Origin Policy Enforcement in Modern Browsers

A Case Study in Same Origin Implementations

Frederik Braun

Table of Contents

1. about:me
2. Motivation
   - Ambient Authentication
   - The Severity of a Same Origin Policy Bypass
3. The Same Origin Policy
   - What is the Same Origin Policy?
   - What is an Origin?
   - Examples
4. Evaluation
   - SOP Bypass: Firefox (2007)
   - SOP Bypass: Flash (2010)
   - SOP Bypass: Java 7 Update 5-X (2012)
5. Other/Better Security Policies
   - CSP
   - `iframe` Sandbox
6. Conclusion

Table of Contents

1. about:me
2. Motivation
   - Ambient Authentication
   - The Severity of a Same Origin Policy Bypass
3. The Same Origin Policy
   - What is the Same Origin Policy?
   - What is an Origin?
   - Examples
4. Evaluation
   - SOP Bypass: Firefox (2007)
   - SOP Bypass: Flash (2010)
   - SOP Bypass: Java 7 Update 5-X (2012)
5. Other/Better Security Policies
   - CSP
   - `iframe` Sandbox
6. Conclusion

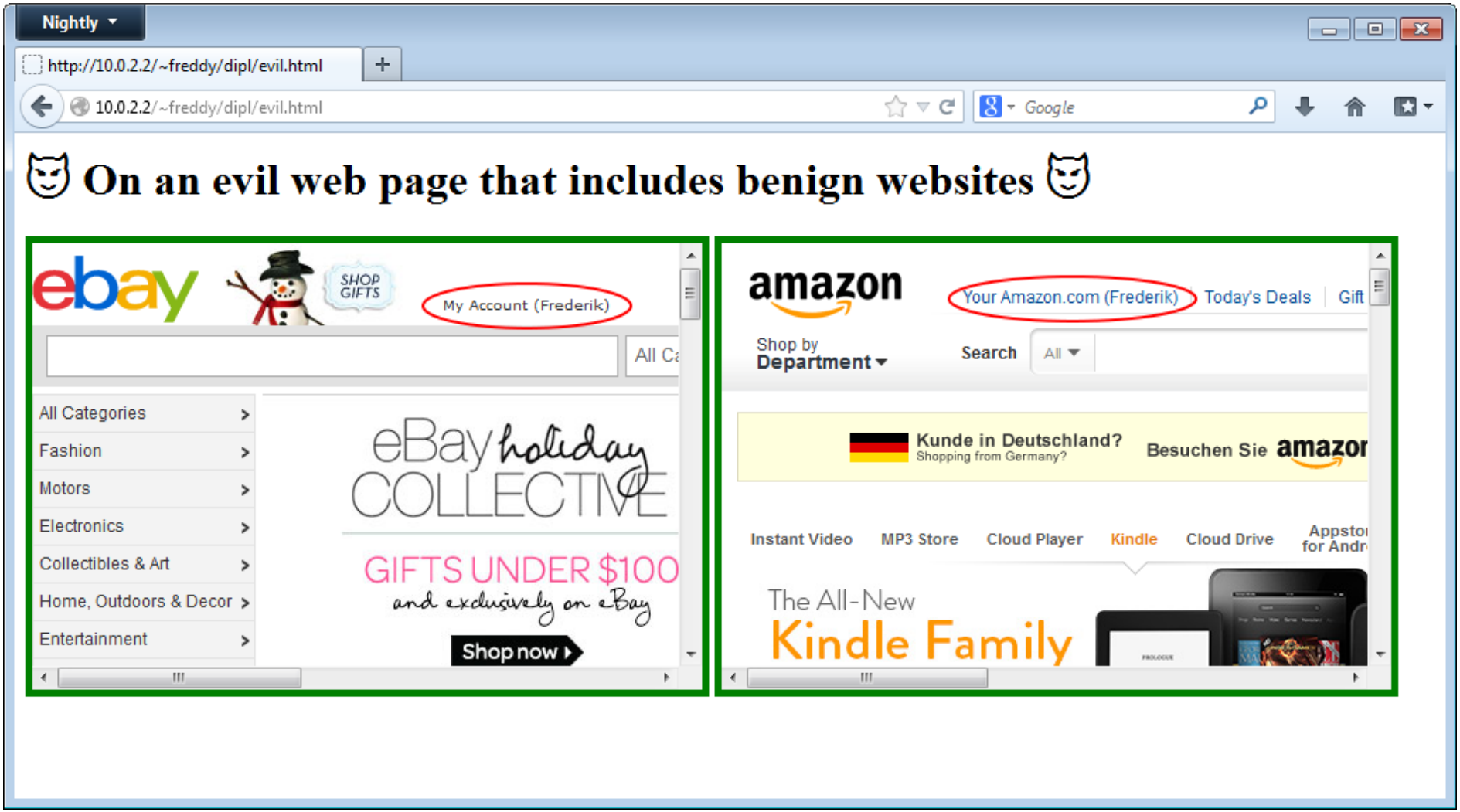
Frederik Braun

- Dipl. Ing. in IT-Security at Ruhr-Uni Bochum (2012)
  - this research!
  - `https://frederik-braun.com/thesis`
- Security Engineer at Mozilla in Berlin
- likes to play CTFs (hi FluxFingers!)
- willing to answer questions :)

Table of Contents

1. about:me
2. Motivation
   - Ambient Authentication
   - The Severity of a Same Origin Policy Bypass
3. The Same Origin Policy
