We're struggling to keep up

A brief history of Browser Security Features

about:frederik

Frederik Braun

FluxFingers Team Member

Security Engineer at Mozilla

fbraun@mozilla.com

https://frederik-braun.com

@freddyb

Why am I here?

02 *The Internet is a global public resource that must remain open and accessible.*

03 *The Internet must enrich the lives of individual human beings.*

04 *Individuals' security and privacy on the Internet are fundamental and must not be treated as optional.*

05 *Individuals must have the ability to shape the Internet and their own experiences on it.*

06 *The effectiveness of the Internet as a public resource depends upon interoperability (protocols, data formats, content), innovation and decentralized participation worldwide.*

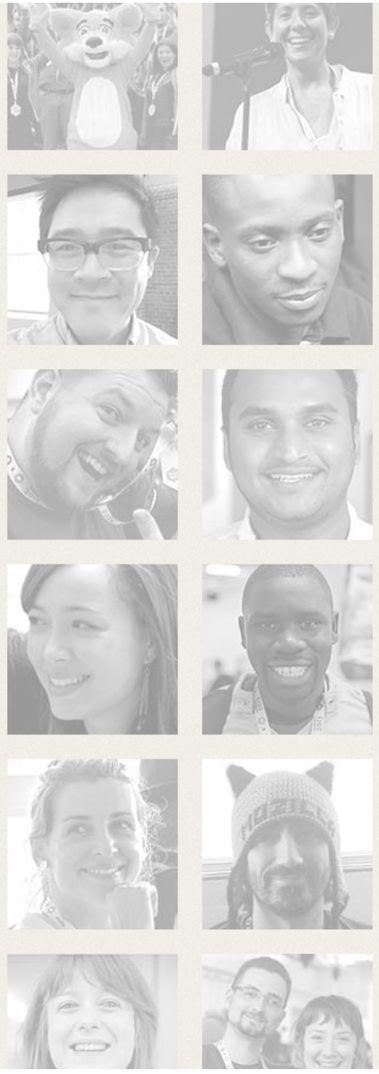


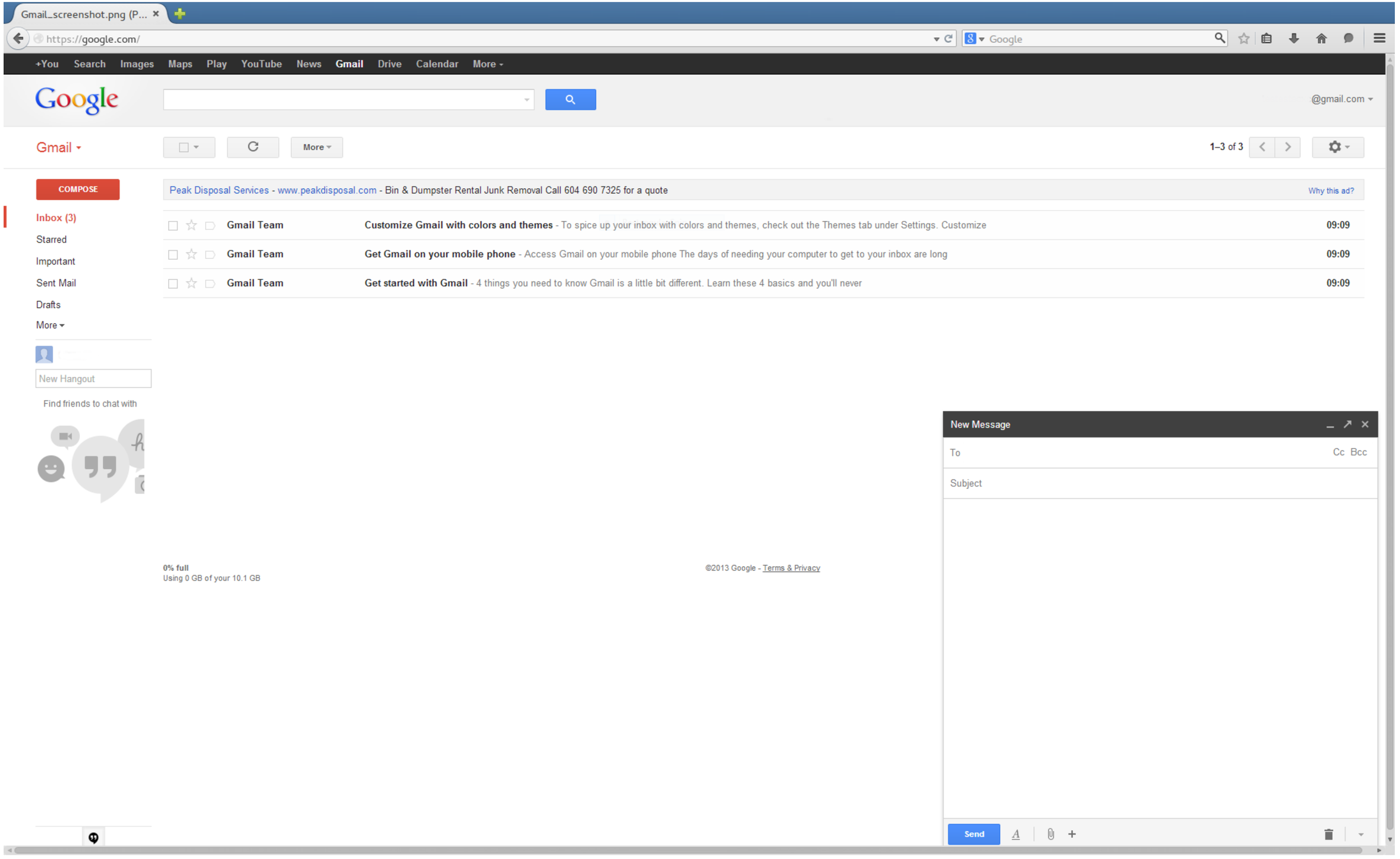
Table Of Contents

Introduction

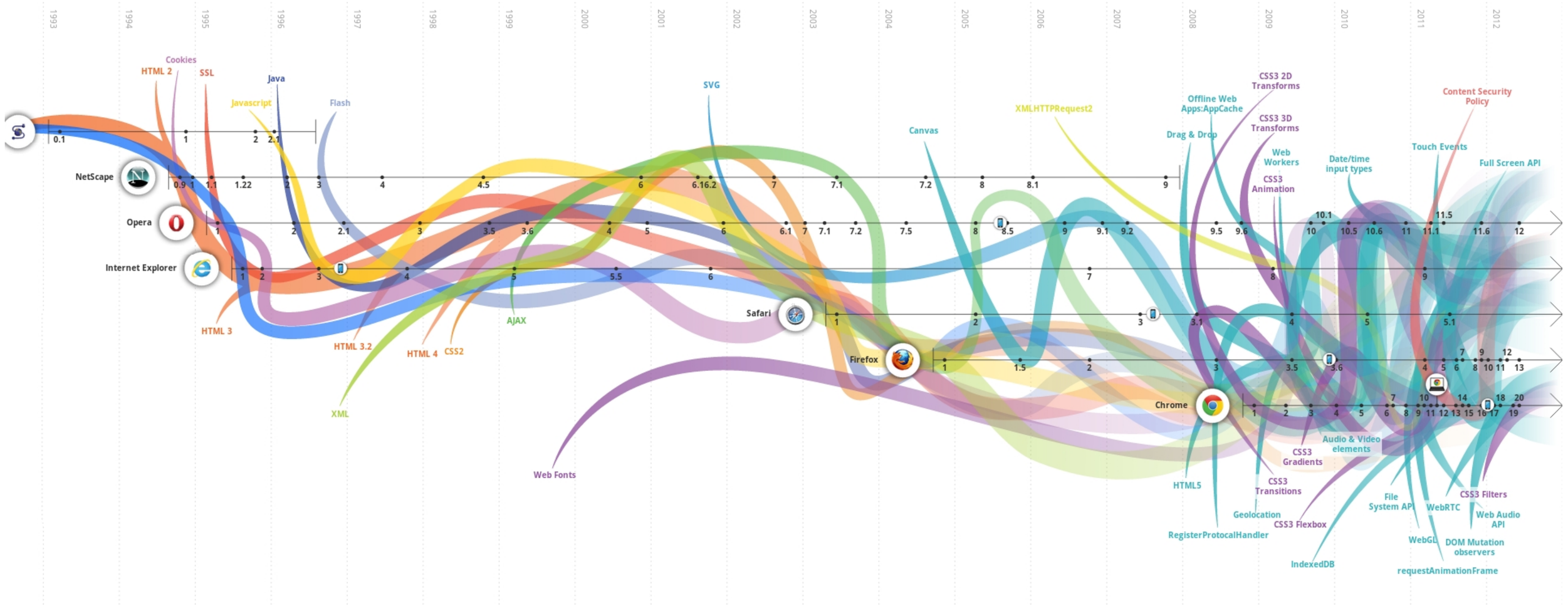
The Web and the Browser

The Web is the platform


Yahoo - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://yahoo.com/
Go Links
Calendar Messenger Check Email
YAHOO!
What's New Personalize Help
Yahoo! Careers
find a job, post your resume
Get your Web address now! YAHOO! Domains CLICK HERE!
Y! Greetings
spook a friend
Search advanced search
Autos - 2002 Car Guide, Blue Book Pricing, Classifieds, Auctions, Consumer Reports, 360° Interior Views
