Sandboxing JavaScript

Lieven Desmet

Nick Nikiforakis

Steven Van Acker

OWASP
The Open Web Application Security Project

KU LEUVEN
DISTRINET RESEARCH GROUP

iMinds
CONNECT.INNOVATE.CREATE

About myself

@lieven_desmet

- Lieven Desmet
- Research manager of the iMinds-DistriNet Research Group (KU Leuven, Belgium)
  - Software security lab with 80+ researchers
  - Dedicated team on Web App Sec
- Active participation in OWASP:
  - Board member of the OWASP Belgium Chapter

Sandboxing JavaScript: Outline

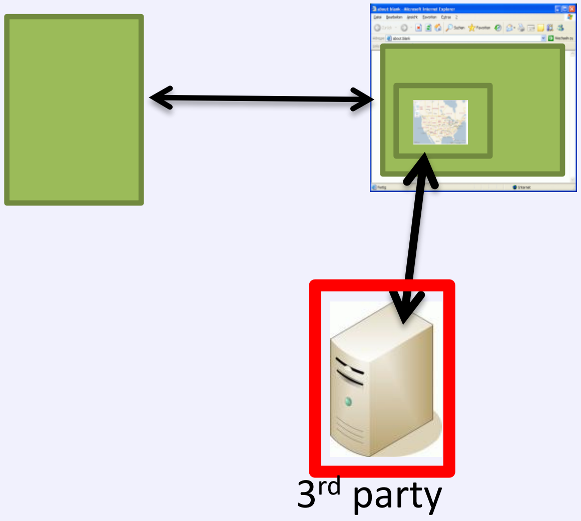
- Integrating JavaScript
- Large-scale analysis of script inclusions
- Overview of mitigation techniques
  - HTML5 Sandbox/CSP-enabled security architecture
  - JSand: Server-driven sandboxing of JavaScript
- Conclusion

INTEGRATING JAVASCRIPT

JavaScript inclusion: security model

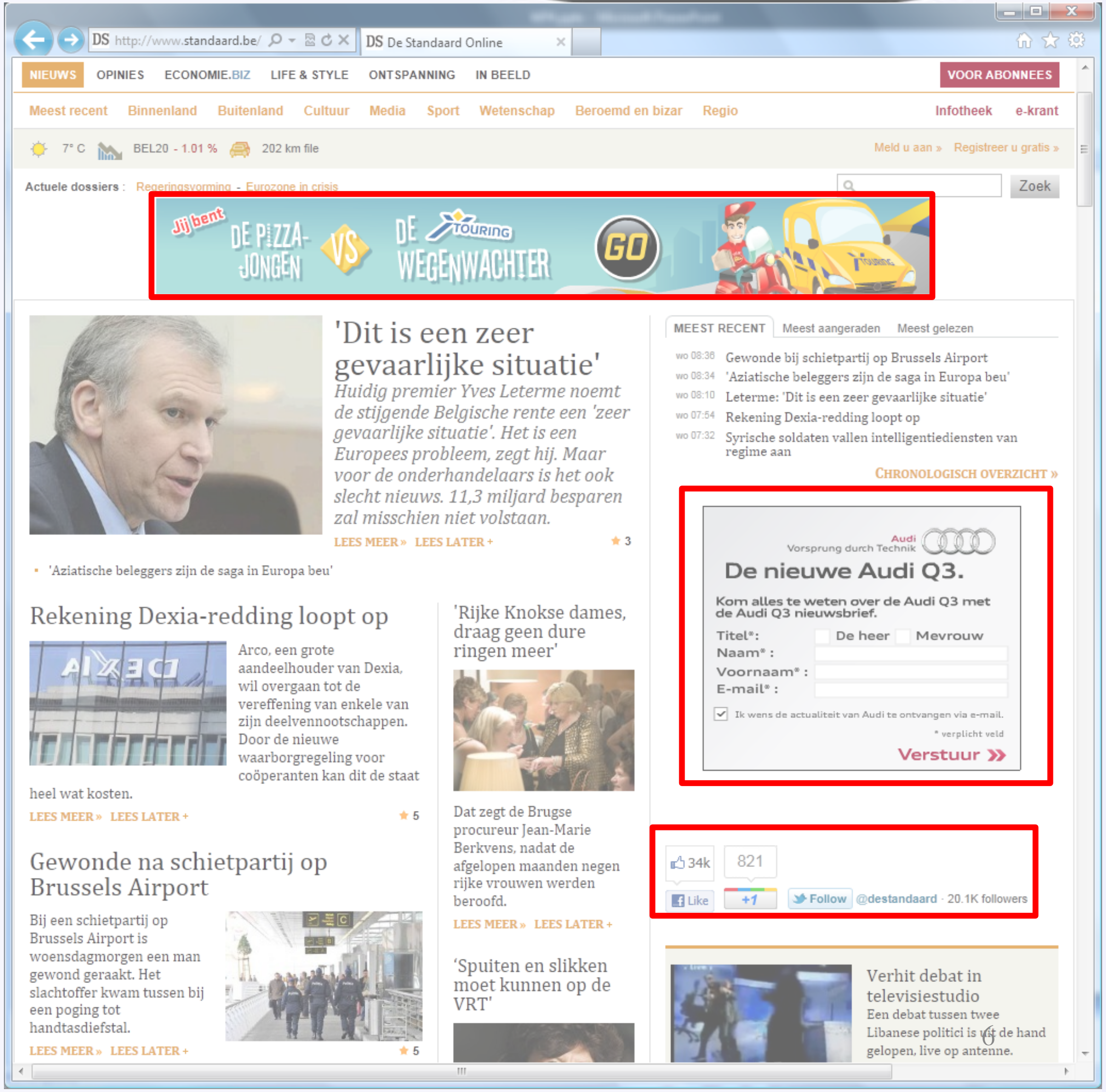
```
<html><body>
…
<script src="http://3rdparty.com/script.js"></script>
…
</body></html>
```

Security model:



Third-party JavaScript is everywhere

- Advertisements
  - Adhese ad network
- Social web
  - Facebook Connect
  - Google+
  - Twitter
  - Feedsburner
- Tracking
  - Scorecardresearch
- Web Analytics
  - Yahoo! Web Analytics
  - Google Analytics
- …



'Dit is een zeer gevaarlijke situatie'

Huidig premier Yves Leterme noemt de stijgende Belgische rente een 'zeer gevaarlijke situatie'. Het is een Europees probleem, zegt hij. Maar voor de onderhandelaars is het ook slecht nieuws. 11,3 miljard besparen zal misschien niet volstaan.