   - What is the Same Origin Policy?
   - What is an Origin?
   - Examples
4. Evaluation
   - SOP Bypass: Firefox (2007)
   - SOP Bypass: Flash (2010)
   - SOP Bypass: Java 7 Update 5-X (2012)
5. Other/Better Security Policies
   - CSP
   - `iframe` Sandbox
6. Conclusion

Ambient Authentication



The Severity of a Same Origin Policy Bypass

OCT
10
2012

Security Vulnerability in Firefox 16

Issue:

Mozilla is aware of a security vulnerability in the current release version of Firefox (version 16). We are actively working on a fix and plan to ship updates tomorrow. Firefox version 15 is unaffected.

Impact:

The vulnerability could allow a malicious site to potentially determine which websites users have visited and have access to the URL or URL parameters. At this time we have no indication that this vulnerability is currently being exploited in the wild.

Status:

Firefox 16 has been temporarily removed from the current installer page and users will automatically be upgraded to the new version as soon as it becomes available. As a precaution, users can downgrade to version 15.0.1 by following these instructions [http://www.mozilla.org

Our Scope

My Thesis - This Talk

- The Same Origin Policy
- Formal Definition
- Actual Implementation
- Exceptions & Loopholes
- Other Policies
- Analysis of Previous Bugs
- Classification
- Bug Hunting