Shop Auctions · Autos · Classifieds · Shopping · Travel · Yellow Pgs · Maps Media Finance/Quotes · News · Sports · Weather
Connect Careers · Chat · Clubs · GeoCities · Greetings · Mail · Members · Messenger · Mobile · Personals · People Search · Photos
Personal Addr Book · Briefcase · Calendar · My Yahoo! · PayDirect Fun Games · Kids · Movies · Music · Radio · TV more...
Make a Connection with Yahoo! Personals
I'm a Man seeking a Woman
Enter City, State or ZIP:
Find My Match!
Take a Tour of Yahoo! Personals - where millions of singles meet!
Arts & Humanities
Literature, Photography...
News & Media
Full Coverage, Newspapers, TV...
Business & Economy
B2B, Finance, Shopping, Jobs...
Recreation & Sports
Sports, Travel, Autos, Outdoors...
Computers & Internet
Internet, WWW, Software, Games...
Reference
Libraries, Dictionaries, Quotations...
Education
College and University, K-12...
Regional
Countries, Regions, US States...
Entertainment
Cool Links, Movies, Humor, Music...
Science
Animals, Astronomy, Engineering...
Government
Elections, Military, Law, Taxes...
Social Science
Archaeology, Economics, Languages...
Health
Medicine, Diseases, Drugs, Fitness...
Society & Culture
People, Environment, Religion...
powered by COMPAQ
In the News
U.S. jets bomb Taliban targets
Some U.S. troops in Afghanistan
U.S. accuses Northrop Grumman of fraud in defense contracts
