

Emerging Web Application Security Standards

Scott Helme

**The Internet is insecure.
We're working to fix it.**

***While trying not to break it too much!**



Transport security is largely a solved problem

1. Deploy encryption
2. Use good configuration
3. Deploy HSTS
4. Deploy HPKP
(only if you're big)

Google Transparency Report

How much email was encrypted in transit?



Generally speaking, use of encryption in transit increases over time, as more providers enable and maintain their support. Factors such as varying volumes of email may explain other fluctuations.

Outbound



73%

Messages from Gmail to other providers.

100%
70%
40%
10%

Jan 2014

Apr 2014

Jul 2014

Sep 2016: 85%

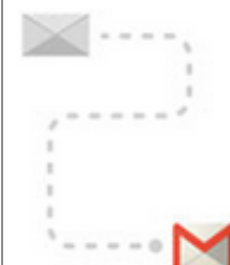
View Past

30 days

90 days

1 year

Inbound



58%

Messages from other providers to Gmail.

100%
70%
40%
10%

Jan 2014

Apr 2014

Jul 2014

Sep 2016: 75%

View Past

30 days

90 days

1 year



Firefox®

46.43%

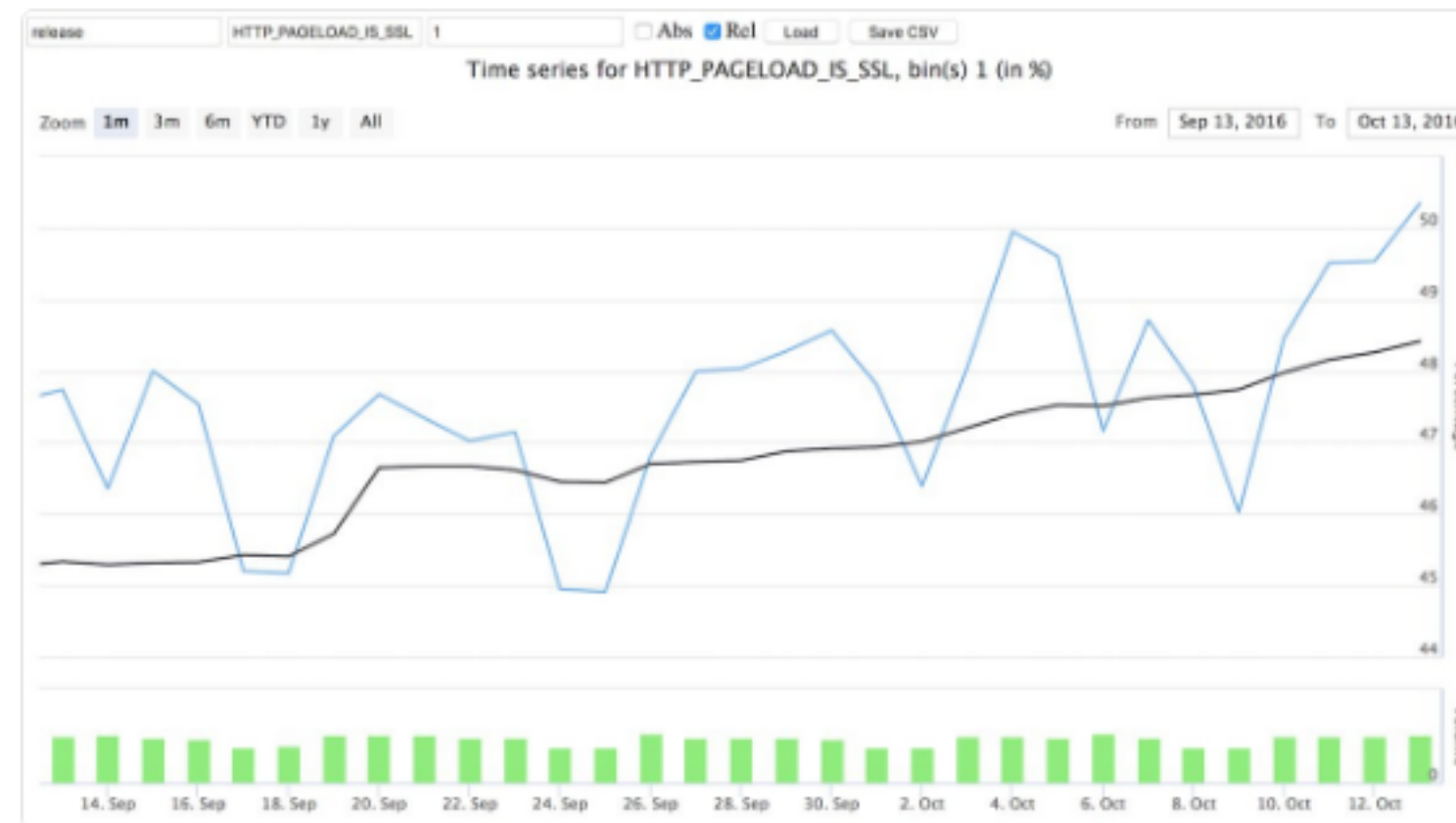
Initial page over HTTPS

Source: April King, <https://marumari.github.io/letsencrypt-overview/>



Following

Yesterday, for the first time, [@Mozilla](#) telemetry shows more than 50% of page loads were encrypted with HTTPS.



RETWEETS

974

LIKES

1,073



6:10 PM - 14 Oct 2016



 974

 1.1K



Google Chrome



Treatment of HTTP pages with
password or credit card form fields:

Current (Chrome 53)

📘 login.example.com

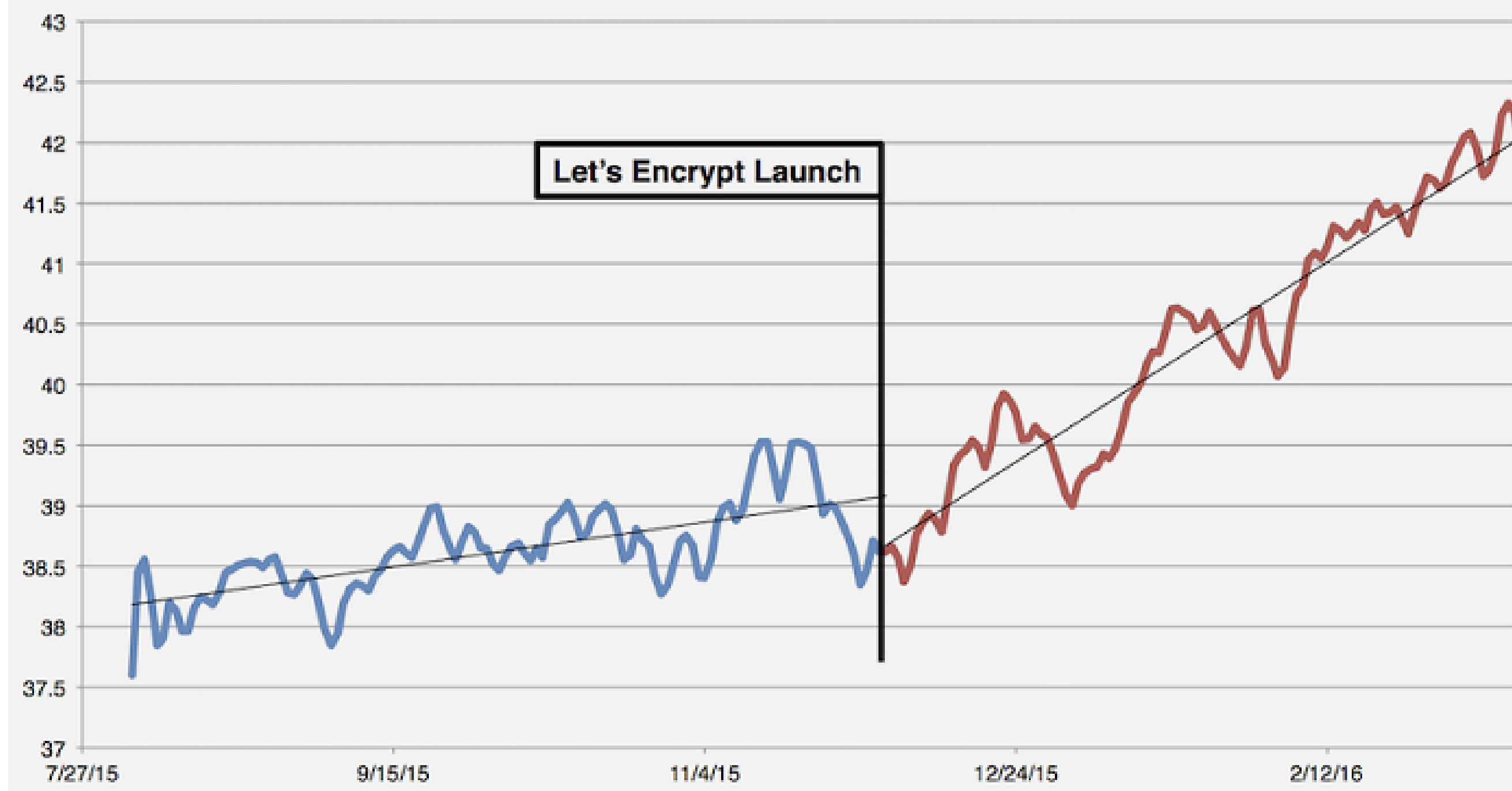
Jan. 2017 (Chrome 56)