Table of Contents

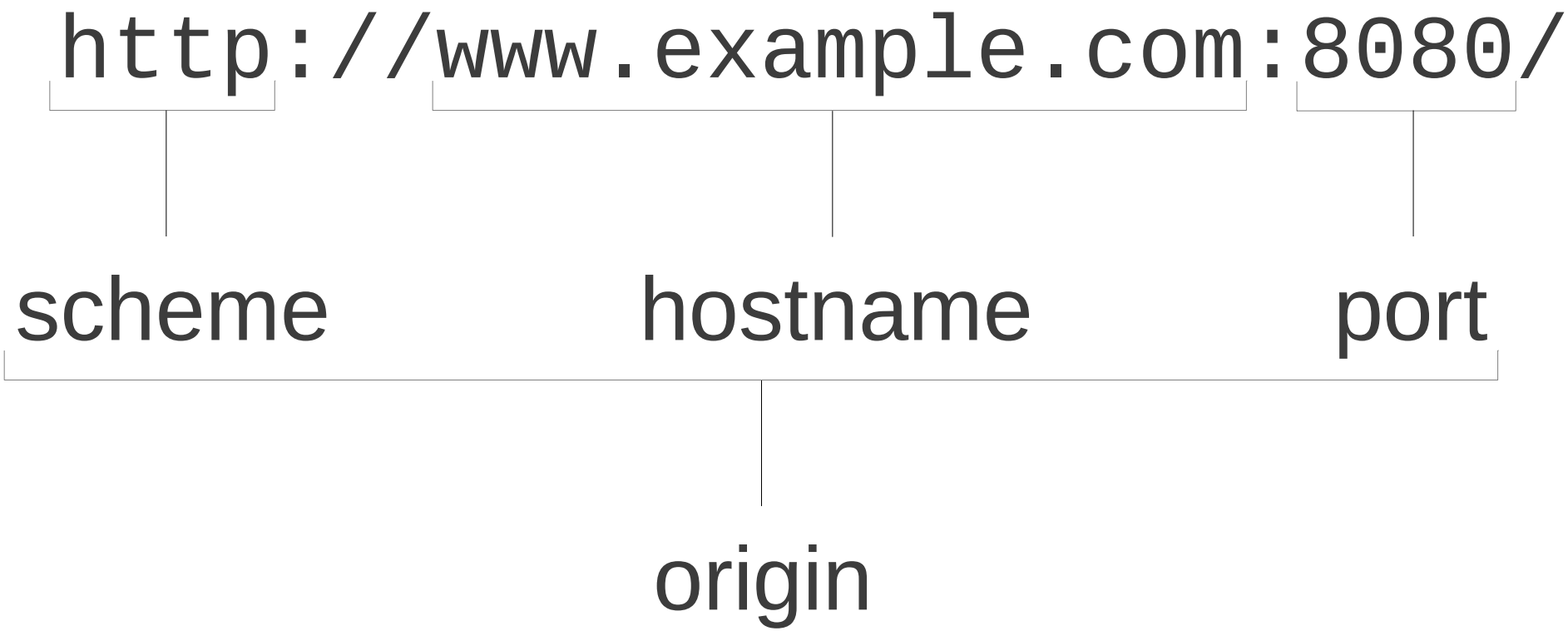
1. about:me
2. Motivation
   - Ambient Authentication
   - The Severity of a Same Origin Policy Bypass
3. The Same Origin Policy
   - What is the Same Origin Policy?
   - What is an Origin?
   - Examples
4. Evaluation
   - SOP Bypass: Firefox (2007)
   - SOP Bypass: Flash (2010)
   - SOP Bypass: Java 7 Update 5-X (2012)
5. Other/Better Security Policies
   - CSP
   - `iframe` Sandbox
6. Conclusion

The Same Origin Policy (SOP)

"An 'origin' (...) is often used as the scope of authority or privilege by user agents. " — Barth

"The same-origin policy is the most important mechanism we have to keep hostile web applications at bay, but it's also an imperfect one." — Zalewski

What is an Origin?



Examples

Compare for http://www.example.com/

URL	same-origin?
http://www.example.com/help	

Examples

Compare for http://www.example.com/

URL	same-origin?
http://www.example.com/help	✓

Examples

Compare for http://www.example.com/

URL	same-origin?
http://www.example.com/help	✓
https://www.example.com/	

Examples

Compare for http://www.example.com/

URL	same-origin?
http://www.example.com/help	✓
https://www.example.com/	✗

Examples

Compare for http://www.example.com/

URL	same-origin?
http://www.example.com/help	✓
https://www.example.com/	✗
about:blank	

Examples

Compare for http://www.example.com/

URL	same-origin?
http://www.example.com/help	✓
https://www.example.com/	✗
about:blank	✓

Examples

Compare for http://www.example.com/

URL	same-origin?
http://www.example.com/help	✓
https://www.example.com/	✗
about:blank	✓
http://www.example.com:8000/phpMyAdmin	

