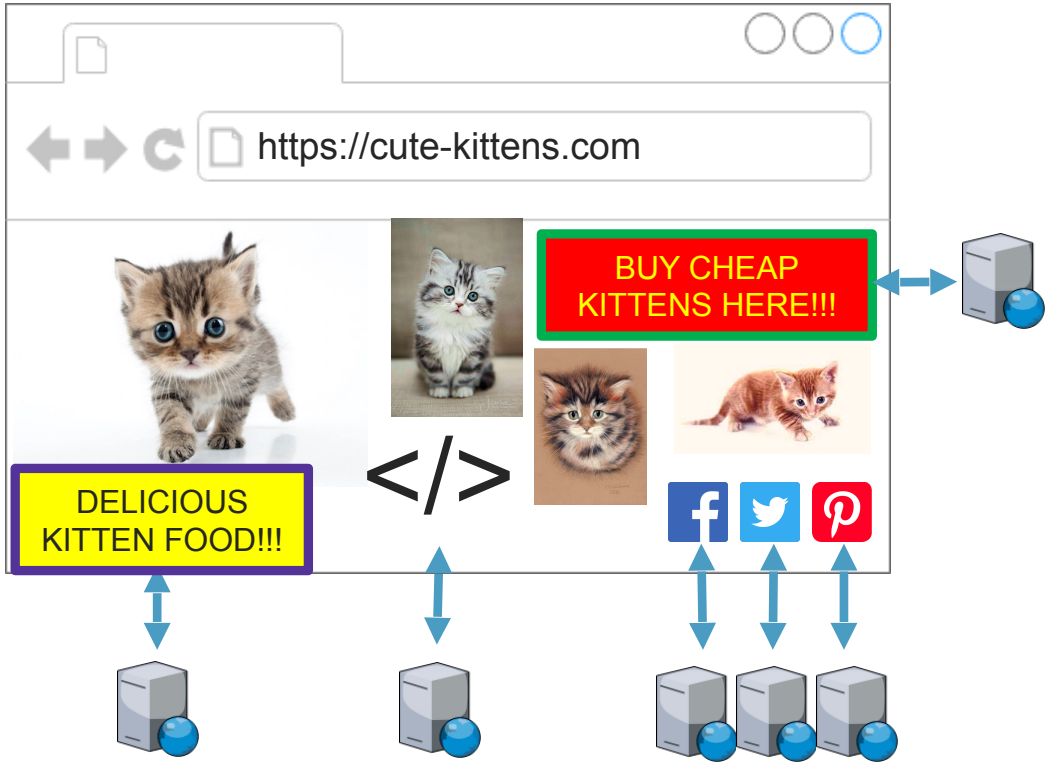
Third-party requests: implicit and ubiquitous

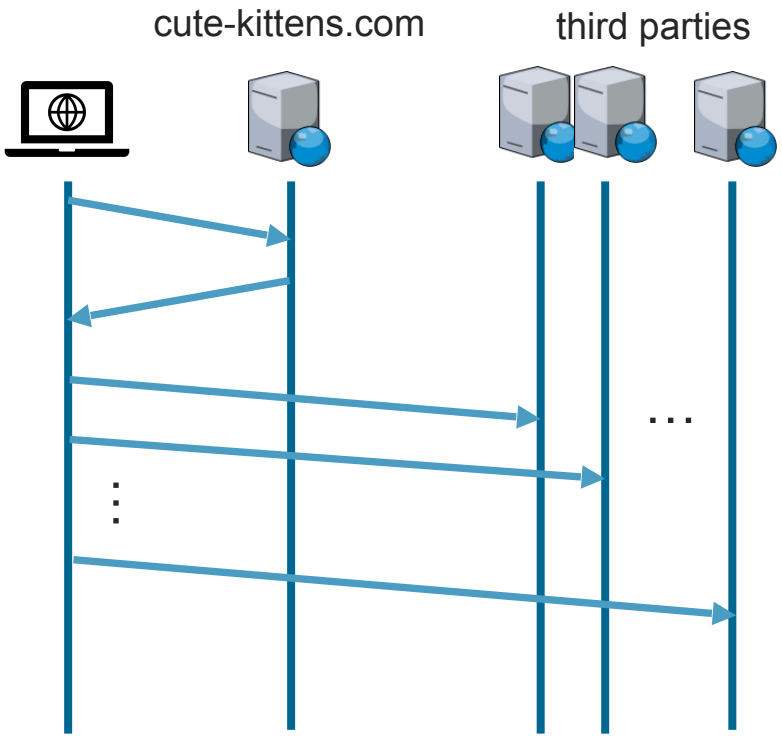


Third-party requests: implicit and ubiquitous



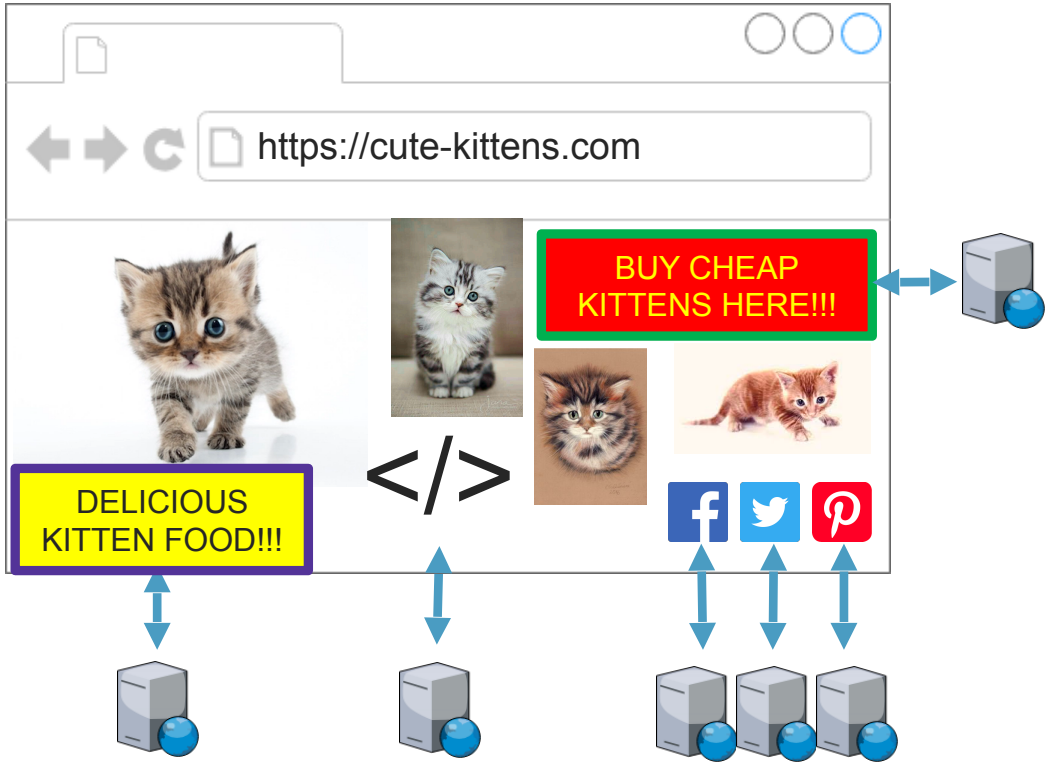
Third-party requests: implicit and ubiquitous

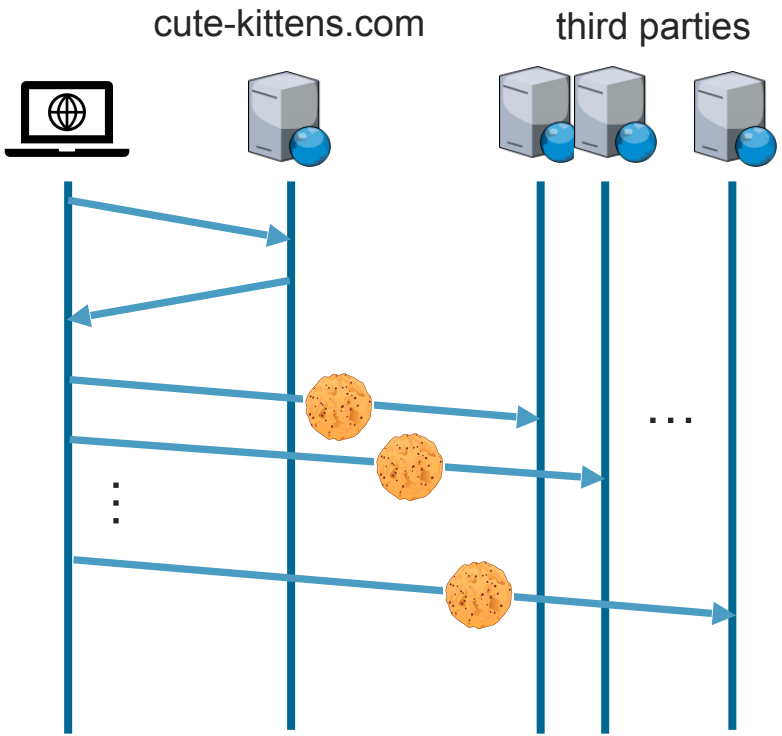




KU LEUVEN DistriNet

Third-party requests: implicit and ubiquitous





KU LEUVEN DistriNet

Cross-site attacks

Cross-site Request Forgery (CSRF)

- Authenticated state-changing request

Cross-site Request Forgery (CSRF)

- Authenticated state-changing request

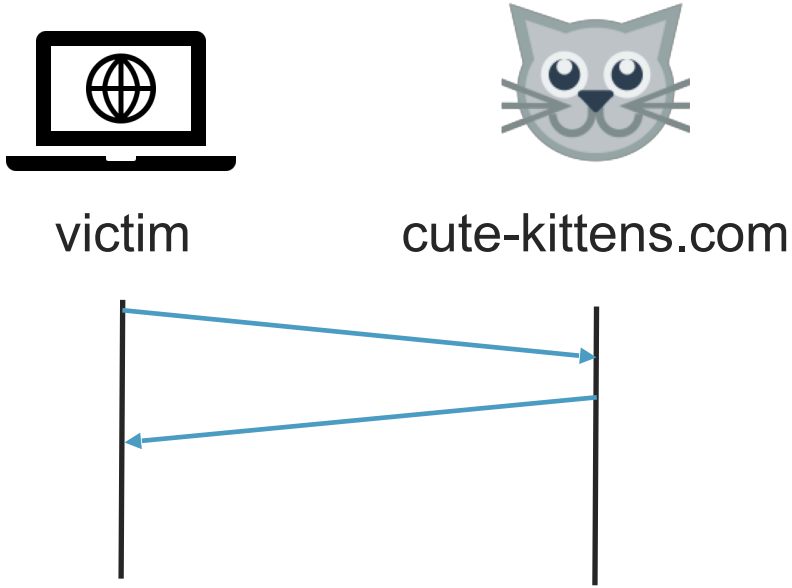
victim

cute-kittens.com

KU LEUVEN DistriNet

Cross-site Request Forgery (CSRF)