Scientists record dual auroras
Bush throws out first pitch in NY
World Series · NBA · NHL · NFL
more...
Marketplace
Register for free webcast by Dr. Stephen R. Covey
New music from Jewel - pre-order CD, watch video
Shrek DVD & Plush Gift Set
Y! Express - expedite your web site listing into Yahoo!'s directory
Yahoo! Shopping - Gift Center
Broadcast Events
FinanceVision - live market coverage M-F 9am-5pm ET
Elton John - artist of the month
Done
Internet


Gmail_screenshot.png (P...
https://google.com/
Google
+You Search Images Maps Play YouTube News Gmail Drive Calendar More
Google
@gmail.com
Gmail
More
1–3 of 3
COMPOSE
Inbox (3)
Starred
Important
Sent Mail
Drafts
More
New Hangout
Find friends to chat with
Peak Disposal Services - www.peakdisposal.com - Bin & Dumpster Rental Junk Removal Call 604 690 7325 for a quote
Why this ad?
Gmail Team Customize Gmail with colors and themes - To spice up your inbox with colors and themes, check out the Themes tab under Settings. Customize 09:09
Gmail Team Get Gmail on your mobile phone - Access Gmail on your mobile phone The days of needing your computer to get to your inbox are long 09:09
Gmail Team Get started with Gmail - 4 things you need to know Gmail is a little bit different. Learn these 4 basics and you'll never 09:09
0% full
Using 0 GB of your 10.1 GB
©2013 Google - Terms & Privacy
New Message
To
Cc Bcc
Subject
Send