LEES MEER » LEES LATER + ★ 3

- 'Aziatische beleggers zijn de saga in Europa beu'

Rekening Dexia-redding loopt op

Arco, een grote aandeelhouder van Dexia, wil overgaan tot de vereffening van enkele van zijn deelvennootschappen. Door de nieuwe waarborgregeling voor coöperanten kan dit de staat heel wat kosten.

LEES MEER » LEES LATER + ★ 5

Gewonde na schietpartij op Brussels Airport

Bij een schietpartij op Brussels Airport is woensdagmorgen een man gewond geraakt. Het slachtoffer kwam tussen bij een poging tot handtasdiefstal.

LEES MEER » LEES LATER + ★ 5

'Rijke Knokse dames, draag geen dure ringen meer'

Dat zegt de Brugse procureur Jean-Marie Berkvens, nadat de afgelopen maanden negen rijke vrouwen werden beroofd.

LEES MEER » LEES LATER +

'Spuiten en slikken moet kunnen op de VRT'

MEEST RECENT | Meest aangeraden | Meest gelezen

wo 08:36 Gewonde bij schietpartij op Brussels Airport
wo 08:34 'Aziatische beleggers zijn de saga in Europa beu'
wo 08:10 Leterme: 'Dit is een zeer gevaarlijke situatie'
wo 07:54 Rekening Dexia-redding loopt op
wo 07:32 Syrische soldaten vallen intelligentiediensten van regime aan

CHRONOLOGISCH OVERZICHT »

De nieuwe Audi Q3.

Kom alles te weten over de Audi Q3 met de Audi Q3 nieuwsbrief.

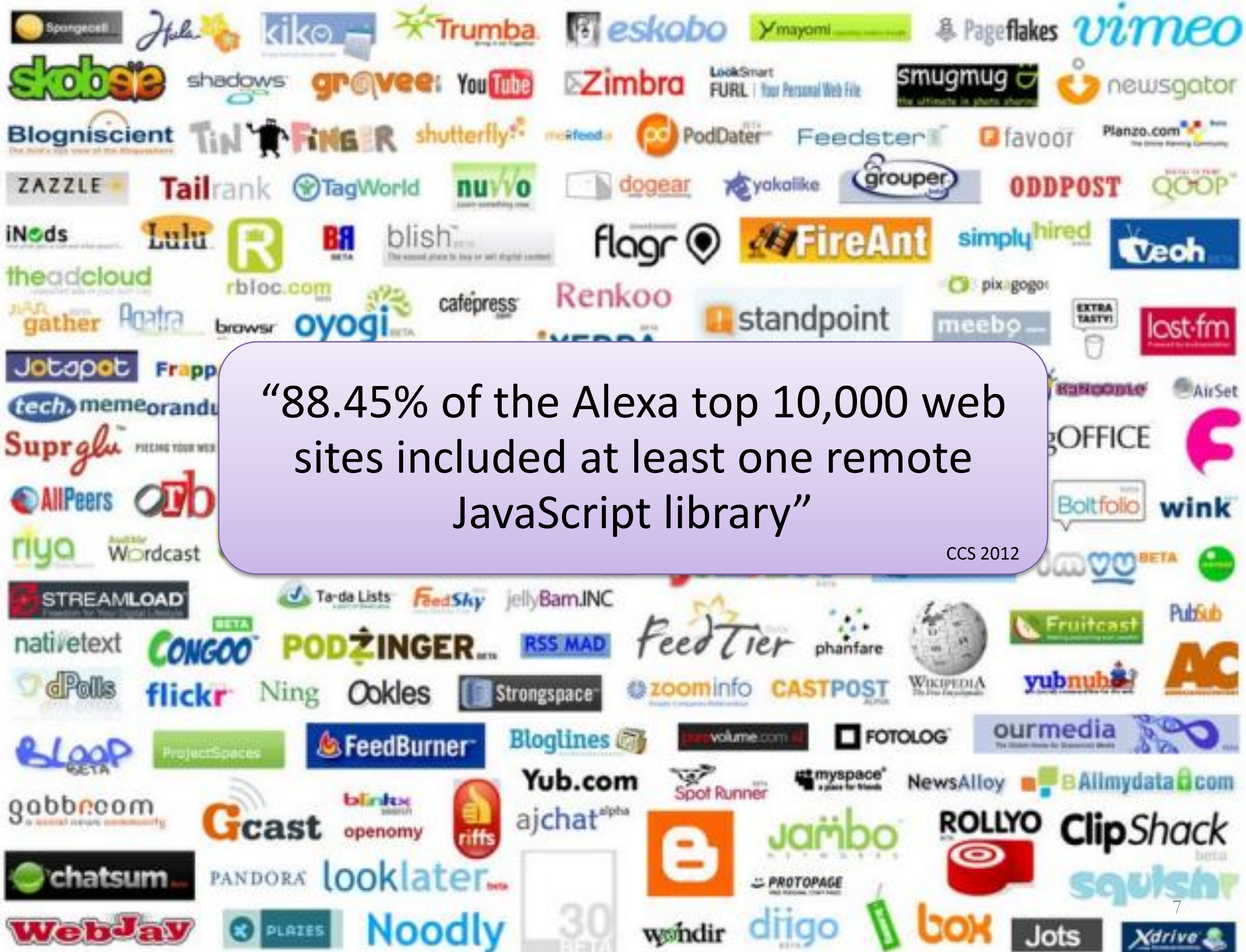
Titel*: □ De heer □ Mevrouw
Naam* :
Voornaam* :
E-mail* :

☑ Ik wens de actualiteit van Audi te ontvangen via e-mail.