- Authenticated state-changing request

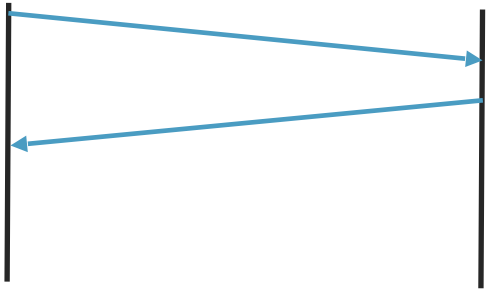


Cross-site Request Forgery (CSRF)

- Authenticated state-changing request

victim

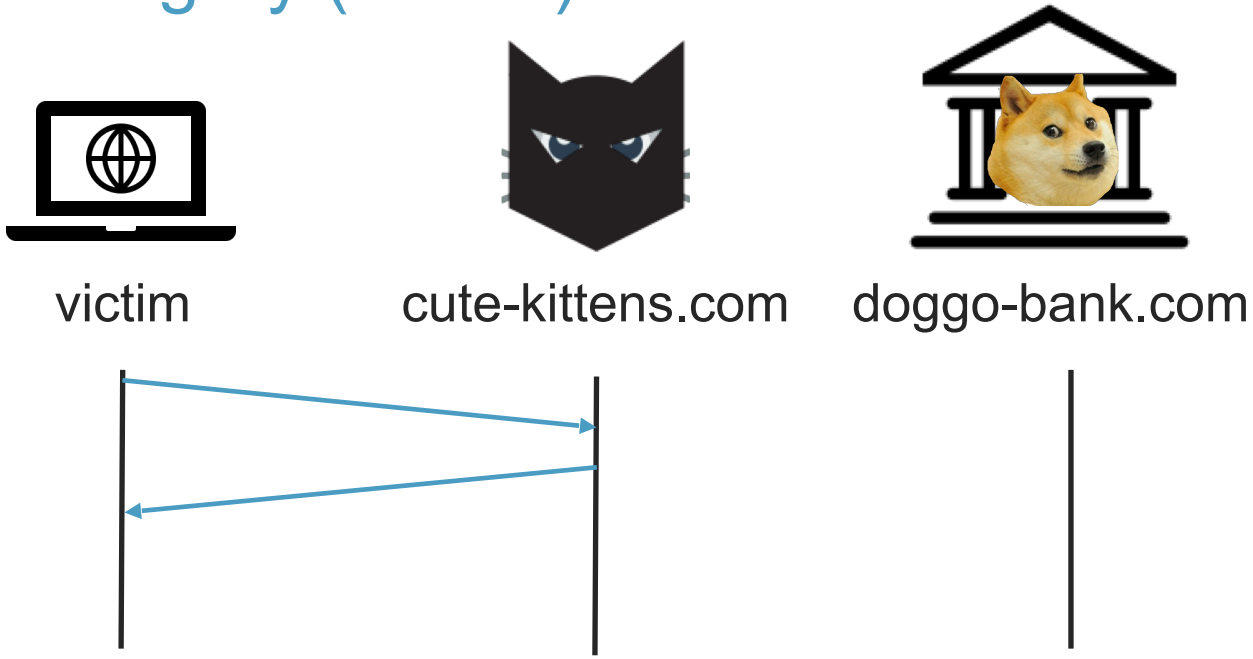
cute-kittens.com



KU LEUVEN DistriNet

Cross-site Request Forgery (CSRF)

- Authenticated state-changing request

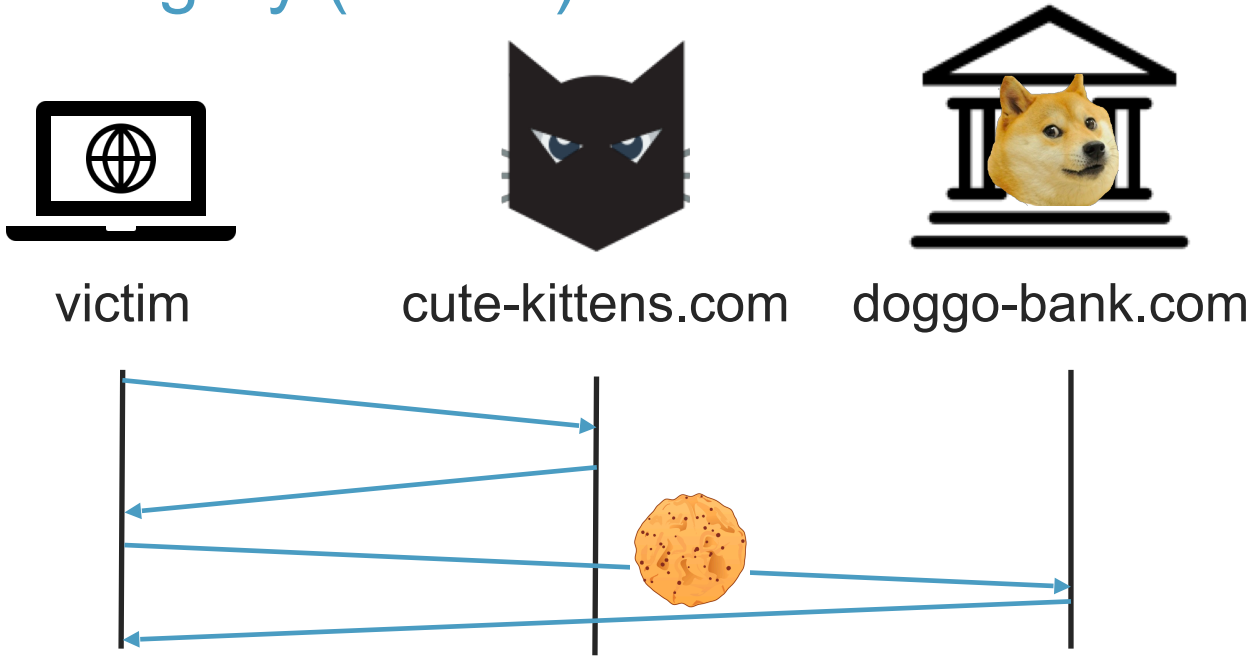



```
<img src="https://doggo-bank.com/transfer.php
      ?amount=999999&recipient=catboss">
```


KU LEUVEN DistriNet

Cross-site Request Forgery (CSRF)

- Authenticated state-changing request




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


KU LEUVEN DistriNet

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 required)

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.

By Charlie Osborne for Zero Day | August 8, 2018 -- 10:40 GMT (11:40 BST) | Topic: Security

0 | 30

The health records of millions of patients worldwide were potentially left open to attack by a slew of critical vulnerabilities uncovered by a single cybersecurity team.

OpenEMR is a popular, open-source software solution for the management of millions of electronic patient records worldwide. However, the software, until recently, also contained over 20 severe security issues.

Discovered by Project Insecurity and disclosed in a security team said the bugs included multiple

RECOMMENDED FOR YOU

Guide to Antivirus (AV) Replacement: What You Need to Know Before Replacing Your Current AV Solution

White Papers provided by CrowdStrike

DOWNLOAD NOW

MORE SECURITY NEWS

This is how government spyware StrongPity uses security researchers' work against them

Facebook approaches major cybersecurity firms, acquisition goals in mind

MORE FROM CHARLIE OSBORNE

Security

Most enterprise vulnerabilities

KU LEUVEN DistriNet

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

APPUALS
FROM THE EXPERTS!

Security

CSRF Vulnerability in phpMyAdmin 4.7.x Lets Attackers Delete Records through malicious URLs

0 Comments 1 minute read

By Zainab Imran • September 6, 2018

A Cross-Site Request Forgery (CSRF) vulnerability has been found in the phpMyAdmin version 4.7.x (before version 4.7.7) through which malicious attackers are able to perform fundamental database operations by tricking users into clicking on maliciously crafted URLs. This vulnerability has been combined under the CVE identification label CVE-2017-1000499 which was assigned to previous CSRF vulnerabilities in phpMyAdmin as well.

Follow Us
5,715 Fans
2,490 Subscribers
Trending
1 MediaTek's Helio P70 Upgr is Kind of a Disapointment
By Sikandar Mahmood 3 hours ago
2 Hitman 2 'Untouchable' T Shows off 7 Different Environments
By Farhan Ali 6 hours ago
3 "Lion. Blackbeard. Ela", Ubisoft on their Mistakes Rainbow Six Siege

ZDNet

CENTRAL EUROPE

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

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 risk management

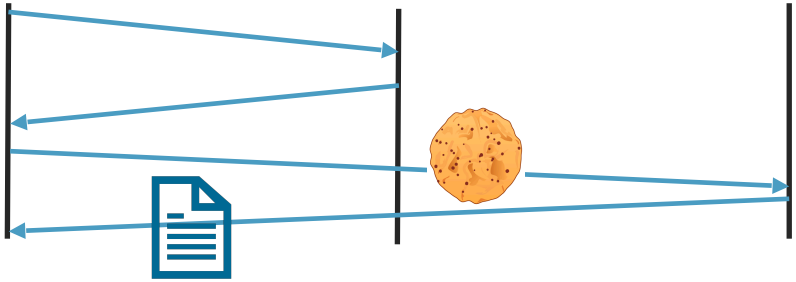
Cross-site Request Forgery

- 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 script inclusion (XSSI) [1]

Same Origin Policy:

victim cute-kittens.com doggo-bank.com



🎯Dynamically generated JavaScript

```
<script src="https://doggo-bank.com/bank-account.js">
</script>
```

[1] Lekies et al. 2015. The unexpected dangers of dynamic JavaScript. In Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15), Jaeyeon Jung (Ed.). USENIX Association, Berkeley, CA, USA, 723-735.

Cross-site script inclusion (XSSI) [1]

Examples

attacker.js

```
sendToServer(account_data);
```

bank-account.js

```
var account_data = {
    "f_name":   "John",
    "s_name":   "Doe",
    "balance":  1500,
};
```

```
JSON.stringify = function(data) {
    sendToServer(data);
}
```

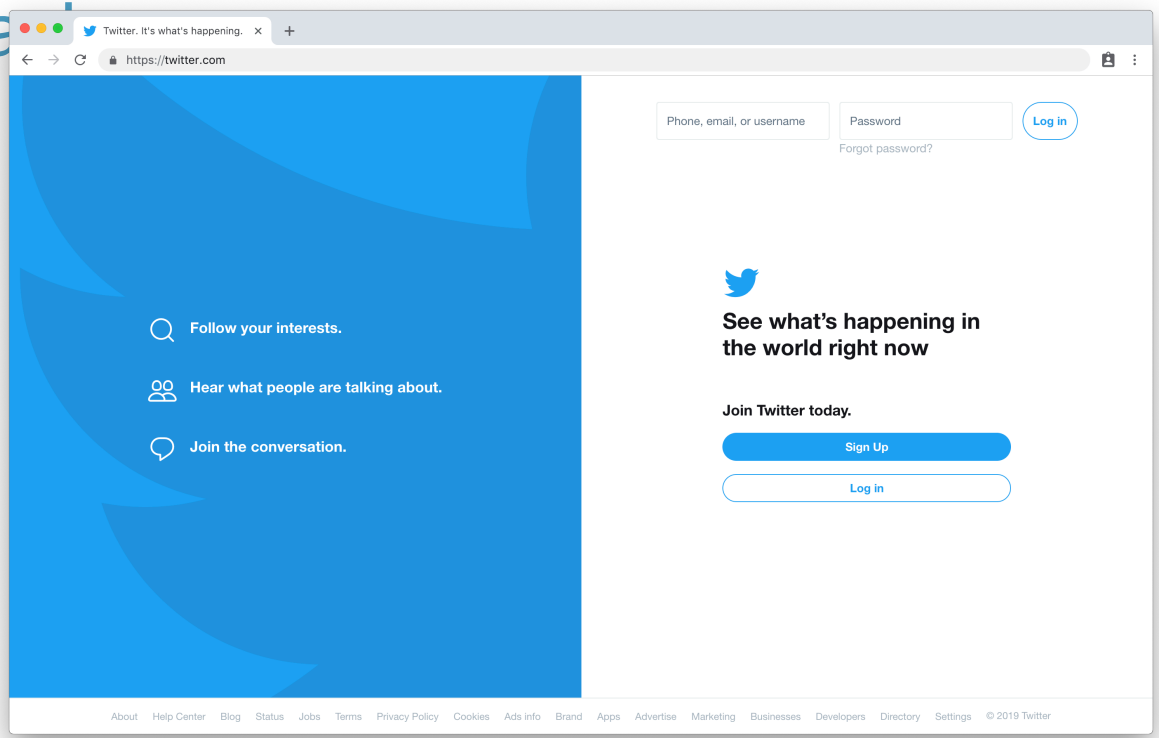
```
JSON.stringify("secret string");
```

[1] Lekies et al. 2015. The unexpected dangers of dynamic JavaScript. In Proceedings of the 24th USENIX Conference on Security Symposium (SEC'15), Jaeyeon Jung (Ed.). USENIX Association, Berkeley, CA, USA, 723-735.