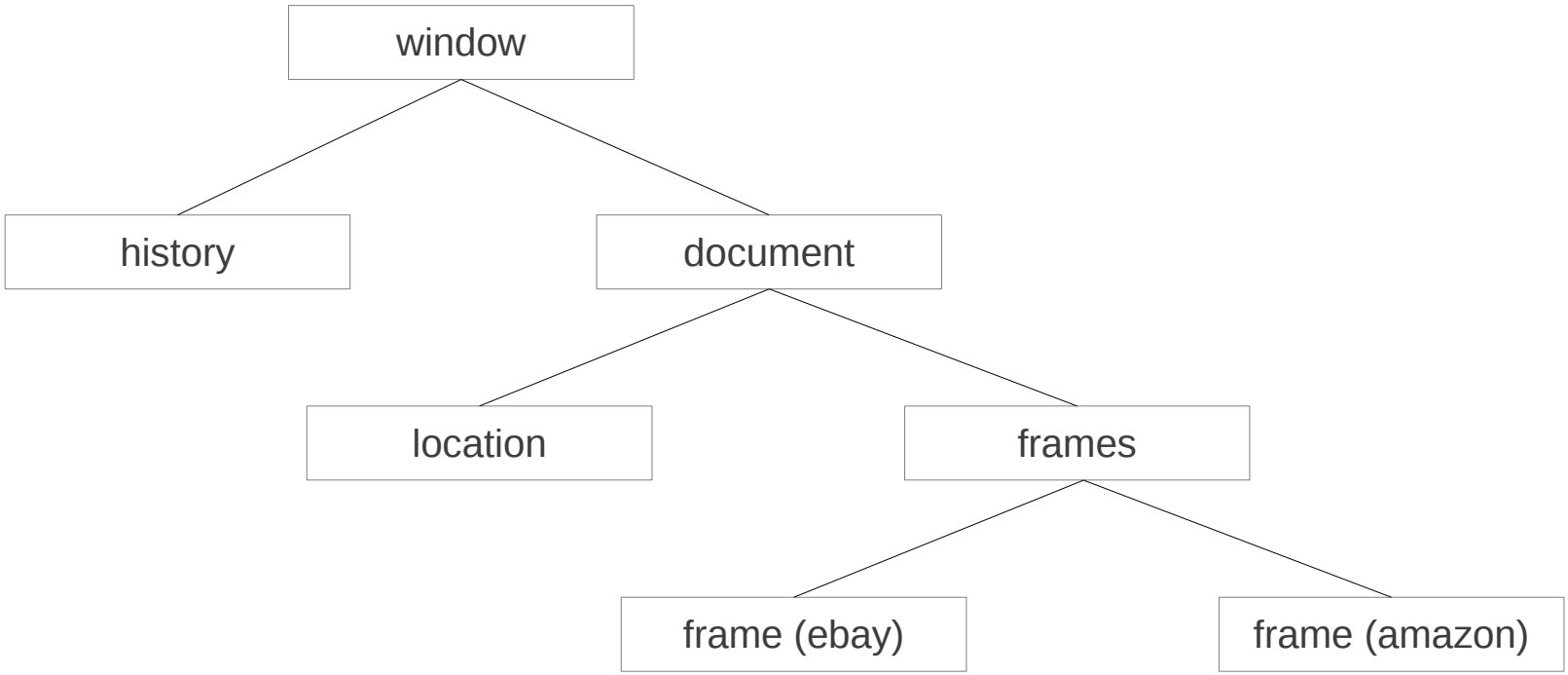
Examples

Compare for http://www.example.com/

URL	same-origin?
http://www.example.com/help	✓
https://www.example.com/	✗
about:blank	✓
http://www.example.com:8000/phpMyAdmin	✗/✓[a]

[a] Internet Explorer doesn't care about ports.

JavaScript Object Hierarchy



No Way Out? - Exceptions

Cookies

window.location setter

window.name persists

document.domain

Internet Explorer Zones

CORS

JSONP

...