* verplicht veld

Verhit debat in televisiestudio

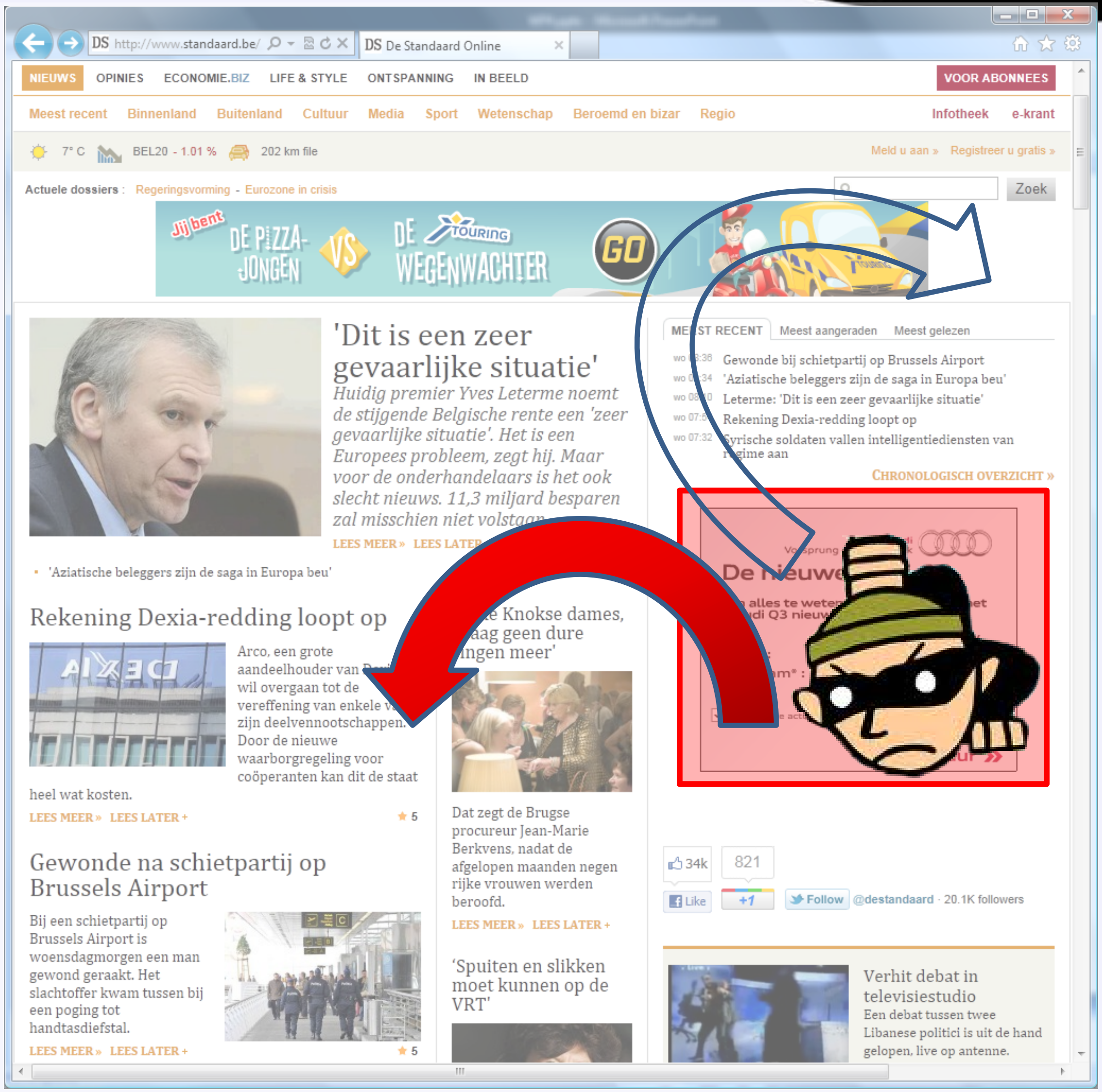
Een debat tussen twee Libanese politici is uit de hand gelopen, live op antenne.



"88.45% of the Alexa top 10,000 web sites included at least one remote JavaScript library"

CCS 2012

Malicious third-party scripts can …



DS http://www.standaard.be/ DS De Standaard Online

NIEUWS OPINIES ECONOMIE.BIZ LIFE & STYLE ONTSPANNING IN BEELD VOOR ABONNEES

Meest recent Binnenland Buitenland Cultuur Media Sport Wetenschap Beroemd en bizar Regio Infotheek e-krant

7° C BEL20 - 1.01 % 202 km file Meld u aan » Registreer u gratis »

Actuele dossiers : Regeringsvorming - Eurozone in crisis Zoek

'Dit is een zeer gevaarlijke situatie'

Huidig premier Yves Leterme noemt de stijgende Belgische rente een 'zeer gevaarlijke situatie'. Het is een Europees probleem, zegt hij. Maar voor de onderhandelaars is het ook slecht nieuws. 11,3 miljard besparen zal misschien niet volstaan

LEES MEER » LEES LATER

- 'Aziatische beleggers zijn de saga in Europa beu'

Rekening Dexia-redding loopt op

Arco, een grote aandeelhouder van De… wil overgaan tot de vereffening van enkele v… zijn deelvennootschappen. Door de nieuwe waarborgregeling voor coöperanten kan dit de staat heel wat kosten.

LEES MEER » LEES LATER + ★ 5

…e Knokse dames, …aag geen dure …ingen meer'

Dat zegt de Brugse procureur Jean-Marie Berkvens, nadat de afgelopen maanden negen rijke vrouwen werden beroofd.

LEES MEER » LEES LATER +

Gewonde na schietpartij op Brussels Airport

Bij een schietpartij op Brussels Airport is woensdagmorgen een man gewond geraakt. Het slachtoffer kwam tussen bij een poging tot handtasdiefstal.

LEES MEER » LEES LATER + ★ 5

'Spuiten en slikken moet kunnen op de VRT'

ME…ST RECENT Meest aangeraden Meest gelezen

wo …:36 Gewonde bij schietpartij op Brussels Airport
wo …:34 'Aziatische beleggers zijn de saga in Europa beu'
wo 08:…0 Leterme: 'Dit is een zeer gevaarlijke situatie'
wo 07:5… Rekening Dexia-redding loopt op
wo 07:32 Syrische soldaten vallen intelligentiediensten van …gime aan

CHRONOLOGISCH OVERZICHT »