XSSI defenses

- Separate sensitive data from scripts
  - Avoid using JSON with Padding (JSONP)
  - Use Cross-Origin Resource Sharing (CORS) instead
- Avoid executable JSON files
  - Unparseable or add valid JS that ends execution

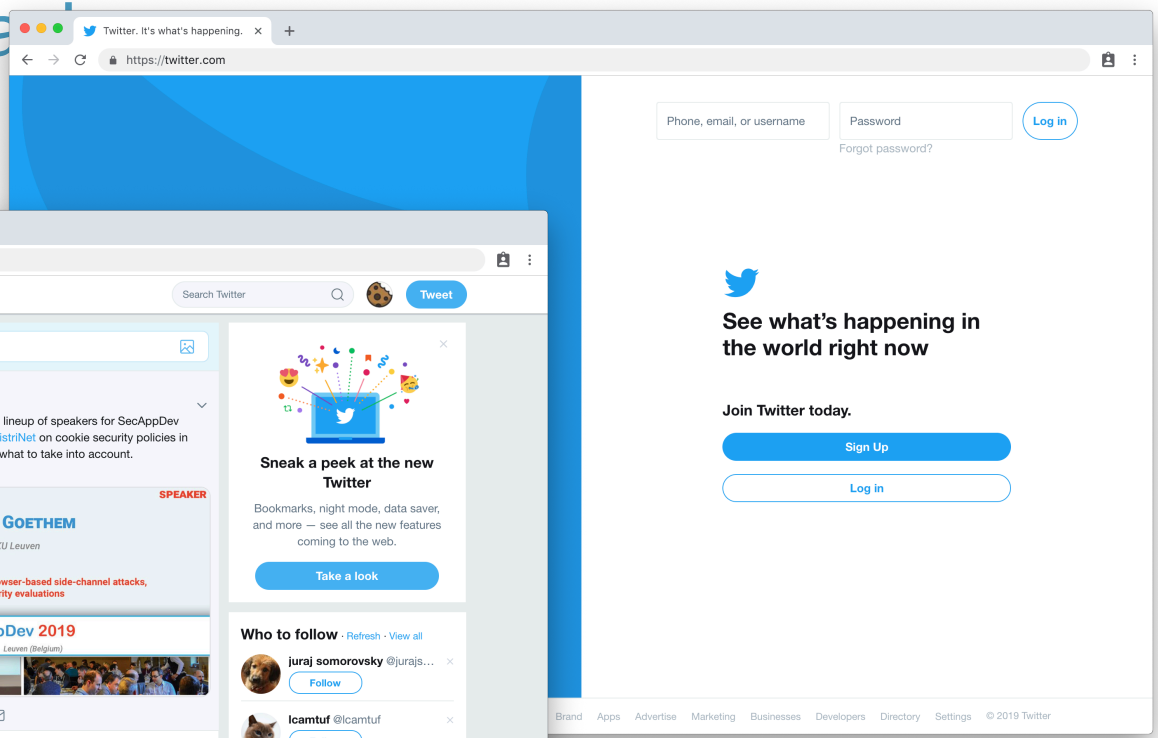
Cross-site timing attacks



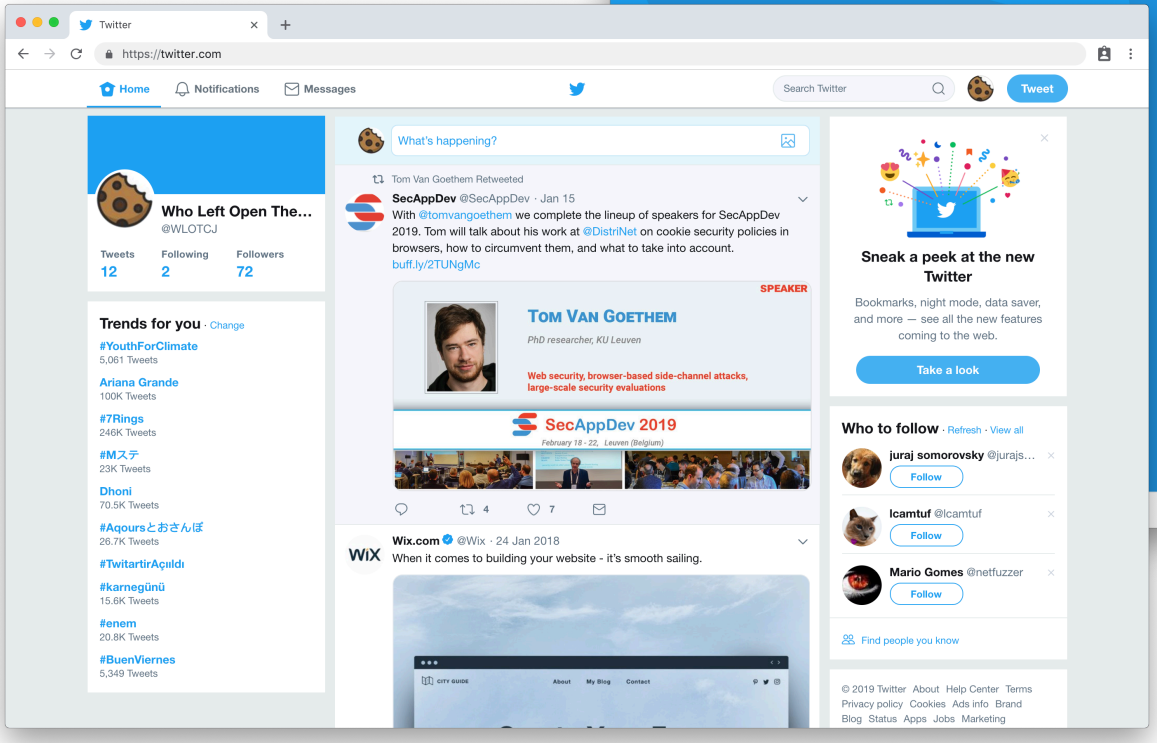
~19kB

KU LEUVEN DistriNet

Cross-site timing attacks



~19kB



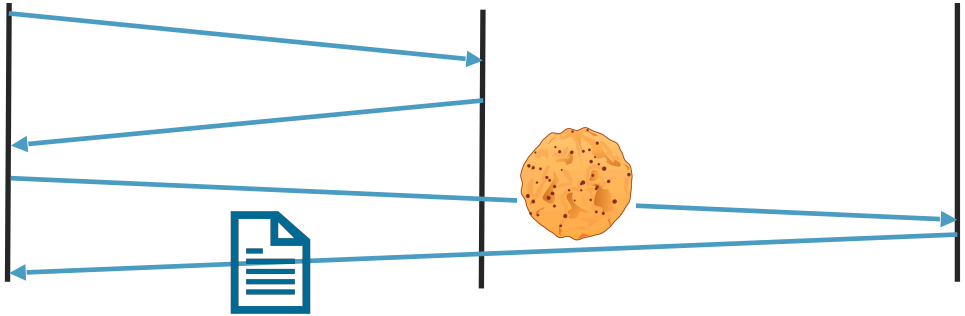
~183kB

KU LEUVEN DistriNet

Cross-site timing attacks [1]

State-dependent content

victim cute-kittens.com doggo-bank.com

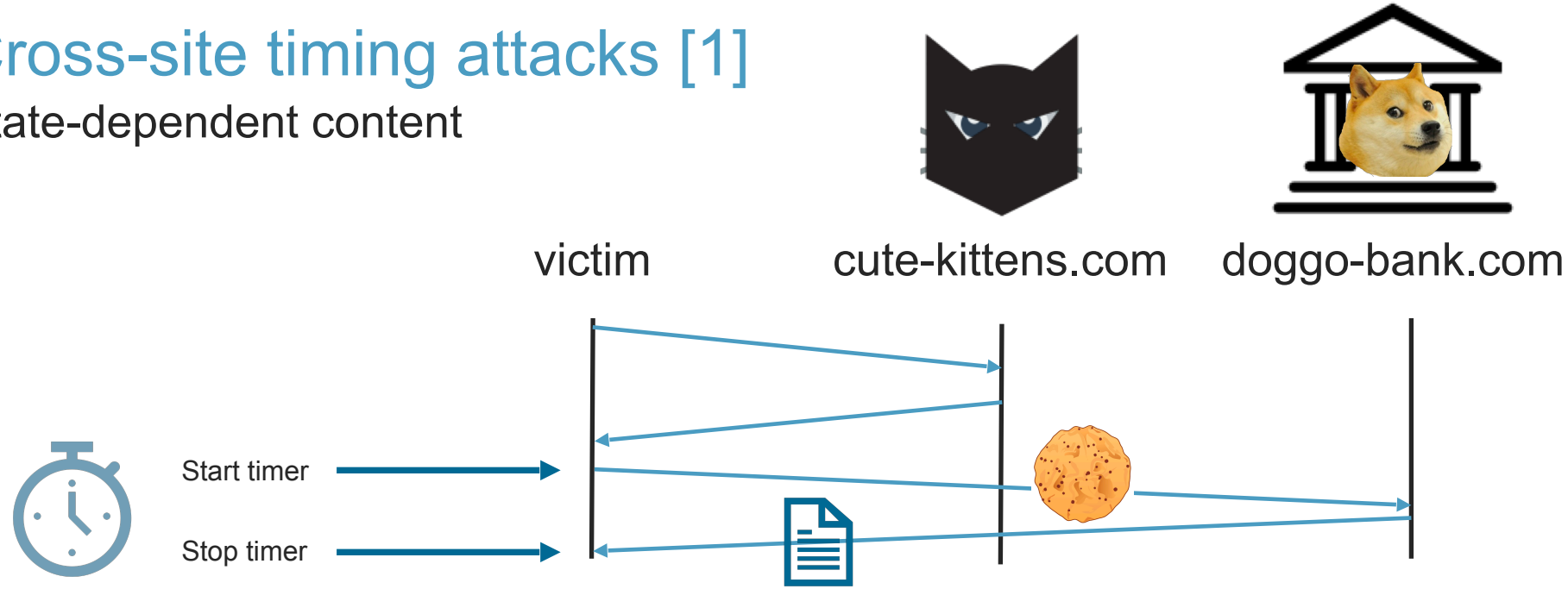


```
<img src="https://doggo-bank.com/index.hmtl">
```

[1] Bortz et al. 2007. Exposing private information by timing web applications. In Proceedings of the 16th international conference on World Wide Web (WWW '07). ACM, New York, NY, USA, 621-628.