📘 Not secure | login.example.com



Let's Encrypt

Percentage of Firefox Pageloads using HTTPS (15-day moving average)



TLS 1.3

- Complete overhaul
- Removes cruft
- Improves performance
- New protocol for the next 20+ years

HTTP Strict Transport Security

Strict-Transport-Security:

max-age=31536000; includeSubDomains; preload

Enter a domain for the HSTS preload list:

example.com

Check status and eligibility

Information

This form is used to submit domains for inclusion in Chrome's [HTTP Strict Transport Security \(HSTS\)](#) preload list. This is a list of sites that are hardcoded into Chrome as being HTTPS only.

Most major browsers (Chrome, [Firefox](#), Opera, Safari, [IE 11 and Edge](#)) also have HSTS preload lists based on the Chrome list. (See the [HSTS compatibility matrix](#).)

Submission Requirements

If a site sends the `preload` directive in an HSTS header, it is considered be requesting inclusion in the preload list and may be submitted via the form on this site.

In order to be accepted to the HSTS preload list through this form, your site must satisfy the following set of requirements:

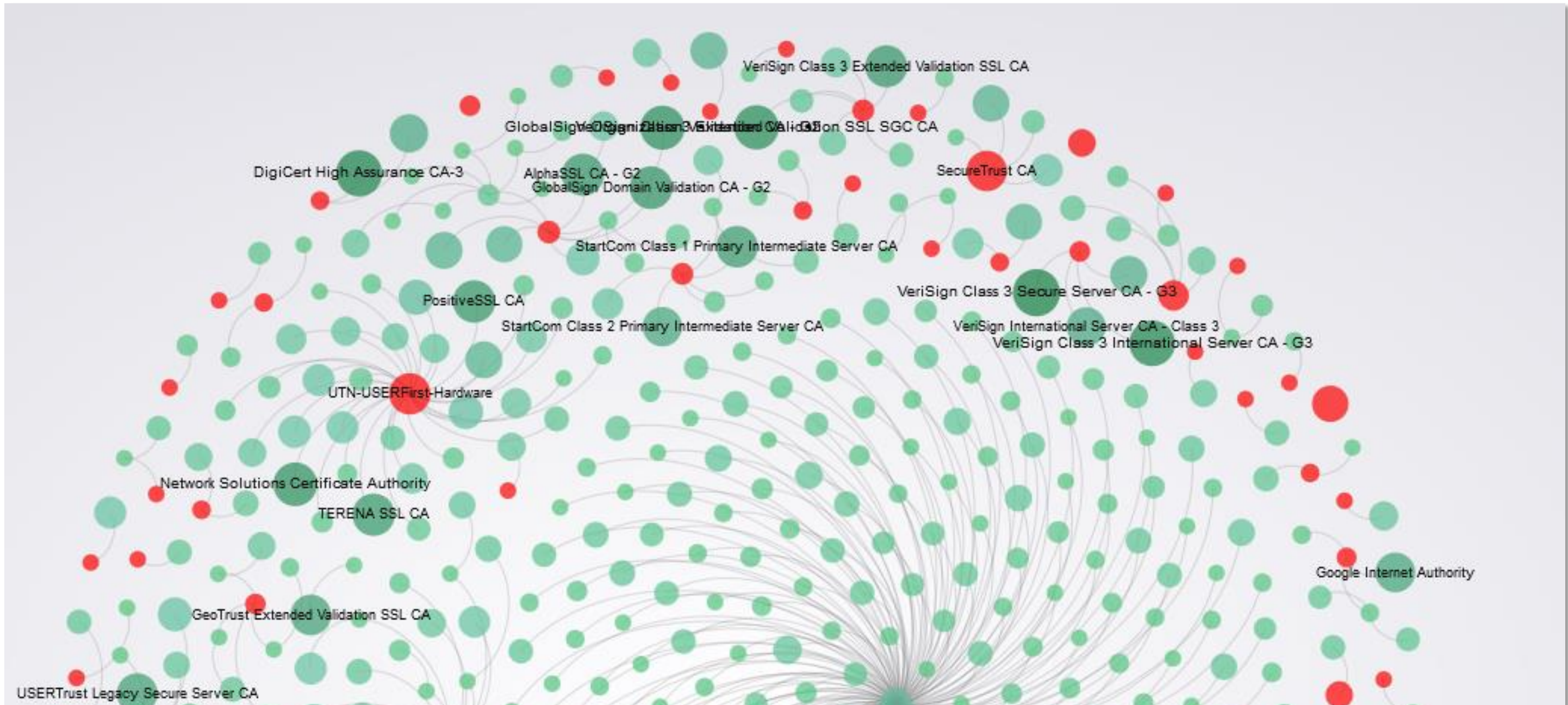
1. Serve a valid **certificate**.
2. **Redirect** from HTTP to HTTPS on the same host.
3. Serve all **subdomains** over HTTPS.
 - In particular, you must support HTTPS for the `www` subdomain if a DNS record for that subdomain exists.