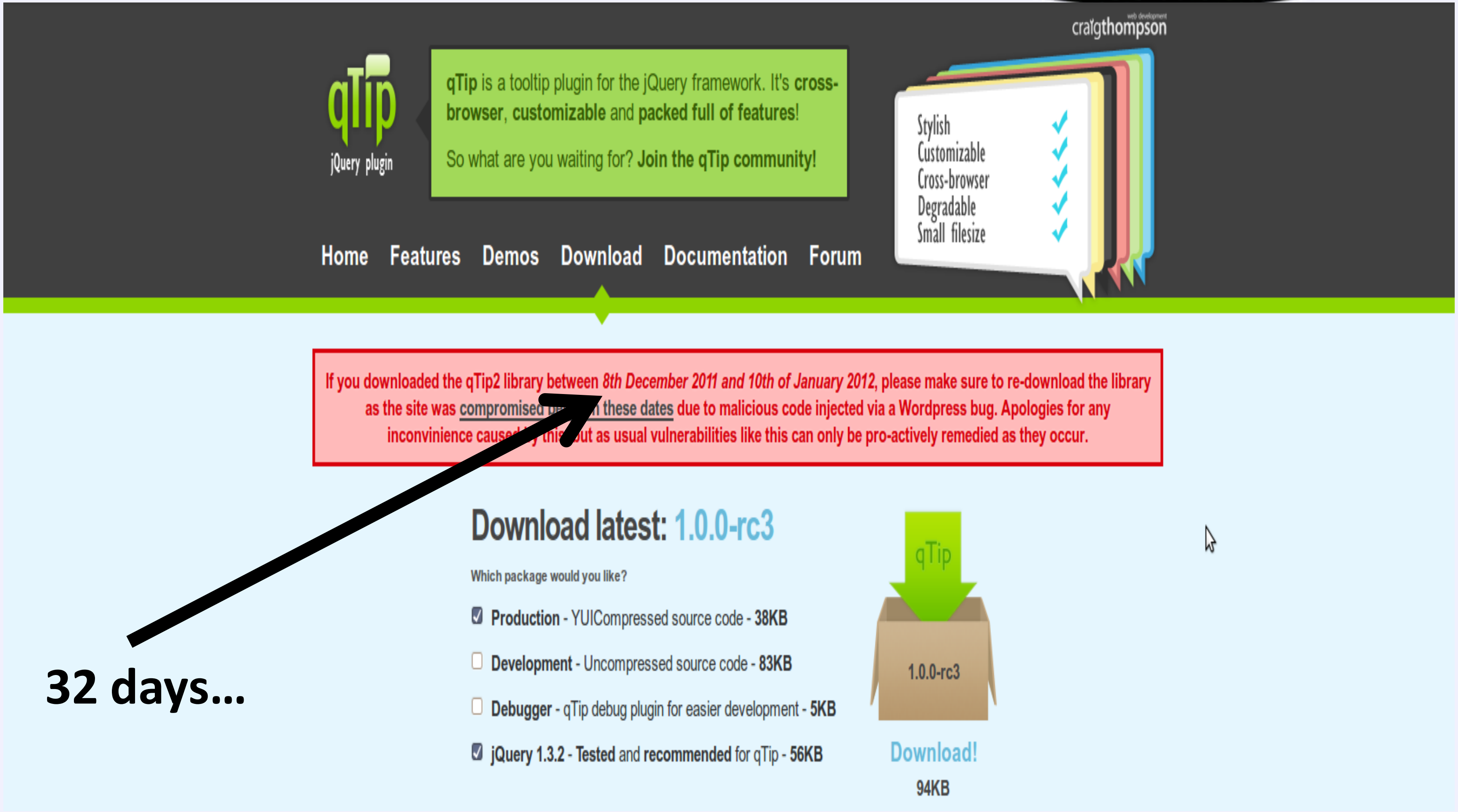
34k 821 Like +1 Follow @destandaard · 20.1K followers

Verhit debat in televisiestudio

Een debat tussen twee Libanese politici is uit de hand gelopen, live op antenne.

And it happens in practice…

OWASP
The Open Web Application Security Project



qTip is a tooltip plugin for the jQuery framework. It's **cross-browser**, **customizable** and **packed full of features**!

So what are you waiting for? **Join the qTip community!**

If you downloaded the qTip2 library between *8th December 2011 and 10th of January 2012*, please make sure to re-download the library as the site was compromised between these dates due to malicious code injected via a Wordpress bug. Apologies for any inconvinience caused by this, but as usual vulnerabilities like this can only be pro-actively remedied as they occur.

Download latest: 1.0.0-rc3

Which package would you like?

☑ **Production** - YUICompressed source code - **38KB**

□ **Development** - Uncompressed source code - **83KB**

□ **Debugger** - qTip debug plugin for easier development - **5KB**

☑ **jQuery 1.3.2** - **Tested** and **recommended** for qTip - **56KB**

Download!
94KB

32 days…

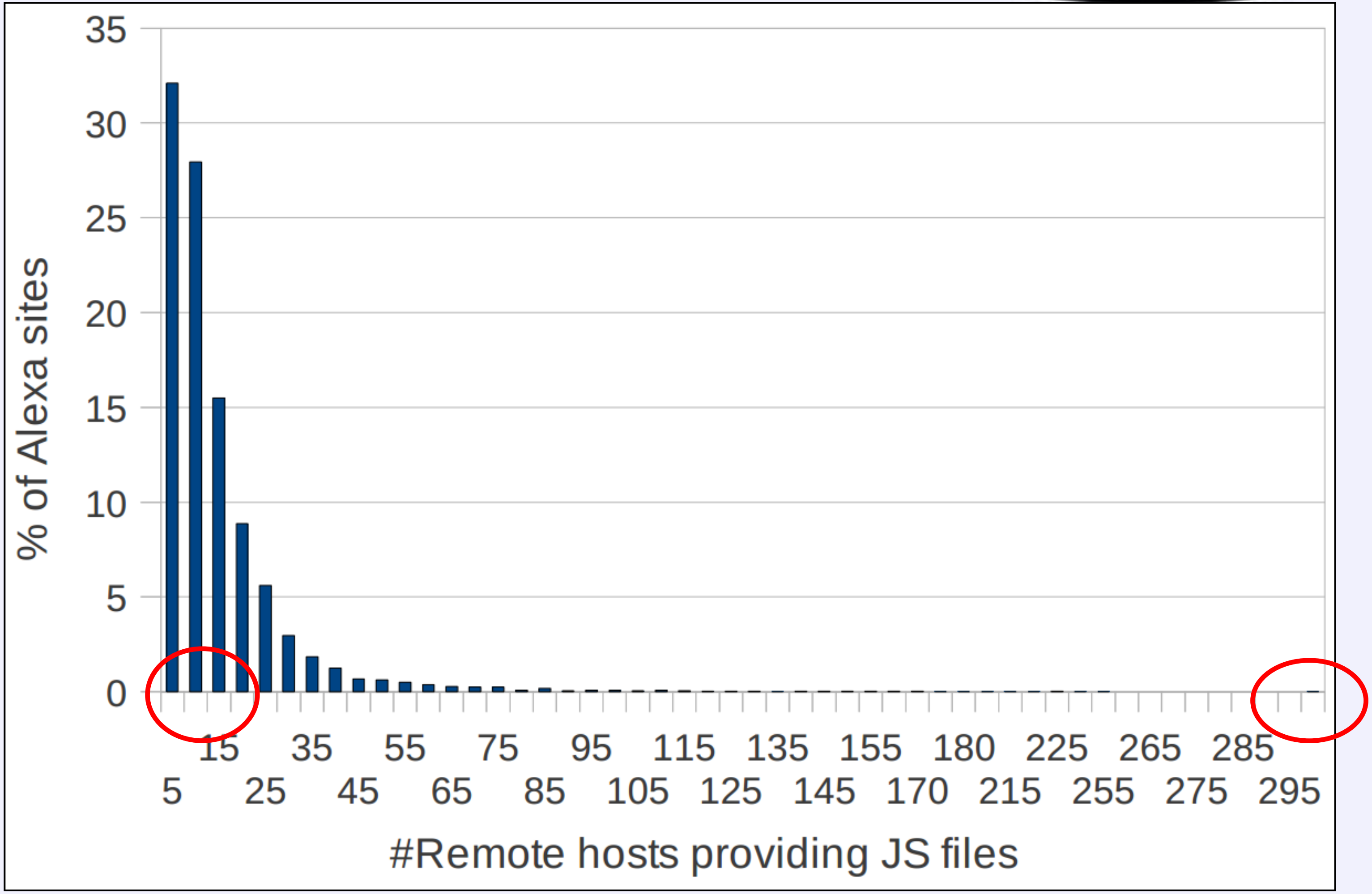
Nick Nikiforaki *et. al*. **You are what you include: Large-scale evaluation of remote JavaScript inclusions**. In *Proceedings of the ACM Conference on Computer and Communications Security*. 2012.