Cross-site timing attacks [1]

State-dependent content

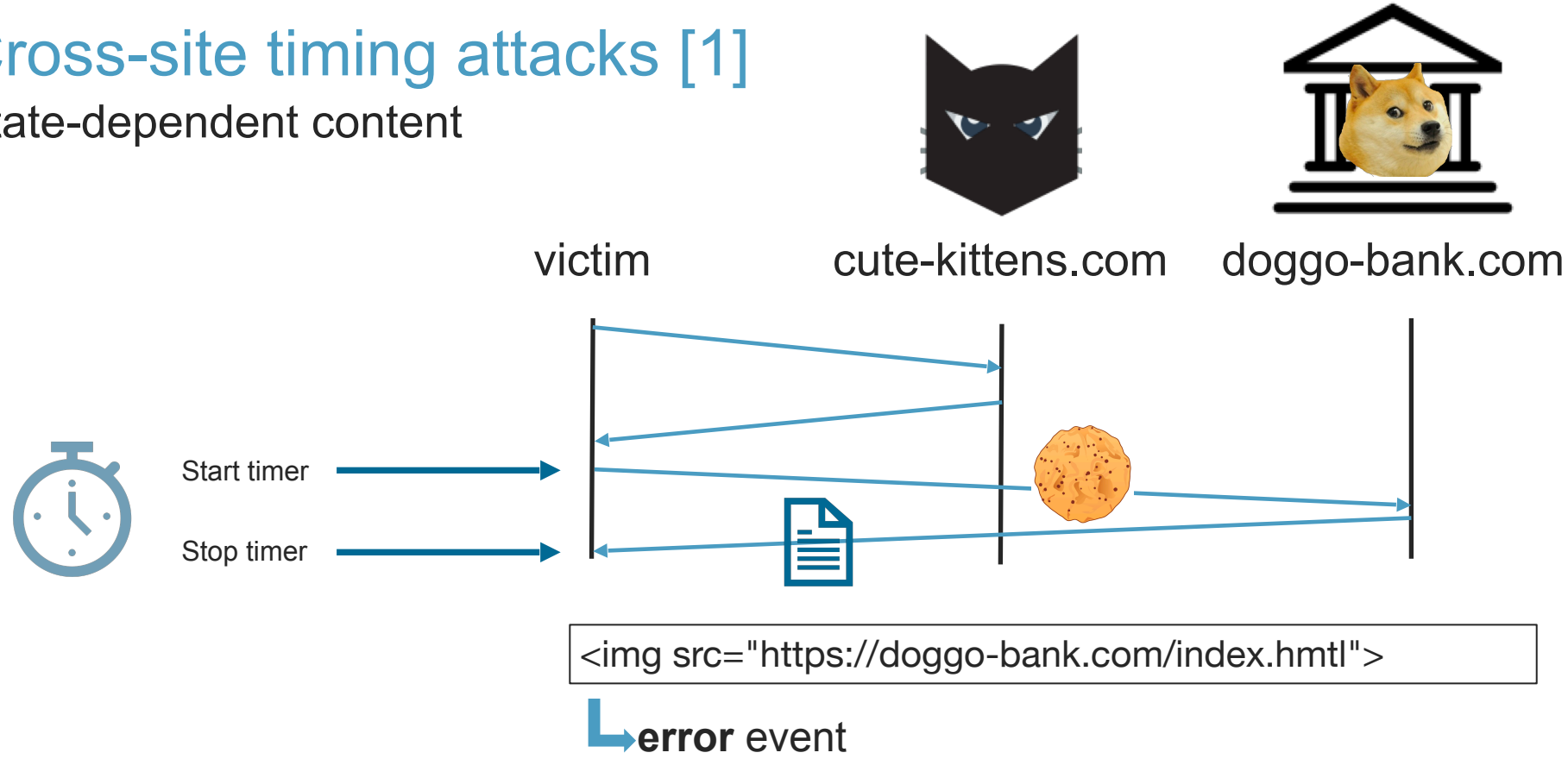



```
<img src="https://doggo-bank.com/index.hmtl">
```

[1] Bortz et al. 2007. Exposing private information by timing web applications. In Proceedings of the 16th international conference on World Wide Web (WWW '07). ACM, New York, NY, USA, 621-628.

Cross-site timing attacks [1]

State-dependent content



[1] Bortz et al. 2007. Exposing private information by timing web applications. In Proceedings of the 16th international conference on World Wide Web (WWW '07). ACM, New York, NY, USA, 621-628.

KU LEUVEN DistriNet

Cross-site timing attacks [1]

State-dependent content

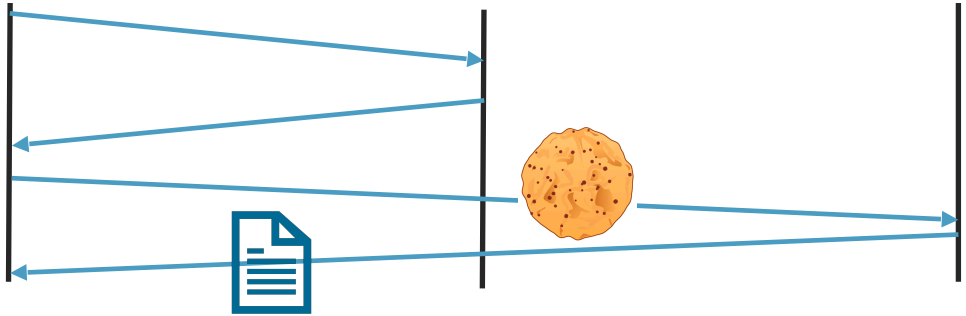
→ Logged in or not?

→ #items in online basket

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

Start timer

Stop timer




```
<img src="https://doggo-bank.com/index.hmtl">
```

error event

[1] Bortz et al. 2007. Exposing private information by timing web applications. In Proceedings of the 16th international conference on World Wide Web (WWW '07). ACM, New York, NY, USA, 621-628.

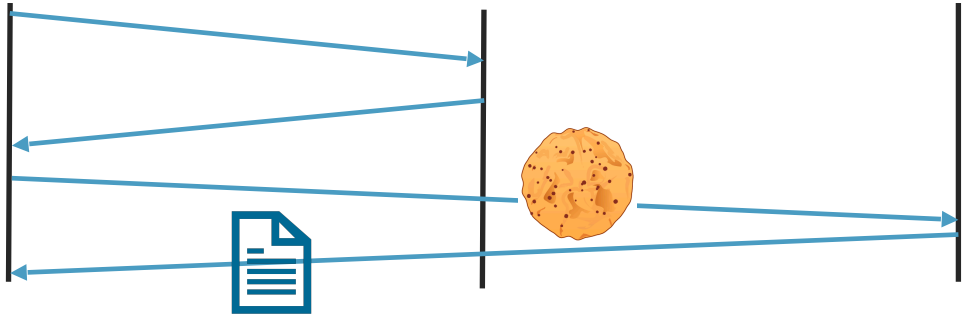
Cross-site timing attacks [1]

State-dependent content

victim cute-kittens.com doggo-bank.com

Start timer

Stop timer

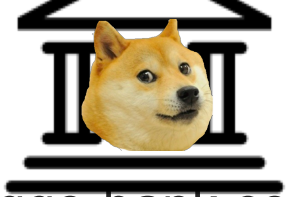



```
<img src="https://doggo-bank.com/index.hmtl">
```

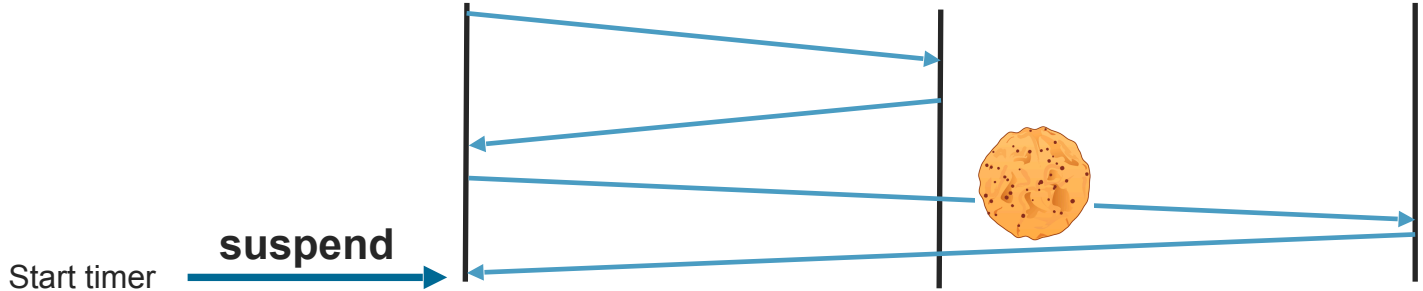
↳ **error** event

[1] Bortz et al. 2007. Exposing private information by timing web applications. In Proceedings of the 16th international conference on World Wide Web (WWW '07). ACM, New York, NY, USA, 621-628.

Browser-based timing attacks [1]



victim cute-kittens.com doggo-bank.com



<video src="https://doggo-bank.com/index.hmtl">

error
Stop timer

→ Abuse of firing events during parsing process
- **suspend** when fetched
- **error** on fail

[1] Van Goethem et al. The Clock is Still Ticking: Timing Attacks in the Modern Web. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS '15). ACM, New York, NY, USA, 1382-1393.