SOP Wrap-Up

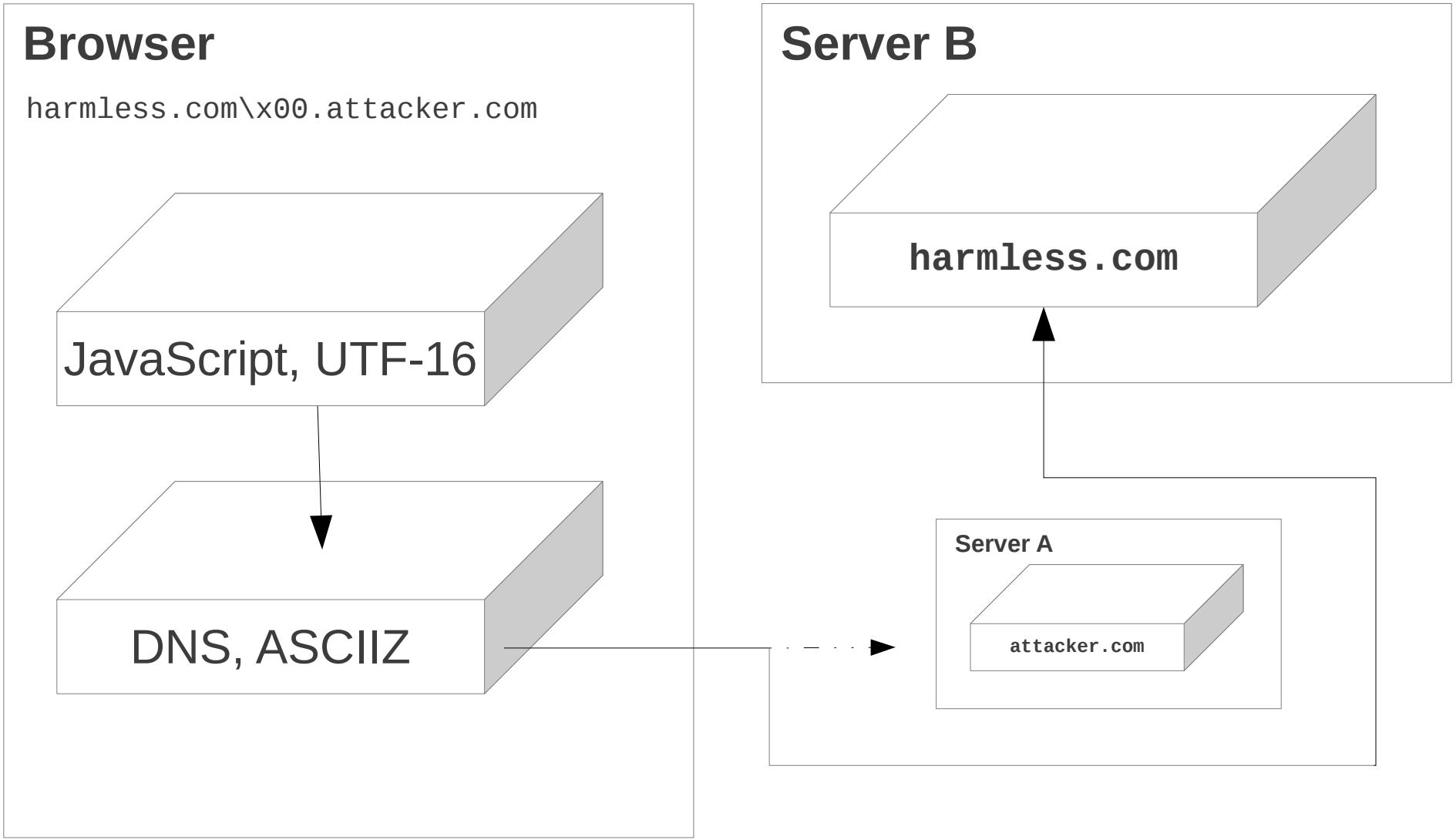
Summary

- read access
- vendor specific
- JavaScript Engine (Object Capability) vs. DOM (Access Control)
- the SOP is highly inhomogenous
- no consistent reference implementation