LARGE-SCALE ANALYSIS OF SCRIPT INCLUSIONS

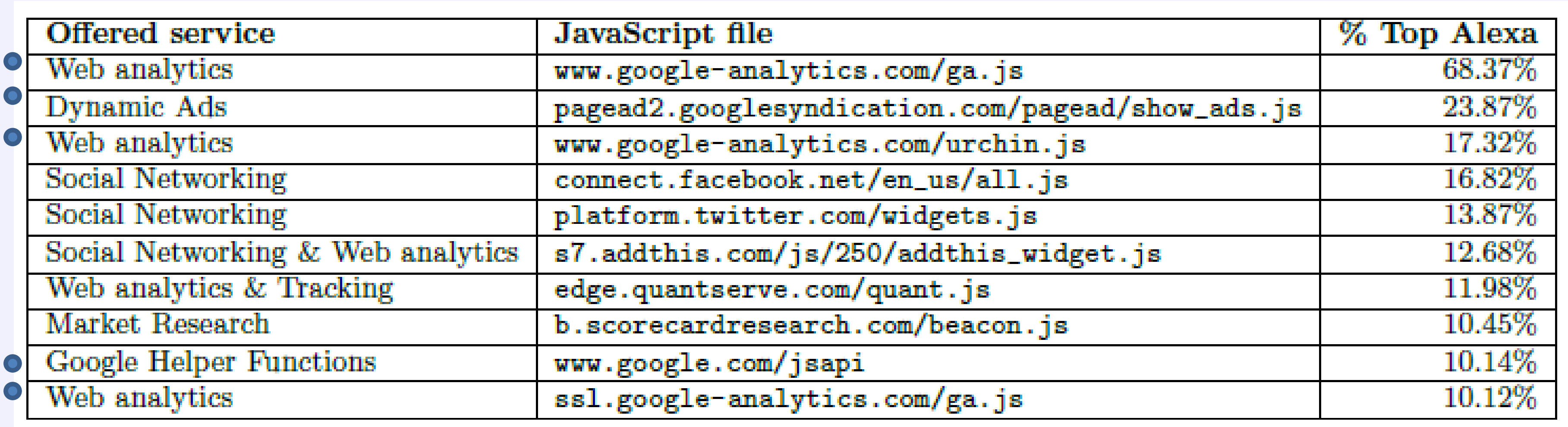
Data Collection Experiment

- Crawled over 3,300,000 pages belonging to the Alexa top 10,000
- Discovered:
  - – 8,439,799 remote inclusions
  - – 301,968 unique JS files
  - – 20,225 uniquely-addressed remote hosts

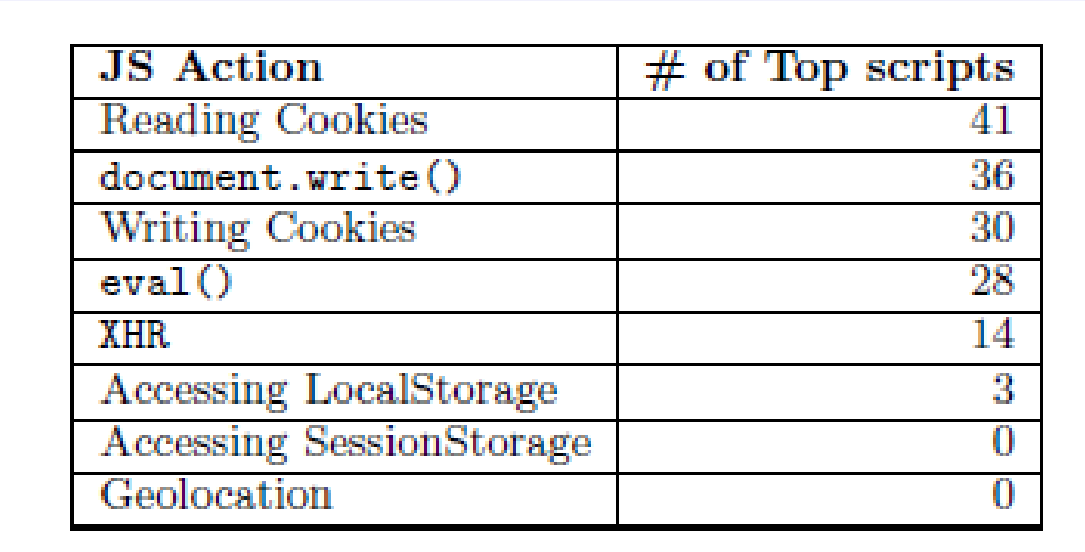
How many remote hosts?



Popular JavaScript libraries and APIs



Offered service	JavaScript file	% Top Alexa
● Web analytics	www.google-analytics.com/ga.js	68.37%
● Dynamic Ads	pagead2.googlesyndication.com/pagead/show_ads.js	23.87%
● Web analytics	www.google-analytics.com/urchin.js	17.32%
Social Networking	connect.facebook.net/en_us/all.js	16.82%
Social Networking	platform.twitter.com/widgets.js	13.87%
Social Networking & Web analytics	s7.addthis.com/js/250/addthis_widget.js	12.68%
Web analytics & Tracking	edge.quantserve.com/quant.js	11.98%
Market Research	b.scorecardresearch.com/beacon.js	10.45%
● Google Helper Functions	www.google.com/jsapi	10.14%
● Web analytics	ssl.google-analytics.com/ga.js	10.12%



JS Action	# of Top scripts
Reading Cookies	41
document.write()	36
Writing Cookies	30
eval()	28
XHR	14
Accessing LocalStorage	3
Accessing SessionStorage	0
Geolocation	0

New Attacks?