KU LEUVEN DistriNet


CROSS-SITE ATTACKS
LIGHTYEAR
CROSS-SITE ATTACKS EVERYWHERE

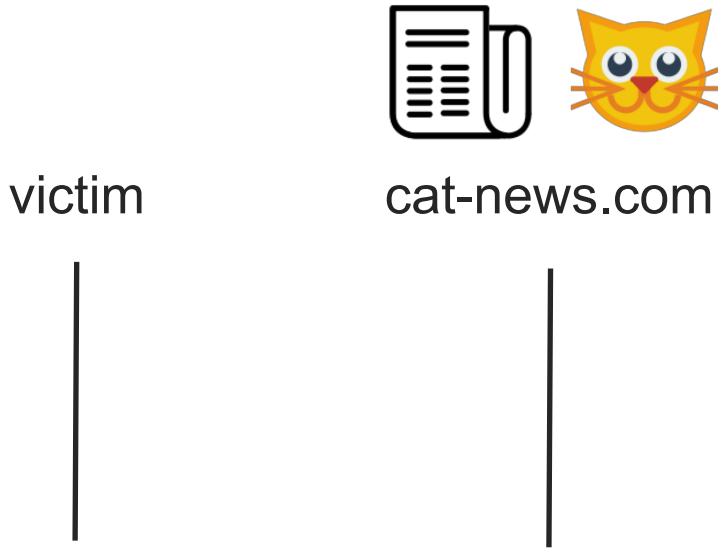
Cross-site attacks everywhere

- HEIST (HTTP Encrypted Information can be Stolen through TCP-windows)
  - Leverages Fetch API + Resource Timing API to apply compression-based attack (BREACH) to leak secrets, such as CSRF token
- Measure cross-origin response size through Cache API
- Use Quota Management API & Storage API to find exact response size
- XS-Search (response inflation, computation inflation)
  - E.g. attack against Google's bug tracker (Monorail) to find undisclosed vulnerabilities (uses XS-Search + Cache API attacks) [1]

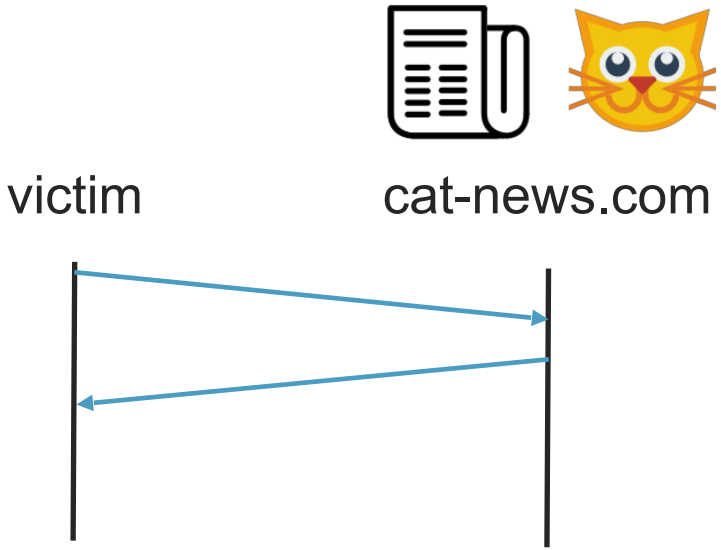
[1] https://medium.com/@luanherrera/xs-searching-googles-bug-tracker-to-find-out-vulnerable-source-code-50d8135b7549

Third-party tracking

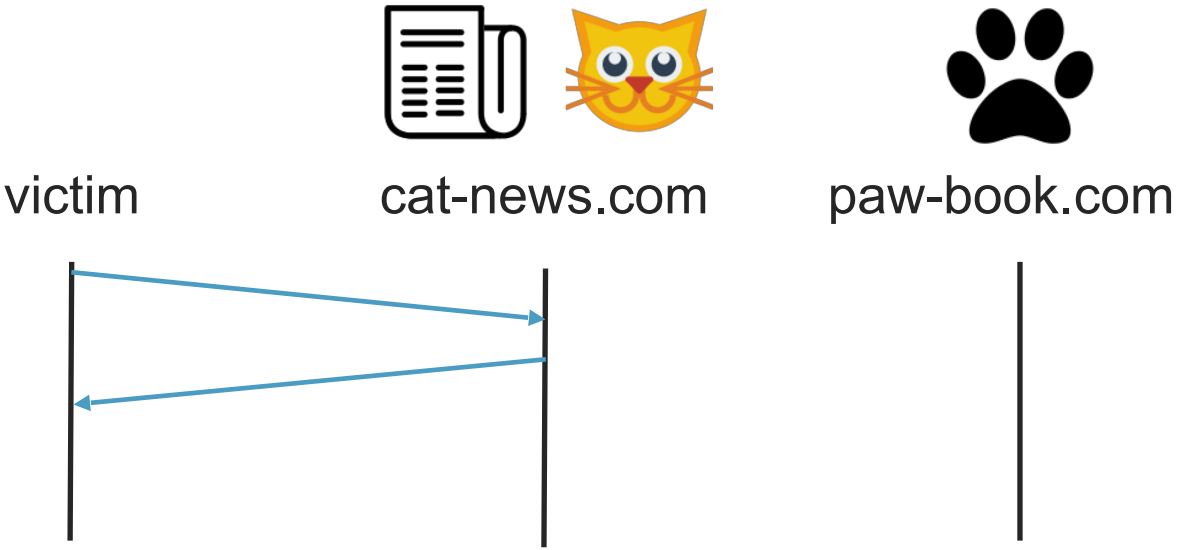
Third-party Tracking



Third-party Tracking

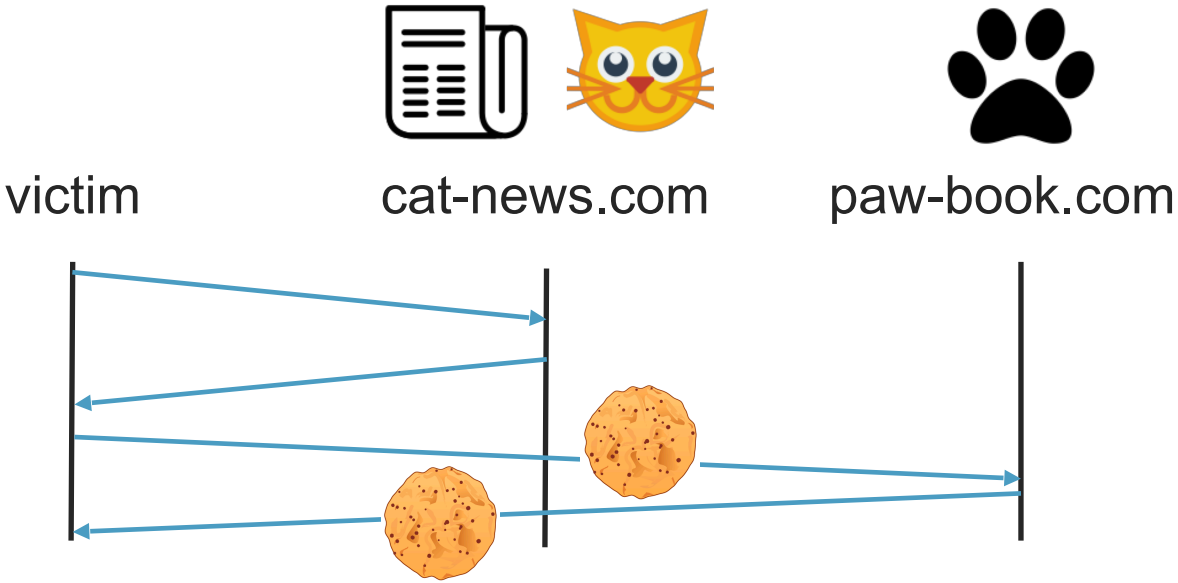


Third-party Tracking




```
<script src="https://paw-book.com/widget.js
      ?url=cat-news.com/catnip.html"></script>
```

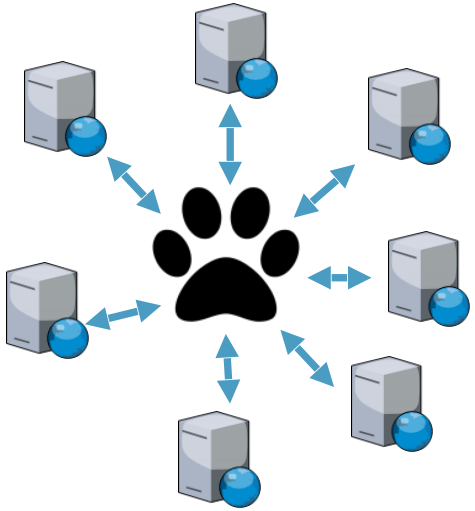
Third-party Tracking

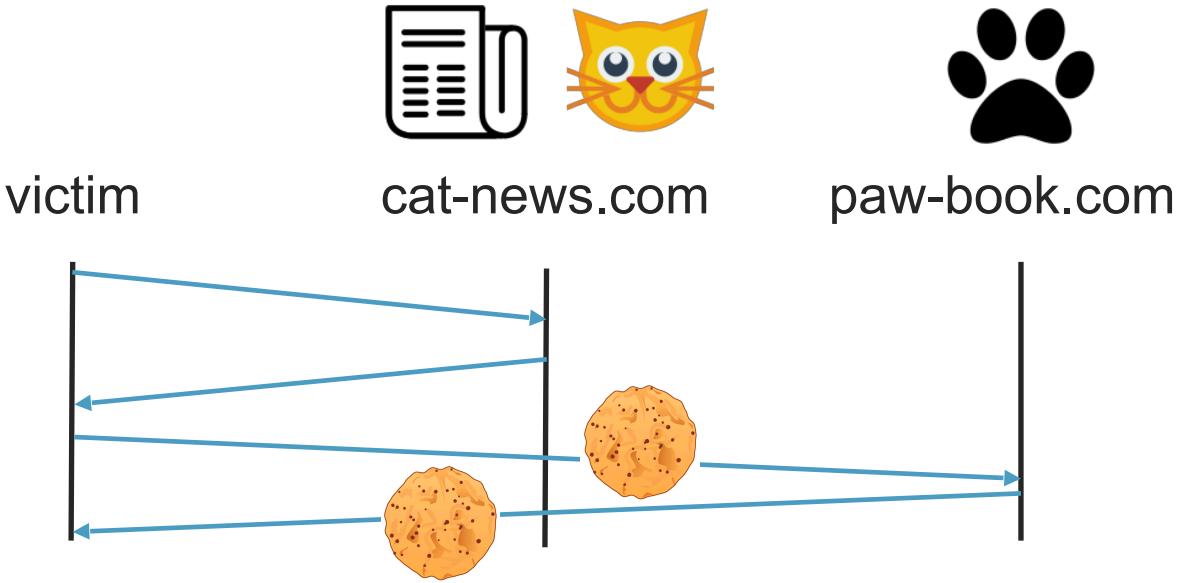



```
<script src="https://paw-book.com/widget.js
      ?url=cat-news.com/catnip.html"></script>
```


KU LEUVEN DistriNet

Third-party Tracking

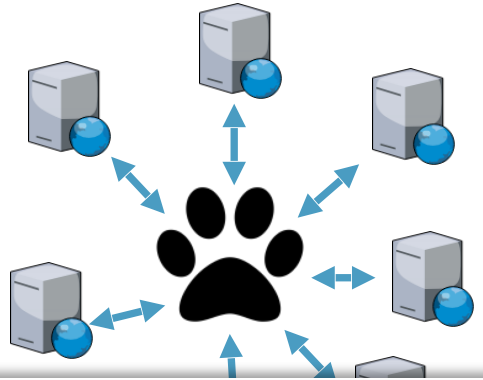


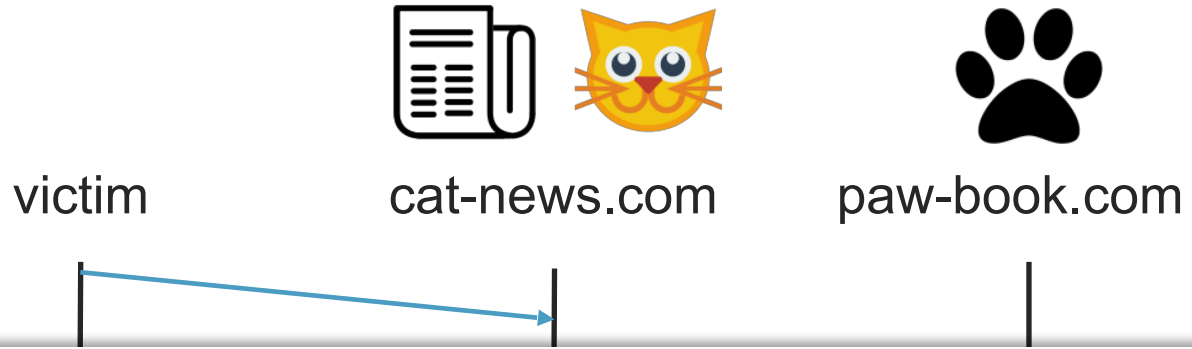


- Aggregate unique browsing profiles

```
<script src="https://paw-book.com/widget.js
      ?url=cat-news.com/catnip.html"></script>
```