The Evolution of the Web



Timeline from http://www.evolutionoftheweb.com/

XSS is the new Buffer Overflow

Browsers are Everywhere

Screenshot from a http://techadvisor.co.uk BMW Video

The Past

“Web browsers' access control policies have evolved piecemeal in an ad-hoc fashion with the introduction of new browser features. This has resulted in numerous incoherencies“

Kapil Singh, Alexander Moshchuk, Helen J. Wang, and Wenke Lee. *On the incoherencies in web browser access control policies,* (Security and Privacy (SP), 2010 IEEE Symposium)

Piecemeal or “Whac a Mole”

Picture from “Bob B. Brown” on Flickr -
https://secure.flickr.com/photos/beleaveme/

The Past (in a nutshell)

Problem	Band Aid
HTTP is Stateless	Cookies (1994)
Cookies are plain-text	HTTPS (1994)
HTTPS is opt-in	Strict Transport Security (HSTS) in 2009
HSTS needs first-contact	Browser preloads HSTS in 2012

Summarizing

The Present

Secure Hosting of Uploaded Content

Fixing Cross-Site Scripting

How to include potentially untrusted content

The Principle of *not-so-much* Authority

Give frames access to the things that are really only necessary

Iframe Sandbox

```
<iframe src="http://example.com" sandbox />
```

Iframe Sandbox

```
<iframe src="http://example.com"
    sandbox="allow-scripts" />
```

XSS is still hard to fix

My name is `<script>alert(1)</script>`

Fixing XSS once and for all?

Content Security Policy (CSP)!

Applying CSP

```
<script>
// fancy animation
</script>
```

➡

```
<script src="fancy_animation.js"></script>
```

Using CSP

```
Content-Security-Policy: default-src: 'self';
 script-src: 'self' https://cdn.example.com/;
                object-src: 'none'
```

CSP 2.0: Nonces for Dynamic Inline Scripts

```
script-src: 'nonce-blahblahblah'
```

&

```
<script nonce="blahblahblah">
// dynamic generated JavaScript…
</script>
```

CSP 2.0: Hashes for static third-party Scripts

```
script-src: 'sha256-blahblahblah'
```

&

```
<script>
// static, third-party JavaScript…
</script>
```

Free CSP Introduction & Development Tools!

Towards a Post-XSS World

Mike West
https://mikewest.org
G+: mkw.st/+
Twitter: @mikewest

Slides: https://mkw.st/r/jsconfeu13

Making CSP Work for You

Mark Goodwin

https://computerist.org
Twitter: @mr_goodwin

Slides: http://mzl.la/1p6w4vh

The Future

HTTPS Public Key Pinning

Fixing DOM-Based Cross-Site Scripting

Untrusted, but oh so fast CDNs

The Situation with Certificate Authorities is not great

Request: Add Honest Achmed's root certificate

This is a request to add the CA root certificate for Honest Achmed's Used Cars and Certificates. The requested information as per the CA information checklist is as follows:

Name: Honest Achmed's Used Cars and Certificates

Website URL: www.honestachmed.dyndns.org

Organizational type: Individual (Achmed, and possibly his cousin Mustafa, who knows a bit about computers).

Primary market / customer base: Absolutely anyone who'll give us money.

Impact to Mozilla Users: Achmed's business plan is to sell a sufficiently large number of certificates as quickly as possible in order to become too big to fail (see "regulatory capture"), at which point most of the rest of this application will become irrelevant.

Why do we allow *every CA out there* to create a valid certificate for all domains?

HTTPS Public Key Pinning (HPKP)

```
Public-Key-Pins: pin-sha256="…";
 max-age=15768000; includeSubDomains
```

Wait a moment, we can fix XSS with Content Security Policy, but what about DOM-based XSS?