OWASP
The Open Web Application Security Project

- 8.5 million records of remote inclusions
- Are there new attack vectors to exploit the script-inclusion pattern?

- 4 new attack vectors
  - Cross-user & Cross-network Scripting
  - Stale domain-based inclusions
  - Stale IP-based inclusions
  - Typo-squatting Cross-Site Scripting

Stale domain-based inclusions

- What happens when you trust a remote site and the domain of that site expires?
  - Anyone can register it, and start serving malicious JS
  - Equal in power to stored XSS
- 56 domains found, used in 47 sites

Shopping spree!

- Registered some of the stale domains:
  - blogtools.us -> goldprice.org (4,779th in Alexa)
  - hbotapadmin.us -> hbo.com

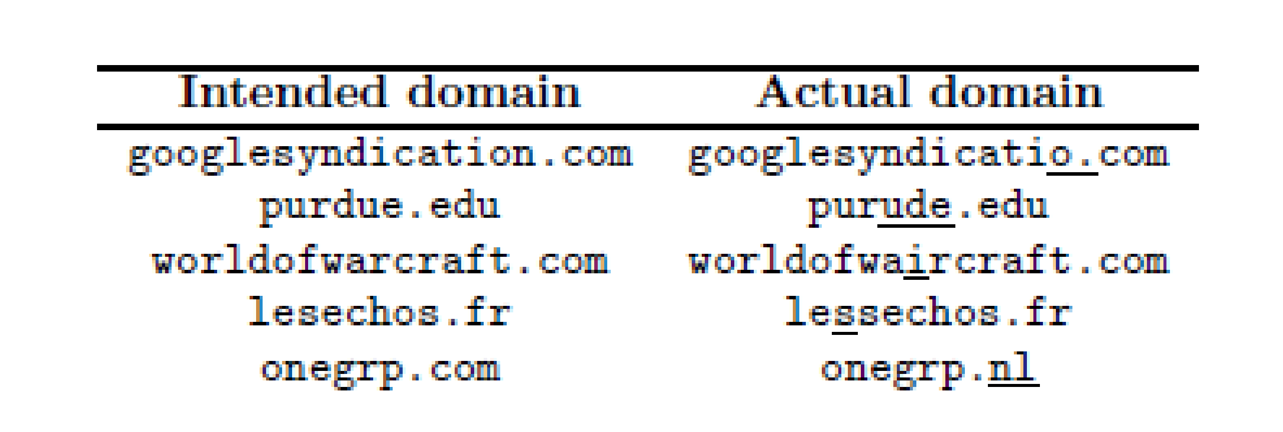
	Blogtools.us	Hbotapadmin.com
Visits	80,466	4,615
Including domains	24	4
Including pages	84	41

Typo-squatting XSS

- Typo-squatting
  - registering domains that are mistypes of popular domains
  - Serve ads, phishing, drive-by downloads etc. to users that mistype the domain
- Unfortunately… developers are also humans
  - <script src=http://googlesyndicatio.com/...>

Examples found…

	Googlesyndicatio.com
Unique visitors	163,188
Including domains	1185
Including pages	21,830



Intended domain	Actual domain
googlesyndication.com	googlesyndicatio.com
purdue.edu	purude.edu
worldofwarcraft.com	worldofwaircraft.com
lesechos.fr	lessechos.fr
onegrp.com	onegrp.nl

OVERVIEW OF MITIGATION TECHNIQUES

Existing mitigation techniques?

OWASP
The Open Web Application Security Project

- Limit third-party code to safe subset of JavaScript
  - Facebook JS, ADSafe, ADSafety, ...

No compatibility with existing scripts

- Browser-based sandboxing solutions
  - ConScript, WebJail, Contego, ...

Browser modifications imply short-term deployment issues

- Server-side transformations of scripts to be included
  - Google Caja, Jacaranda, BrowserShield, ...

No direct script delivery to browser

Changes architecture of the web

KU LEUVEN
DISTRINET RESEARCH GROUP
iMinds
CONNECT.INNOVATE.CREATE

Emerging solutions: Client-side security architectures

- JavaScript security architecture on top of mainstream browsers
  - Sandboxing/isolation of untrusted JavaScript code
  - Policy-controlled mediation to the actual DOM

- HTML5 sandbox/CSP-enabled security architecture
- TreeHouse: web workers sandbox architecture
- JSand: SES-enabled sandbox architecture