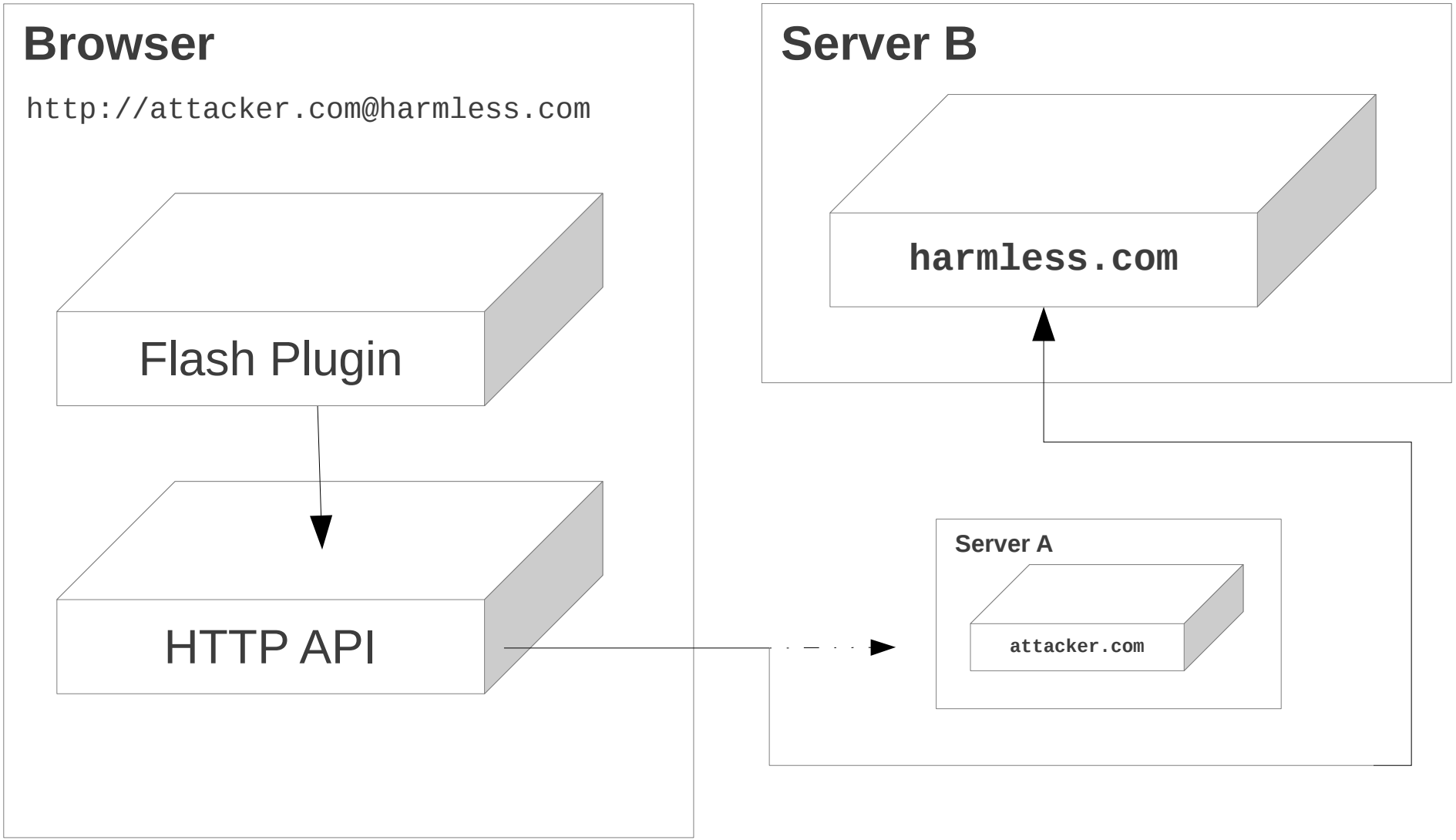
Table of Contents

1. about:me
2. Motivation
   - Ambient Authentication
   - The Severity of a Same Origin Policy Bypass
3. The Same Origin Policy
   - What is the Same Origin Policy?
   - What is an Origin?
   - Examples
4. Evaluation