DOM Based XSS

```
el.innerHTML = "<input type='text' value='" +
        searchFromURLParams() + "' />"
```

Style Injections & Content Exfiltration

Scriptless Attacks

Stealing the Pie without touching the Sill

Mario Heiderich, Felix Schuster, Marcus Niemietz,
Jörg Schwenk, Thorsten Holz
ACM CCS 2012

HGI / Chair for Network and Data Security
Ruhr-University Bochum
mario.heiderich@rub.de || @0x6D6172696F

ECMAScript6 Template Strings: Interpolation

```
var x = 1;
var y = 2;
`${ x } + ${ y } = ${ x + y}`  // "1 + 2 = 3"
```

Examples from the ESWiki at tc39wiki.calculist.org

ECMAScript6 Template Strings: Multiline

```
var s = `a
    b
    c`;
assert(s == 'a\n    b\n    c');
```

Examples from the ESWiki at tc39wiki.calculist.org

ECMAScript6 Template Strings: Tagging

```
function tag(strings, ...values) {
  assert(strings[0] == 'a');
  assert(strings[1] == 'b');
  assert(values[0] == '42');
  Return 'whatever';
}
tag `a${ 42 }b` // "whatever"
```

Examples from the ESWiki at tc39wiki.calculist.org

ECMAScript6 Template Strings: Tagging

```
function tag(strings, ...values) {
  assert(strings[0] == 'a');
  assert(strings[1] == 'b');
  assert(values[0] == '42');
  Return 'whatever';
}
tag `a${ 42 }b` // "whatever"
```

This gives us an array of all Interpolated values!

Examples from the ESWiki at tc39wiki.calculist.org

DEMO

Let's look at this JS REPL for the DEMO

Speed trumps Security

```
<script src="//code.jquery.com/jquery-1.11.0.min.js"></script>
```

Locking it down with Subresource Integrity

```
<script src="//code.jquery.com/jquery-1.11.0.min.js"
integrity="ni:///sha-256;C6CB9UYIS9UJeqinPHWTHVqh_E1uhG5Twh-
Y5qFQmYg?ct=application/javascript"></script>
```

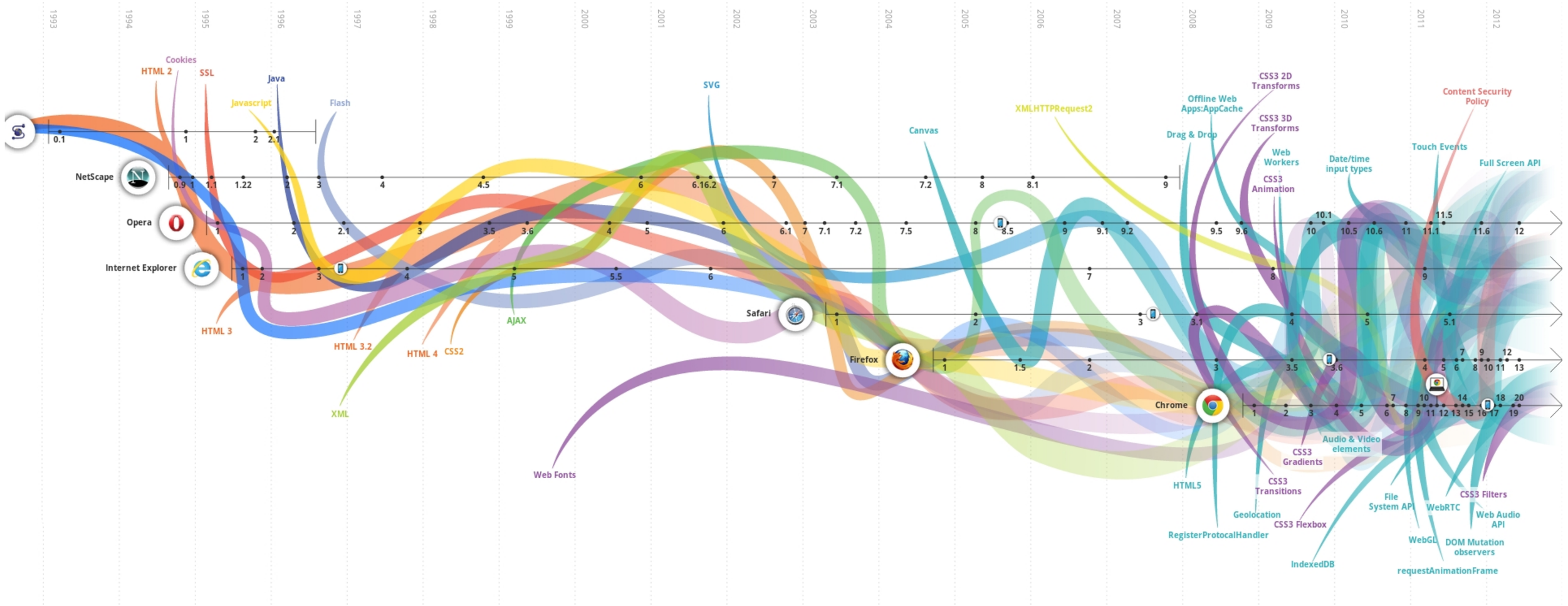
Subresource Integrity and Fallbacks

```
<script src="/static/lib/jquery-1.11.0.min.js"
noncanonical-src="//code.jquery.com/jquery-1.11.0.min.js"
integrity="ni:///sha-256;C6CB9UYIS9UJeqinPHWTHVqh_E1uhG5Twh-
Y5qFQmYg?ct=application/javascript"></script>
```