Based on the talk of Mike West at Devoxx 2012

Securing the Client-Side: Building safe web applications with HTML5

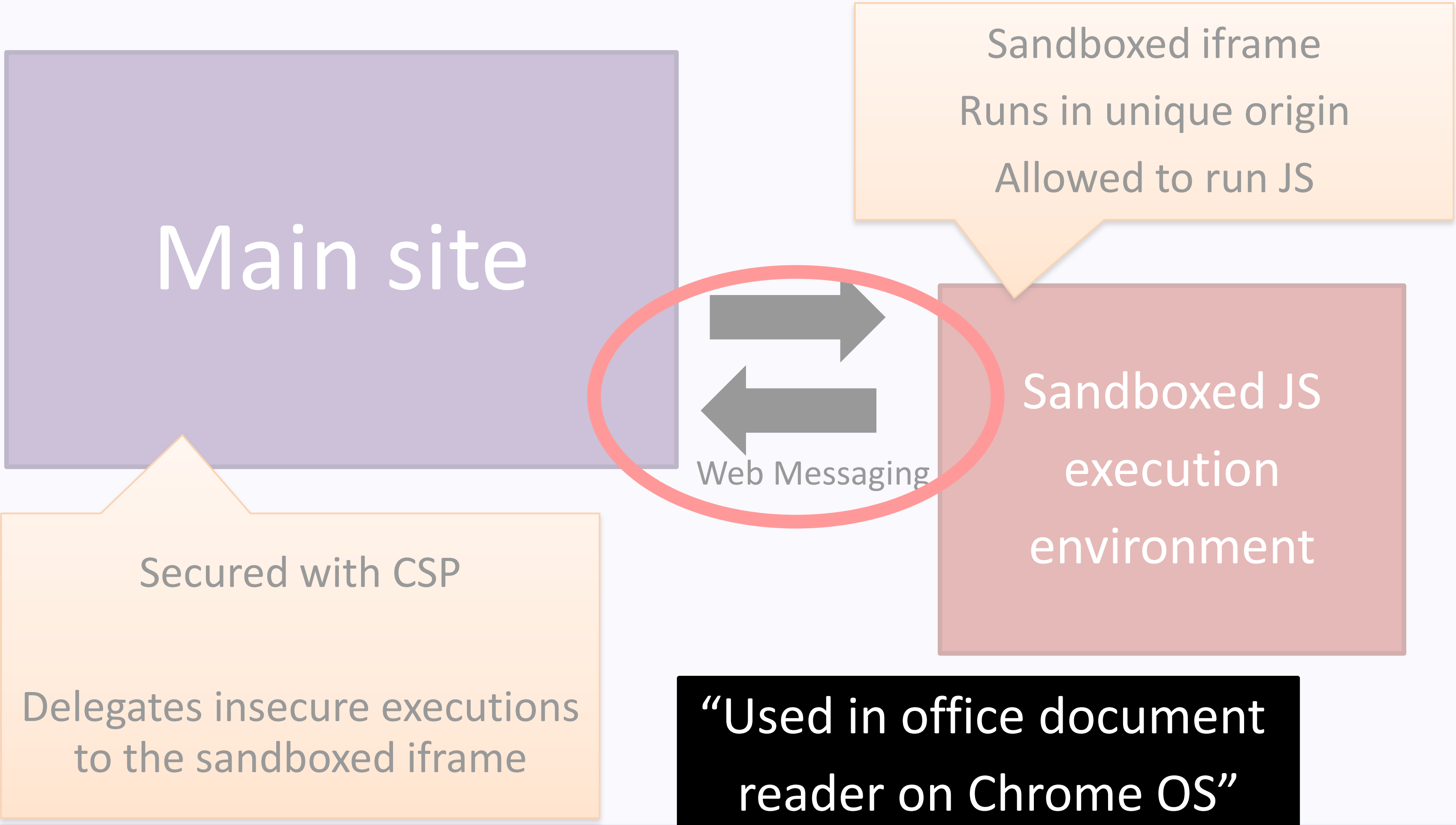
https://mikewest.org/2013/02/securing-the-client-side-devoxx-2012

HTML5 SANDBOX/CSP-ENABLED SECURITY ARCHITECTURE

Content Security Policy (CSP)

- Issued as HTTP response header
  - Content-Security-Policy: script-src 'self'; object-src 'none'
- Specifies which resources are allowed to be loaded as part of your page
- Extremely promising as an additional layer of defense against script injection

Example of sandboxing unsafe JavaScript



Main site

Secured with CSP

Delegates insecure executions to the sandboxed iframe

Web Messaging

Sandboxed iframe

Runs in unique origin

Allowed to run JS

Sandboxed JS execution environment

"Used in office document reader on Chrome OS"

"Securing the Client-Side: Building safe web applications with HTML5" (Mike West, Devoxx 2012)

Main page (index.html)

```
Content-Security-Policy: script-src 'self'
```

```
<html><head>
   <script src="main.js"></script>
</head>
<body>
   <a href="#" id="sandboxFrame"/>Click here</a>
   <iframe id="sandboxFrame" sandbox="allow-scripts"
src="sandbox.html">
   </iframe>
   <div ="#content"></div>
</body></html>
```

“Securing the Client-Side: Building safe web applications with HTML5” (Mike West, Devoxx 2012)

Sandboxed frame (sandbox.html)

```
<html><head>
  <script>
        window.EventListener('message', function(event) {
         var command = event.data.command;
              var context = event.data.context;
              var result = callUnsafeFunction(command, context);
              event.source.postMessage({
                     html: result}, event.origin);
              });
  </script>
</head></html>
```

“Securing the Client-Side: Building safe web applications with HTML5” (Mike West, Devoxx 2012)

Main script (main.js)

OWASP

The Open Web Application Security Project

```
document.querySelector('#click').addEventListener('click',
  function(){
    var iframe = document.querySelector('#sandboxFrame');
              var message = { command = 'render‘; context = {thing: 'world‘}};
              iframe.contentWindow.postMessage(message, '*');
});

window.addEventListener('message', function(event){
  //Would be dangerous without the CSP policy!
  var content = document.querySelector('#content');
  content.innerHTML = event.data.html;
});
```

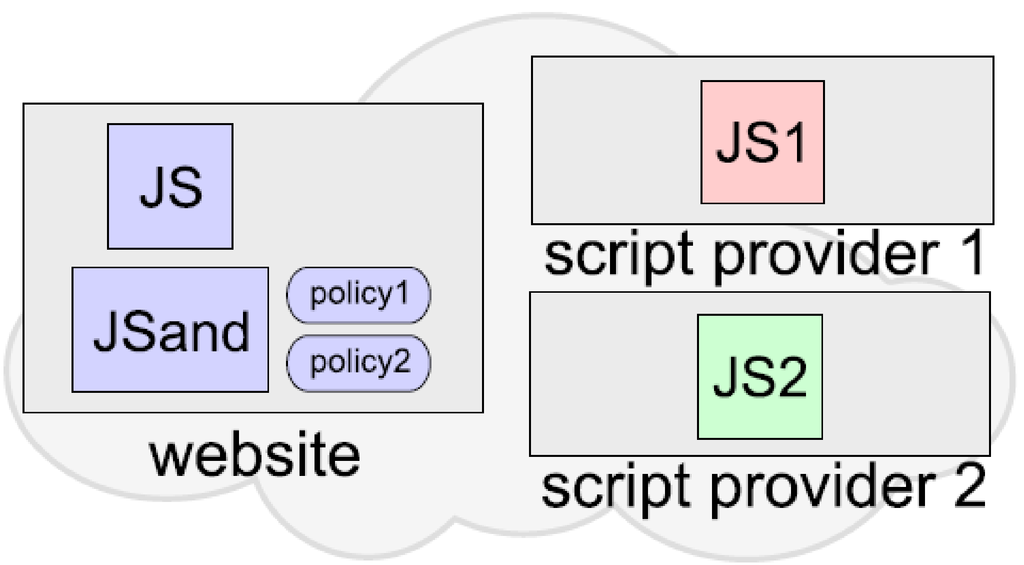
KU LEUVEN DISTRINET RESEARCH GROUP iMinds CONNECT.INNOVATE.CREATE

“Securing the Client-Side: Building safe web applications with HTML5” (Mike West, Devoxx 2012)

Pieter Agten *et. al.* **JSand: Complete Client-Side Sandboxing of Third-Party JavaScript without Browser Modifications.** In proceedings of the Annual Computer Security Applications Conference (ACSAC 2012).