   - SOP Bypass: Firefox (2007)
   - SOP Bypass: Flash (2010)
   - SOP Bypass: Java 7 Update 5-X (2012)
5. Other/Better Security Policies
   - CSP
   - `iframe` Sandbox
6. Conclusion

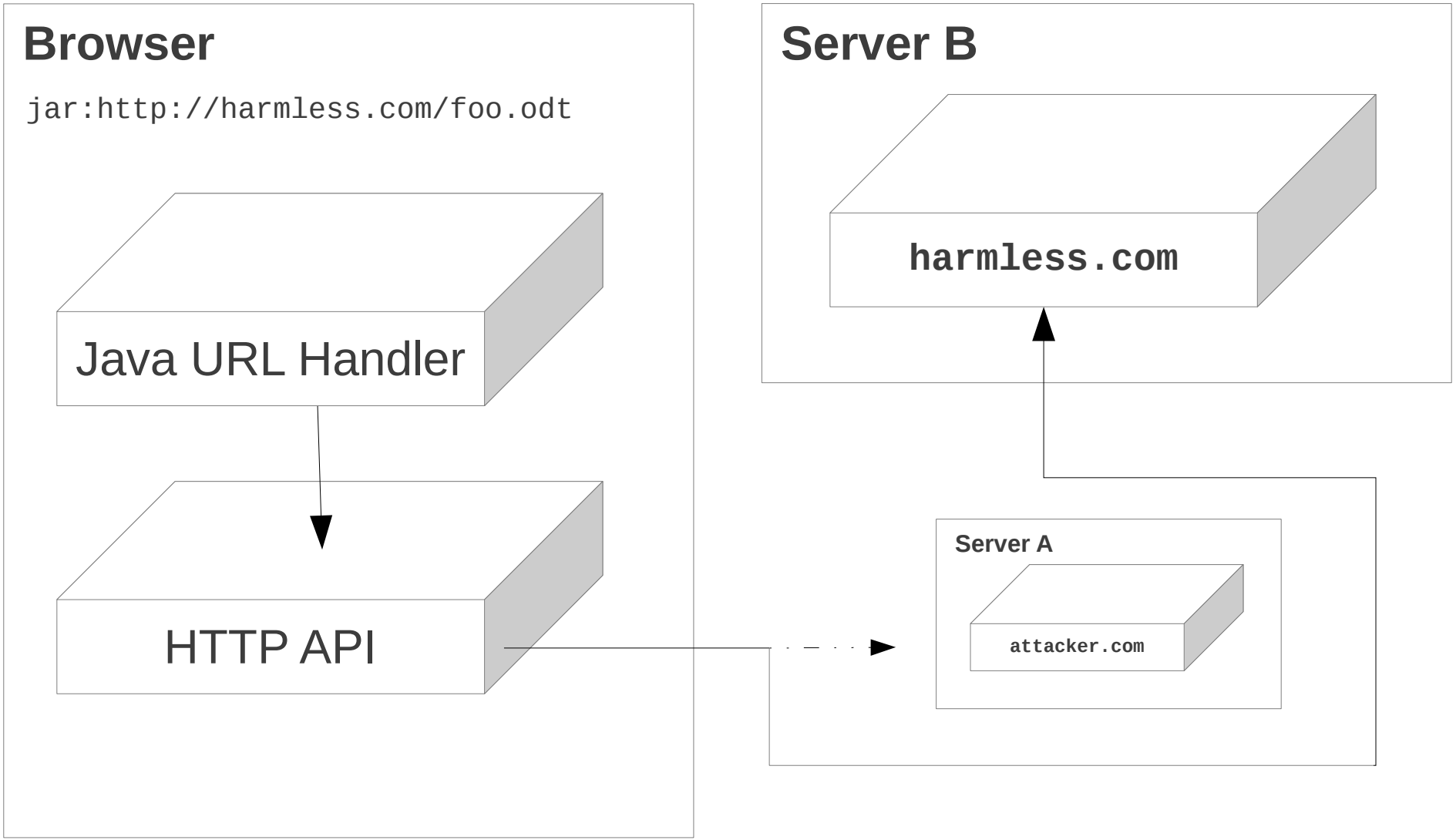
All SOP Flaws are alike (CVE-2007-0981)