Conclusion

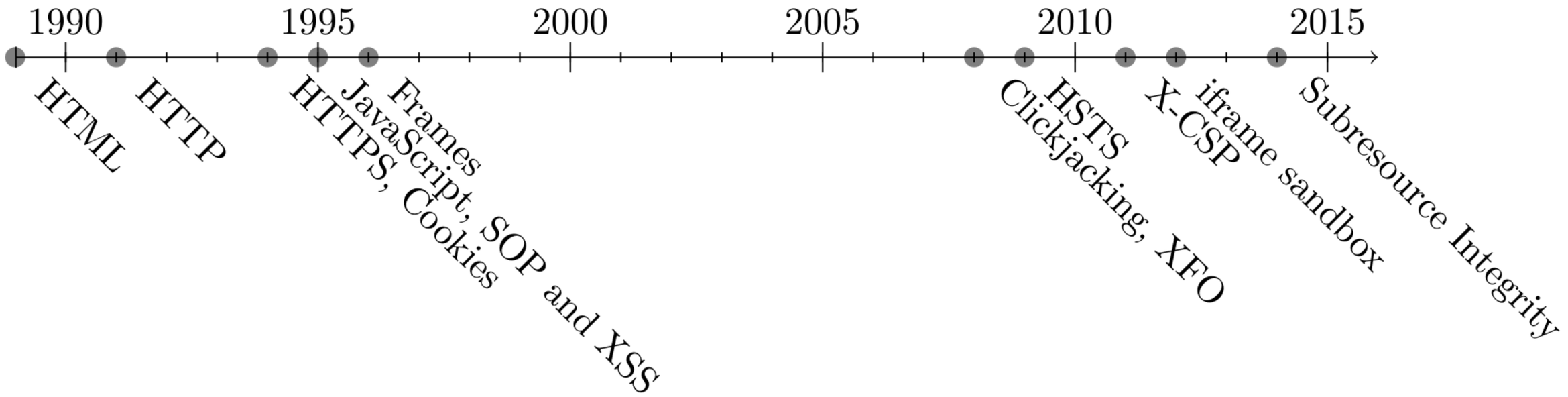
The Browser can aid the Website

Conclusion

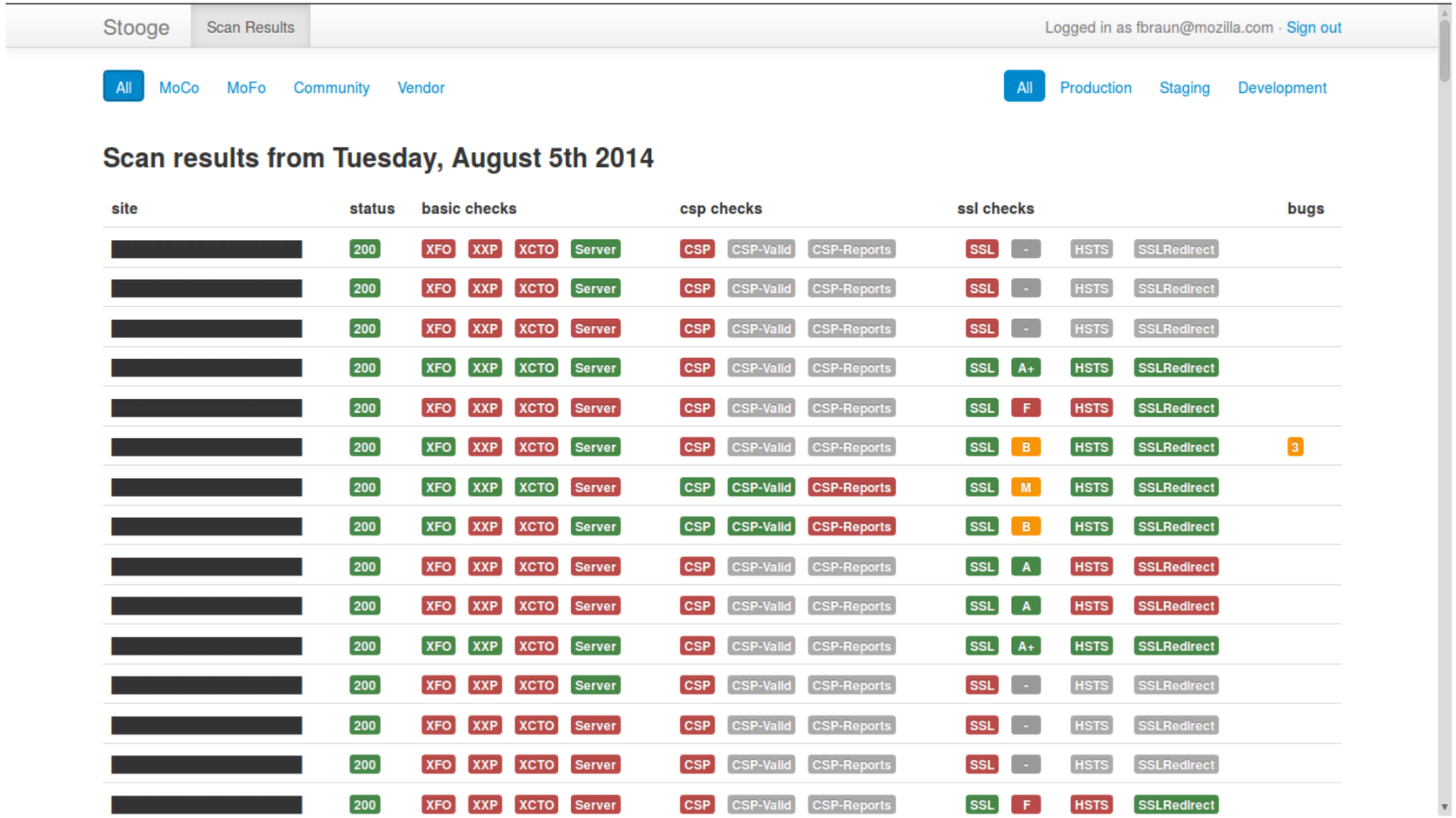


Timeline from http://www.evolutionoftheweb.com/

The Evolution of Web Security



github.com/st3fan/moz-stooge



github.com/st3fan/moz-stooge

Thank you for listening!

Frederik Braun

fbraun@mozilla.com

@freddyb

#security on irc.mozilla.org

Obligatory Red Panda photo by Wikipedia user Aconcagua, CC-BY-SA-3.0

Further reading and Thanks

- Mike West and Brad Hill have given presentations about browser security features in the past.
- Stefan Arentz explained Web Security 101.
- Mark Goodwin talked about how to make Content Security Policy (CSP) work for you at SteelCon in Sheffield.
- Devdatta Akhawe et al. wrote about Privilege Separation for HTML5 Applications
- Mario Heiderich's research & white papers
- My Blog post on X-Frame-Options (joint work with Mario Heiderich)
- This presentation also borrows from my diploma thesis which itself builds on great research as listed in its Reference section (p. 67).
- Thanks to Pascal “Pepo” Szewczyk, Tim Taubert, Romain Gauthier, and Christian Heilmann for reviewing.
- Sequence Diagrams made with https://bramp.github.io/js-sequence-diagrams/