Third-party Tracking





Tracking the Trackers

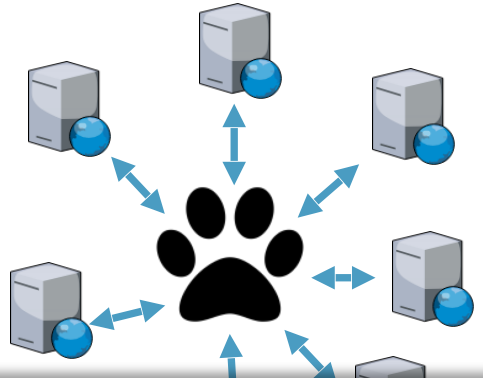
Zhonghao Yu
Cliqz
Arabellastraße 23
Munich, Germany
zhonghao@cliqz.com

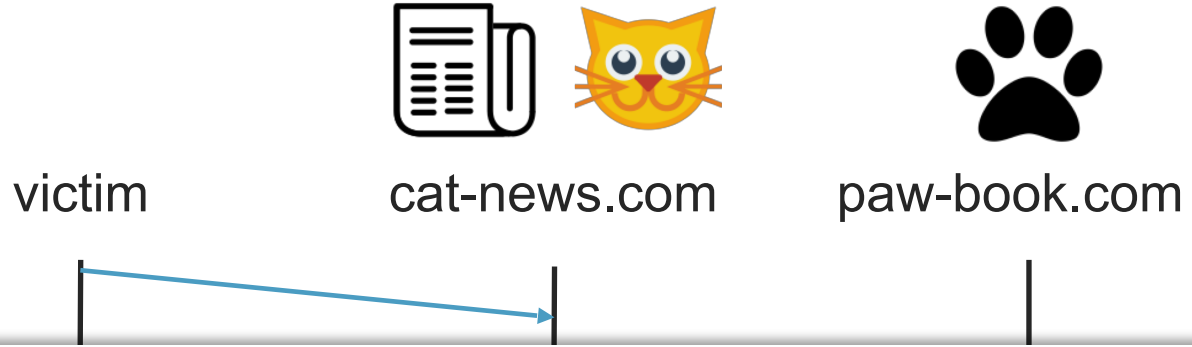
Sam Macbeth
Cliqz
Arabellastraße 23
Munich, Germany
sam@cliqz.com

Konark Modi
Cliqz
Arabellastraße 23
Munich, Germany
konarkm@cliqz.com

Josep M. Pujol
Cliqz
Arabellastraße 23

Third-party Tracking





Tracking the Trackers

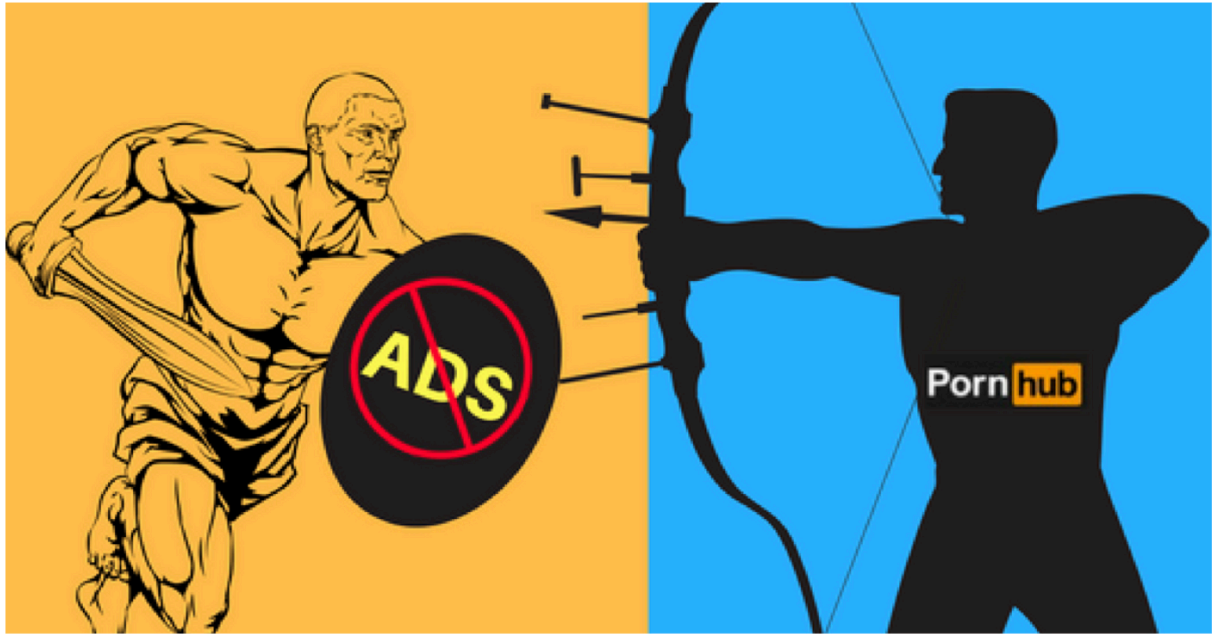
Zhonghao Yu Sam Macbeth Konark Modi

"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

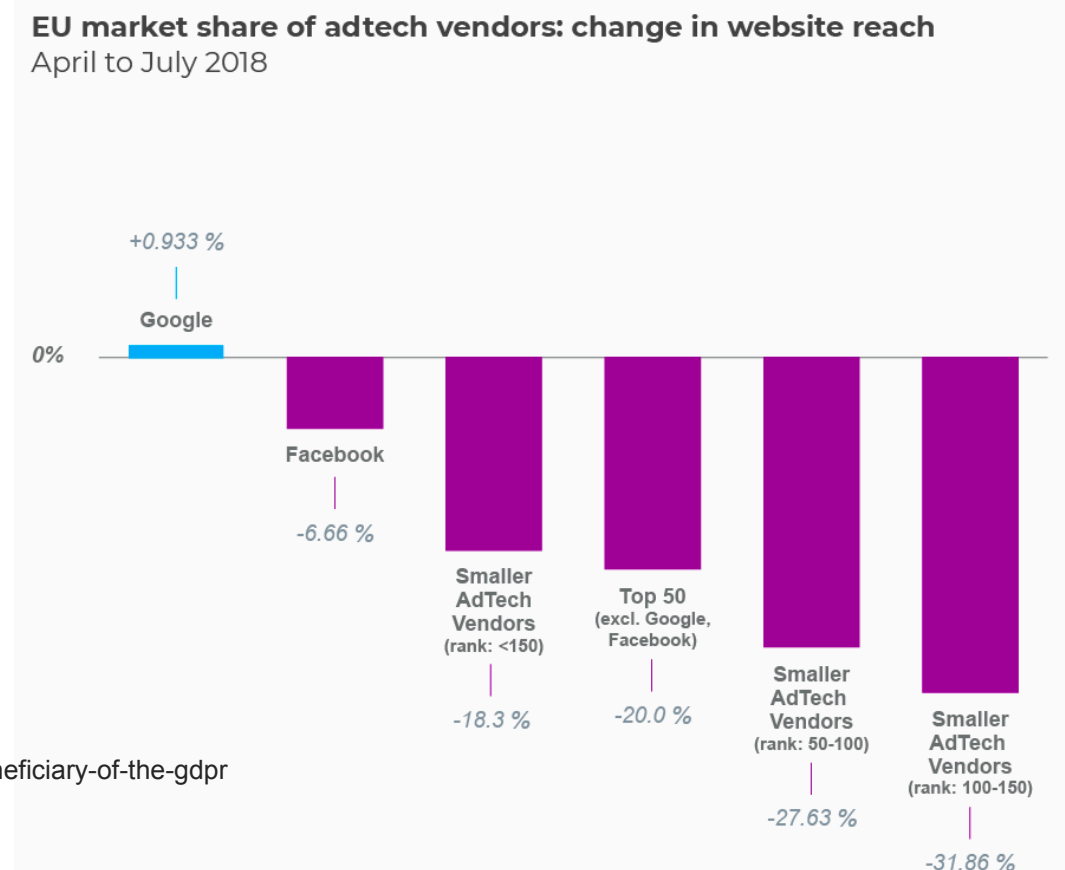
BugReplay Follow
Nov 1, 2016 · 4 min read



Juridical perspective: GDPR

Joint study by Cliqz and Ghostery [1]

- Average number of trackers per website decreased
- Most advertisers lost reach
- Google slightly gained reach



[1] https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr

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

KU LEUVEN DistriNet

How do the more advanced policies work?

- Block cross-site requests/cookies, based on:
  - Blacklists (e.g. EasyList)
    - Publicly available
    - Systematically updated
  - Machine learning (e.g. Safari)
    - Based on browsing behavior

```
&action=js_stats&
&callback=hitStats_
&ctxId=*&pubId=*&clientDT=
&ctxId=*&pubId=*&objId=
&event=view&
&funnel_state=
&http_referer=$script
&pageReferrer=
&ref=*&tag=
&refer=http$script
&refererPageDetail=
&trackingserver=
-action/fingerprint?
-action/ping?
-ads-tracking-
-AdTracking.
-analitycs//fab.
-analitycs//ga.
-analitycs//metrica.
-analitycs/fab.
-analitycs/ga.
-analitycs/metrica.
-analytics-tagserver-
-analytics-wi.
-analytics/insight.
-appanalytics-
-asset-tag.
-audience-science-pixel/
-baynote.
```

Same-site cookie [1] (= defense for security)