All SOP Flaws are alike (CVE-2010-2179)



All SOP Flaws are alike (CVE TBA)



Demo

Table of Contents

1. about:me
2. Motivation
   - Ambient Authentication
   - The Severity of a Same Origin Policy Bypass
3. The Same Origin Policy
   - What is the Same Origin Policy?
   - What is an Origin?
   - Examples
4. Evaluation
   - SOP Bypass: Firefox (2007)
   - SOP Bypass: Flash (2010)
   - SOP Bypass: Java 7 Update 5-X (2012)
5. Other/Better Security Policies
   - CSP
   - `iframe` Sandbox
6. Conclusion

Content Security Policy (CSP)

Content Security Policy

- Security Header
- Whitelist approach for resource inclusion
- XSS Mitigation
- The cool kids do it

Example: A quite strict policy

```
Content-Security-Policy: default-src: 'self'; img-src:
https://static.example.org; script-src:
https://static.example.org google-analytics.com
```

CSP Adoption

Inline JavaScript

- On more than 96% of the web
- No easy way to safely allow inline JavaScript with CSP 1.0
- Disadvantages with CSP 1.1 proposals for inline JS

Safe Content Inclusion

`<iframe sandbox>`

- Displaying content. That's it.
- can be reduced with `allow-` values in the attribute
- Browser adoption is a problem

Partial Sandbox Bypass in Mozilla Firefox

with `allow-scripts` set

- `if (top != window) { top.location = window.location; }`
- non-unique origin. popups, forms, plugins allowed.

Table of Contents

1. about:me
2. Motivation
   - Ambient Authentication
   - The Severity of a Same Origin Policy Bypass
3. The Same Origin Policy
   - What is the Same Origin Policy?
   - What is an Origin?
   - Examples
4. Evaluation
   - SOP Bypass: Firefox (2007)
   - SOP Bypass: Flash (2010)
   - SOP Bypass: Java 7 Update 5-X (2012)
5. Other/Better Security Policies
   - CSP
   - `iframe` Sandbox
6. Conclusion

Conclusion: Same Origin Policy

- an inconsistent policy
- vendor specific
- theoretically, it's a black list
- plugins
- late 2012: Java in nearly 70% of all browsers
- but only 0.2% of websites
- 2013: exploits, Click-To-Play, ..
- But: There are safe & well designed security models on the horizon

Future Work: Automation?

Picture by Jason Huggins on flickr

"This same origin policy is the dumbest thing ever. . . . All this 'protection' serves to do is aggravate legitimate developers trying to get JavaScript to do the simplest of tasks." — Somebody on stackoverflow.com

Thanks

References


Barth, Adam.
The web origin concept.
http://tools.ietf.org/html/rfc6454, December 2011.


Q-Success.
Usage of client-side programming languages for websites.
http://w3techs.com/technologies/overview/client_side_language/all.
Last visited 2012-10-17.


Michal Zalewski.
The Tangled Web: A Guide to Securing Modern Web Applications.
No Starch Press, November 2011.

- For all references please see full thesis on
  `https://frederik-braun.com/thesis`