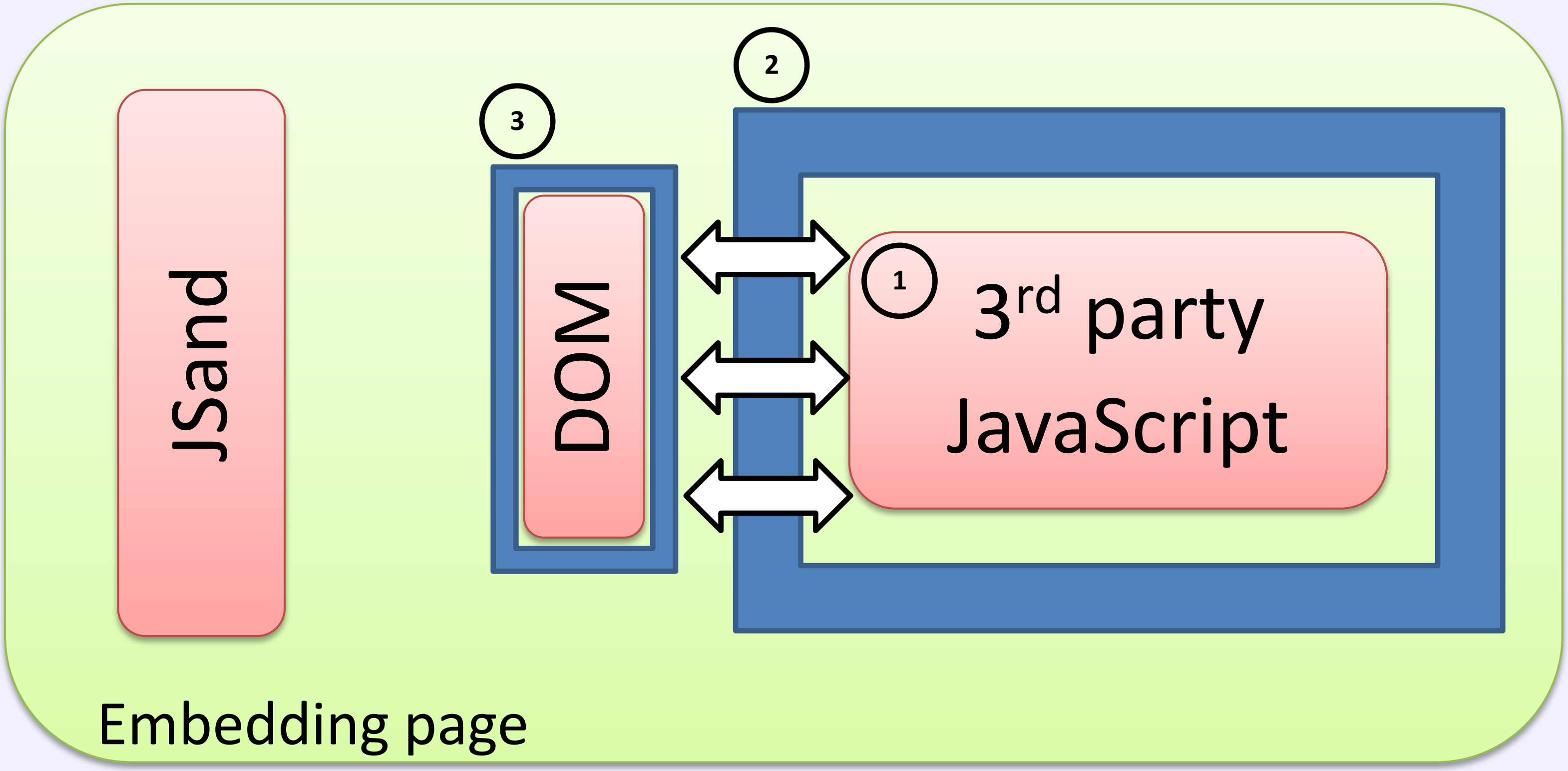
JSAND: SERVER-DRIVEN SANDBOXING OF JAVASCRIPT

JSand: Server-driven sandboxing of JavaScript



Browser

Jsand: under the hood



SES, Proxies, and membranes

- Secure ECMAScript library (SES)
  - Developed by Google CAJA Team
  - Provides object-capability functionality within JavaScript
- JS Proxy API
  - Provides transparent proxy capabilities in wrapping native functionality
- Membrane pattern
  - Guarantees that no object capabilities (i.e. References) leak through the sandbox perimeter

Sandboxing/ isolation

Policy-controlled DOM mediation

Server-driven policy enforcement (1)

```
<html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
    <title>JSP Page</title>
    <jsand:initialize/>
    <jsand:sandbox policy="my embedded script">
      <jsand:code>alert("inline code on the page");</jsand:code>
    </jsand:sandbox>
  </head>
  <body>
    <h1>Hello World!</h1>
  </body>
</html>
```

Server-driven policy enforcement (2)

```
<jsand:sandbox policy="googlemapsNoGeolocation">
        <jsand:code>
                canvasID = "map_canvas2";
                failcity = "New York";
                failpos = new google.maps.LatLng(40.69, -73.95);
        </jsand:code>
        <jsand:script src="googlemaps-geolocation.js"/>
</jsand:sandbox>
```

Evaluation on legacy scripts

OWASP
The Open Web Application Security Project

- Google Analytics ✓
  - Needs 1 client-side JS AST transformation
- Google Maps ✓
  - Needs support for dynamic script loading
  - Needs 3 client-side JS AST transformation
- JQuery ✓

Demo available at http://demo-jsand.websand.eu/

DEMO

CONCLUSION

JavaScript inclusion

- Most common way of integrating 3rd party JavaScript
  - More than 88% of websites integrate 3rd party scripts
  - Google is the absolute #1 script provider
- Malicious or compromised script providers obtain full control over websites on which they are integrated
  - E.g. qTip2, googlesyndycatio.com, blogtoos.us, …

Existing mitigation techniques

OWASP
The Open Web Application Security Project

- None of them can be integrated seamlessly
  - Require browser modifications
  - Require server-side processing
  - Require re-architecting the application
  - Have restrictions on JS the language features

- Showed some insights in 2 promising directions
  - iFrame/CSP based sandboxing
  - Server-driven sandboxing with JSand

Acknowledgements

OWASP
The Open Web Application Security Project

- The work is partially funded by the European FP7 projects WebSand, STREWS and NESSoS.

SEVENTH FRAMEWORK PROGRAMME

WebSand

NESSoS

STREWS

- With the financial support from the Prevention of and Fight against Crime Programme of the European Union.

b·ccentre
BELGIAN CYBERCRIME CENTRE OF EXCELLENCE
FOR TRAINING, RESEARCH & EDUCATION