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

KU LEUVEN DistriNet

Use of same-site cookies

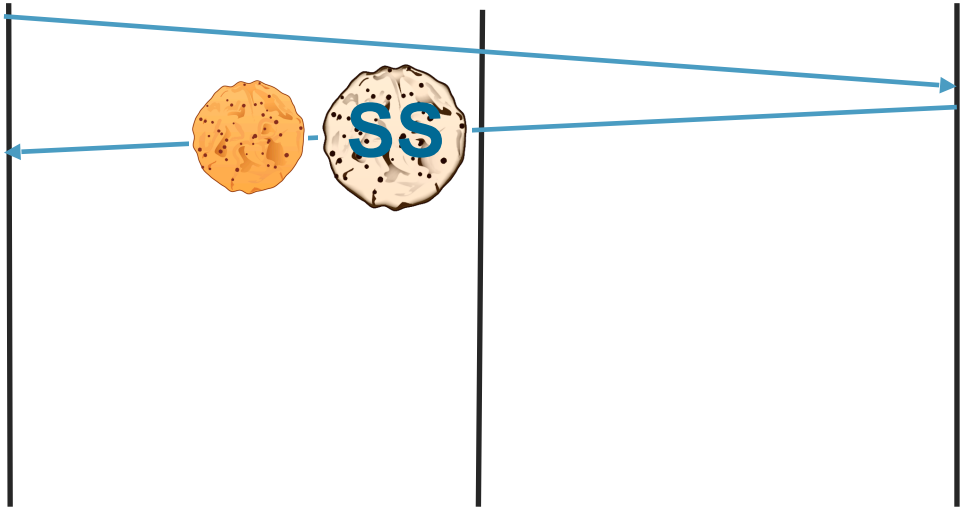
against cross-site attacks

doggo-bank.com

victim

cute-kittens.com

doggo-bank.com



Set-Cookie: auth=ekSd2lksq090pQDs; SameSite=strict

KU LEUVEN DistriNet

Use of same-site cookies

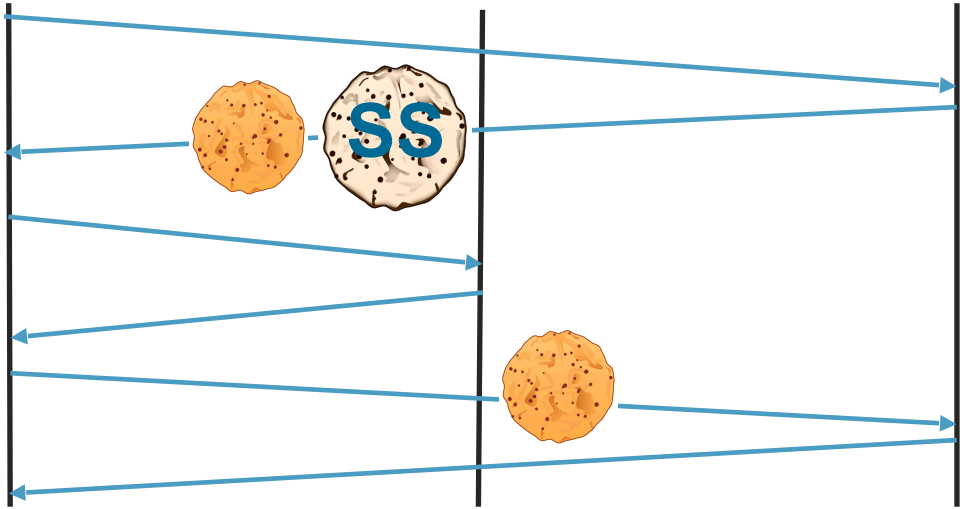
against cross-site attacks

doggo-bank.com

victim

cute-kittens.com

doggo-bank.com



Set-Cookie: auth=ekSd2lksq090pQDs; SameSite=strict

KU LEUVEN DistriNet

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

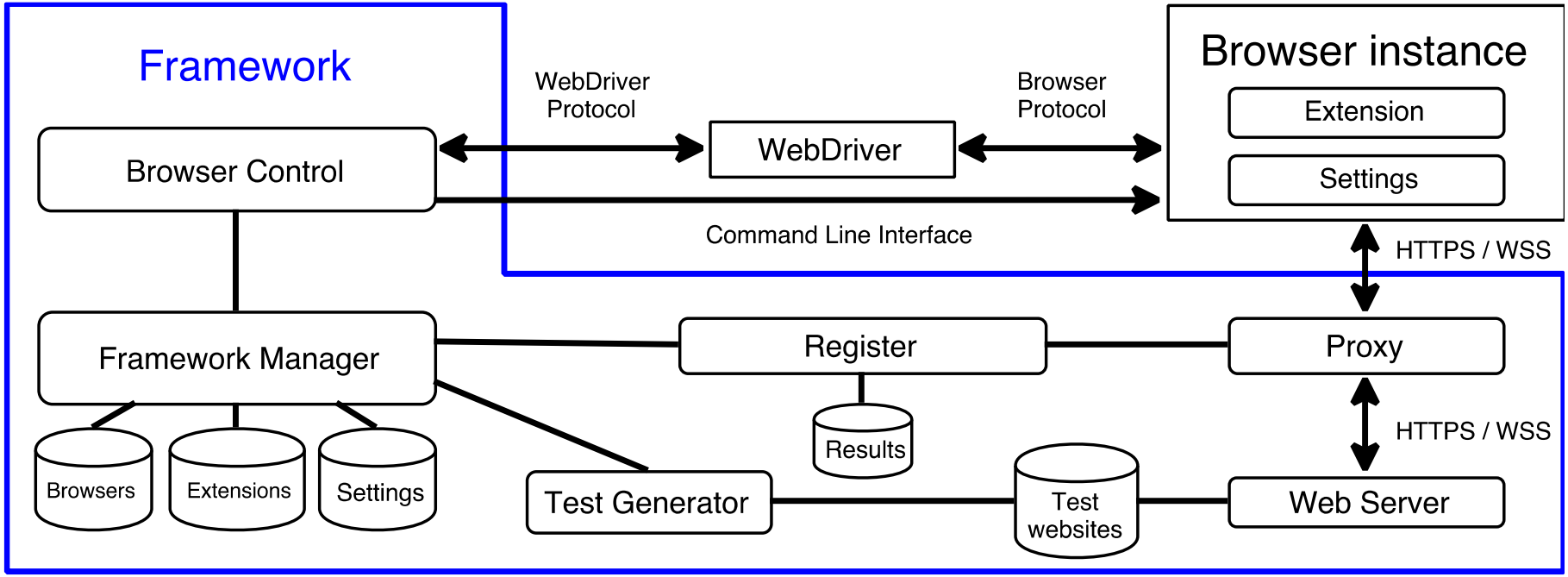
Black box approach

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

KU LEUVEN DistriNet

Framework

Design



KU LEUVEN DistriNet

Inside the framework

- Browser control
  - Selenium / Command line interface
- Web server
  - Initiate cross-site requests to blacklisted domain
  - Proxy intercepts all requests

KU LEUVEN DistriNet

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

KU LEUVEN DistriNet

Overview

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

		AppCache	HTML	Headers	Redirect	PDF JS	JavaScript	SW
Chrome	SET A1 (3/14)	●	●	●	●	●	●	●
	SET A2 (3/14)	●	○	◐	●	●	●	●
	SET A3 (1/14)	●	○	○	●	●	●	●
	SET A4 (1/14)	●	○	○	●	●	○	●
	SET A5 (1/14)	●	○	○	○	●	●	●
	SET A6 (3/14)	●	○	○	○	●	○	●
	SET A7 (2/14)	○	○	○	●	●	○	○
Opera	SET A8 (2/9)	●	●	●	●	●	●	●
	SET A9 (1/9)	●	○	◐	●	●	●	●
	SET A10 (2/9)	●	○	○	●	●	●	●
	SET A11 (1/9)	●	○	○	●	●	○	●
	SET A12 (1/9)	●	○	○	○	●	●	●
	SET A13 (1/9)	●	○	○	○	●	○	●
	SET A14 (1/9)	○	○	○	●	●	○	○
Firefox	SET A15 (2/5)	●	●	◐	●	○	●	○
	SET A16 (1/5)	●	●	○	●	○	○	○
	SET A17 (1/5)	●	●	○	○	○	○	○
	SET A18 (1/5)	○	●	○	●	○	○	○
Edge	SET A19 (1/4)	●	●	◐	●	○	●	N/A
	SET A20 (1/4)	●	○	○	●	○	●	N/A
	SET A21 (1/4)	○	●	○	●	○	●	N/A
	SET A22 (1/4)	○	○	○	●	○	●	N/A

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

KU LEUVEN DistriNet

		AppCache	HTML	Headers	Redirect	PDF JS	JavaScript	SW
Chrome	SET A1 (3/14)	●						
	SET A2 (3/14)	●						
	SET A3 (1/14)	●						
	SET A4 (1/14)	●						
	SET A5 (1/14)	●						
	SET A6 (3/14)	●						
	SET A7 (2/14)	○						
Opera	SET A8 (2/9)	●						
	SET A9 (1/9)	●						
	SET A10 (2/9)	●						
	SET A11 (1/9)	●						
	SET A12 (1/9)	●						
	SET A13 (1/9)	●						
	SET A14 (1/9)	○						
Firefox	SET A15 (2/5)	●						
	SET A16 (1/5)	●						
	SET A17 (1/5)	●						
	SET A18 (1/5)	○						
Edge	SET A19 (1/4)	●						
	SET A20 (1/4)	●						
	SET A21 (1/4)	○						
	SET A22 (1/4)	○						

```
<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).

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

KU LEUVEN DistriNet

		AppCache	HTML	Headers	Redirect	PDF JS	JavaScript	SW
Chrome	SET A1 (3/14)	●	●	●	●	●	●	●
	SET A2 (3/14)	●	○	◐	●	●	●	●
	SET A3 (1/14)	●	○	○	●	●	●	●
	SET A4 (1/14)							●
	SET A5 (1/14)							●
	SET A6 (3/14)						○	●
	SET A7 (2/14)						○	○
Opera	SET A8 (2/9)					●		●
	SET A9 (1/9)					●		●
	SET A10 (2/9)							●
	SET A11 (1/9)							●
	SET A12 (1/9)					●	●	●
	SET A13 (1/9)					●	○	●
	SET A14 (1/9)				●	●	○	○
Firefox	SET A15 (2/5)						●	○
	SET A16 (1/5)							○
	SET A17 (1/5)							○
	SET A18 (1/5)						○	○
Edge	SET A19 (1/4)	●	●	◐	●	○	●	N/A
	SET A20 (1/4)	●	○	○	●	○	●	N/A
	SET A21 (1/4)	○	●	○	●	○	●	N/A
	SET A22 (1/4)	○	○	○	●	○	●	N/A

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

Local Service Worker
- Fetch
- XHR
- SendBeacon
- EventSource
- …

tabId == -1

tabId >= 0

KU LEUVEN DistriNet

		AppCache	HTML	Headers	Redirect	PDF JS	JavaScript	SW
Chrome	SET A1 (3/14)	●	●	●	●	●	●	●
	SET A2 (3/14)	●	○	◐	●	●	●	●
	SET A3 (1/14)	●	○	○	●	●	●	●
	SET A4 (1/14)	●	○	○	●	●	○	●
	SET A5 (1/14)	●	○	○	○	●	●	●
	SET A6 (3/14)	●	○	○	○	●	○	●
	SET A7 (2/14)	○	○					
Opera	SET A8 (2/9)	●	●					
	SET A9 (1/9)	●	○	◐	●	●	●	●
	SET A10 (2/9)	●	○	○	●	●	●	●
	SET A11 (1/9)	●	○	○	●	●	○	●
	SET A12 (1/9)	●	○	○	○	●	●	●
	SET A13 (1/9)	●	○	○	○	●	○	●
	SET A14 (1/9)	○	○	○	○	○	○	○
Firefox	SET A15 (2/5)	●	●	◐	○	○	○	○
	SET A16 (1/5)	●	●	○	○	○	○	○
	SET A17 (1/5)	●	●	○	○	○	○	○
	SET A18 (1/5)	○	●	○	○	○	○	○
Edge	SET A19 (1/4)	●	●	◐	●	○	●	N/A
	SET A20 (1/4)	●	○	○	●	○	●	N/A
	SET A21 (1/4)	○	●	○	●	○	●	N/A
	SET A22 (1/4)	○	○	○	●	○	●	N/A

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

<link rel="shortcut icon" href="https://tracker.com/?url=example.com" />

Fetching of favicon
- was already reported
- now FIXED

KU LEUVEN DistriNet

		AppCache	HTML	Headers	Redirect	PDF JS	JavaScript	SW
Chrome	SET A1 (3/14)	◐	◐	◐	◐	●	◐	◐
	SET A2 (3/14)	◐	○	◐	◐	●	◐	◐
	SET A3 (1/14)	◐	○	○	◐	●	◐	◐
	SET A4 (1/14)	◐	○	○	◐	●	○	◐
	SET A5 (1/14)	◐	○	○	○	●	◐	◐
	SET A6 (3/14)	◐	○	○	○	●	○	◐
	SET A7 (2/14)	○	○	○	◐	●	○	○
Opera	SET A8 (2/9)	◐	◐	◐	◐	●	◐	◐
	SET A9 (1/9)	◐	○	◐	◐	●	◐	◐
	SET A10 (2/9)	◐	○	○	◐	●	◐	◐
	SET A11 (1/9)	◐	○	○	◐	●	○	◐
	SET A12 (1/9)	◐	○	○	○	●	◐	◐
	SET A13 (1/9)	◐	○	○	○	●	○	◐
	SET A14 (1/9)	○	○	○	◐	●	○	○
Firefox	SET A15 (2/5)	◐	◐	◐	◐	○	◐	○
	SET A16 (1/5)	◐	◐	○	◐	○	○	○
	SET A17 (1/5)	◐	◐	○	○	○	○	○
	SET A18 (1/5)	○	◐	○	◐	○	○	○
Edge	SET A19 (1/4)	◐	◐	◐	◐	○	◐	N/A
	SET A20 (1/4)	◐	○	○	◐	○	◐	N/A
	SET A21 (1/4)	○	◐	○	◐	○	◐	N/A
	SET A22 (1/4)	○	○	○	◐	○	◐	N/A

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

KU LEUVEN DistriNet

PDFium design flaw

Chrome and Opera

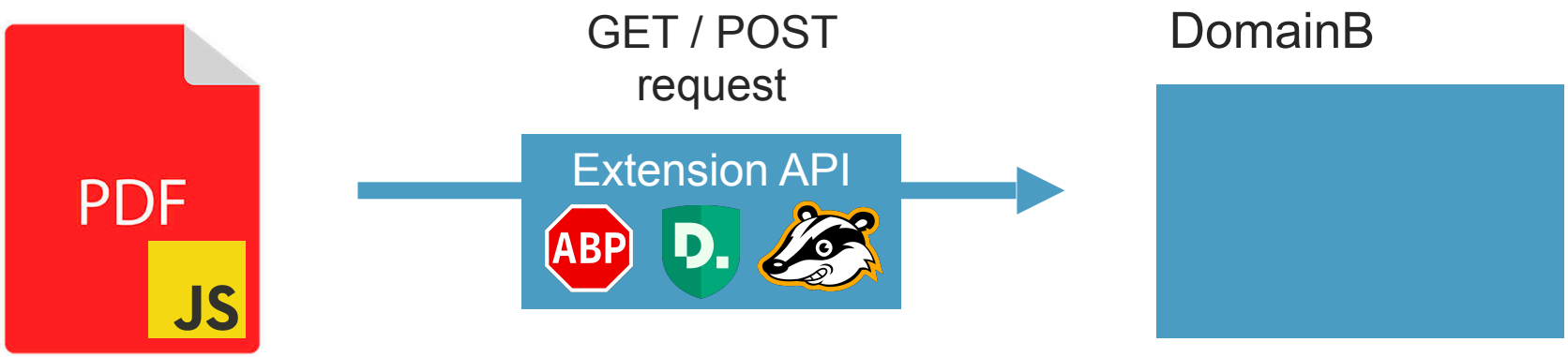
GET / POST
request

DomainB

KU LEUVEN DistriNet

PDFium design flaw

Chrome and Opera



PDFium design flaw

Chrome and Opera

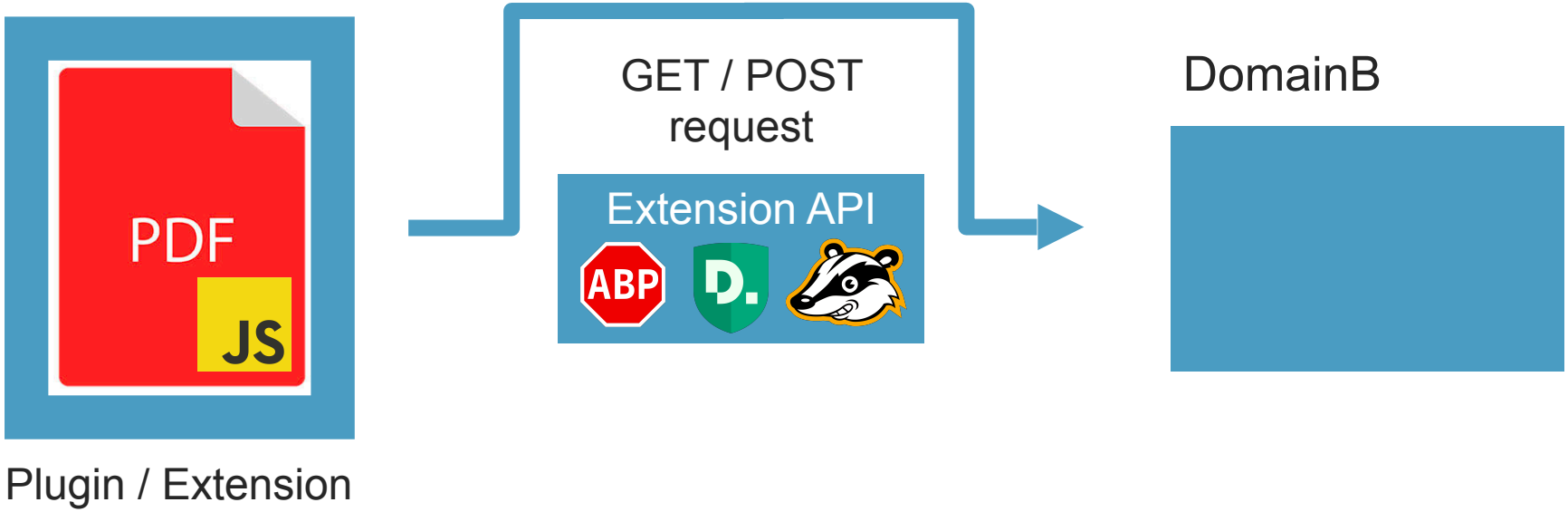
Plugin / Extension

GET / POST request

DomainB

PDFium design flaw

Chrome and Opera



PDFium design flaw

Chrome and Opera

Plugin / Extension

GET / POST request

Extension API

Block third-party cookie option

DomainB

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

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

Exploitation of a bypass

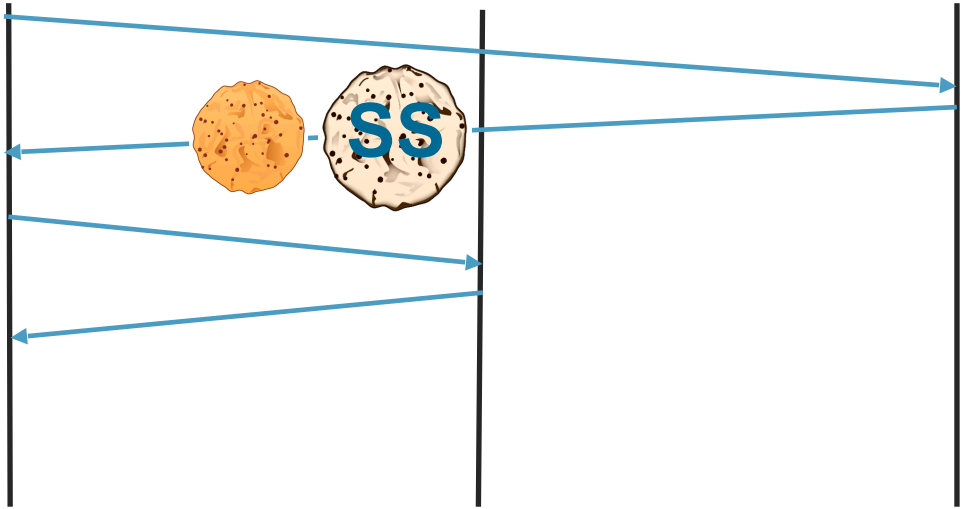
Same-site cookies

bank.com

victim

cute-kittens.com

doggo-bank.com



Exploitation of a bypass

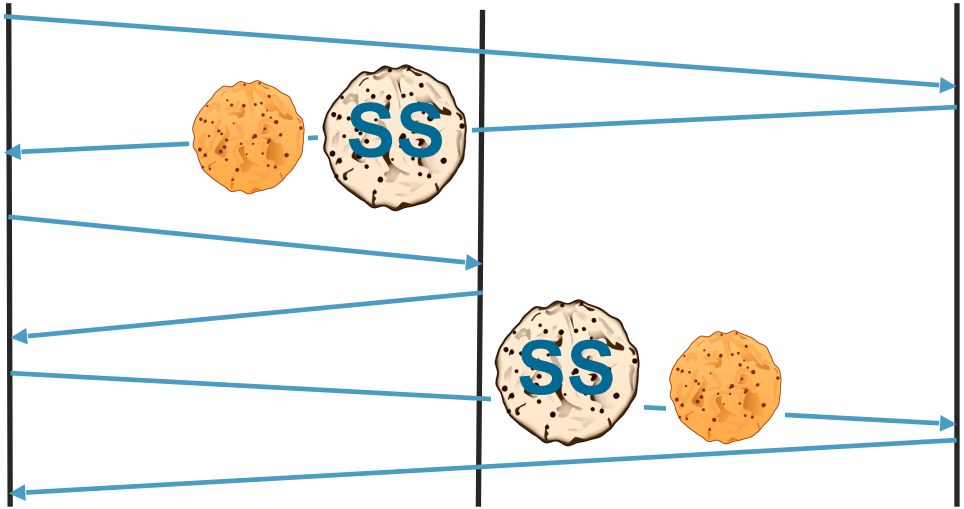
Same-site cookies

bank.com

victim

cute-kittens.com

doggo-bank.com




```
<link rel="prerender" href="https://bank.com/transfer.php
      ?amount=999999&recipient=attacker" />
```

KU LEUVEN DistriNet

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

Reevaluation: significant bugfixes?

- Chrome 71: fixed third-party cookie block bypass by PDF
- Opera 57
  - FIXED: prerender bypass for same-site cookies
  - PARTIALLY FIXED: built-in adblocker blocks HTML mechanisms
- Bug fixing is rather slow

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

Thank you!

https://WhoLeftOpenTheCookieJar.com

@tomvangoethem