hstspreload.appspot.com

HTTP Public Key Pinning

Public-Key-Pins:

max-age=2592000; pin-sha256="HASH"; pin-sha256="HASH"





Revocation doesn't work.

Must-staple certificates to the rescue!

Certification Authority Authorization (CAA)

New DNS RR type (257) that specifies which CA is allowed to issue certificates for your domain name.

example.org. CAA 1 issue "letsencrypt.org"



Source: CloudFlare



DNSSEC & DANE

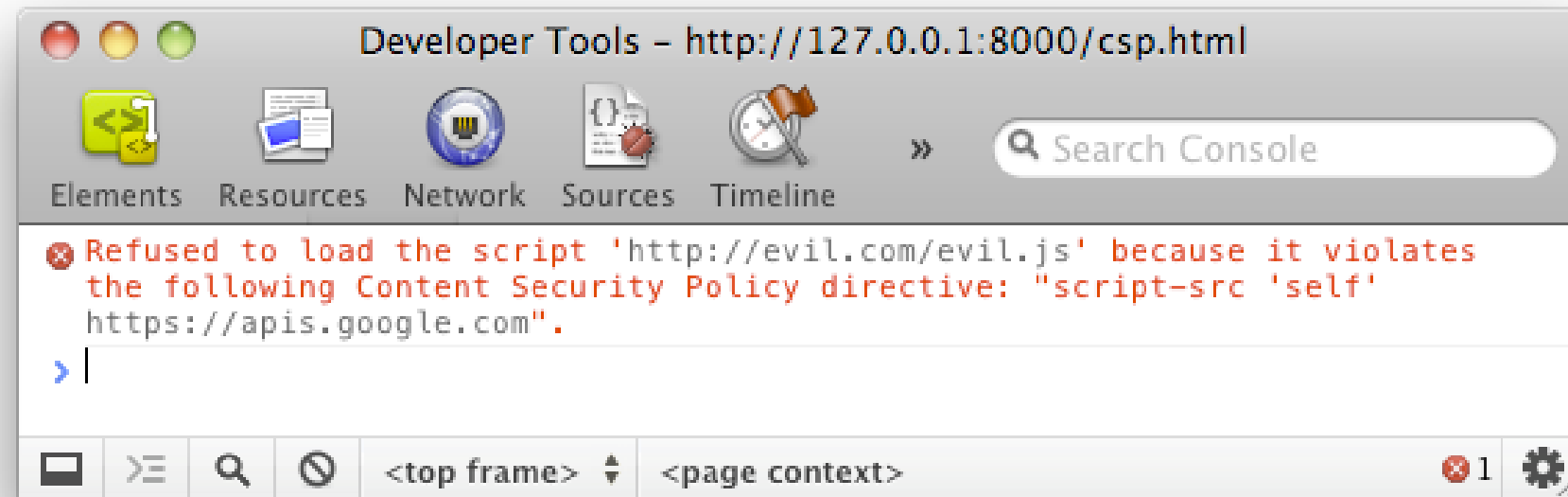
Love/Hate

Content Security Policy



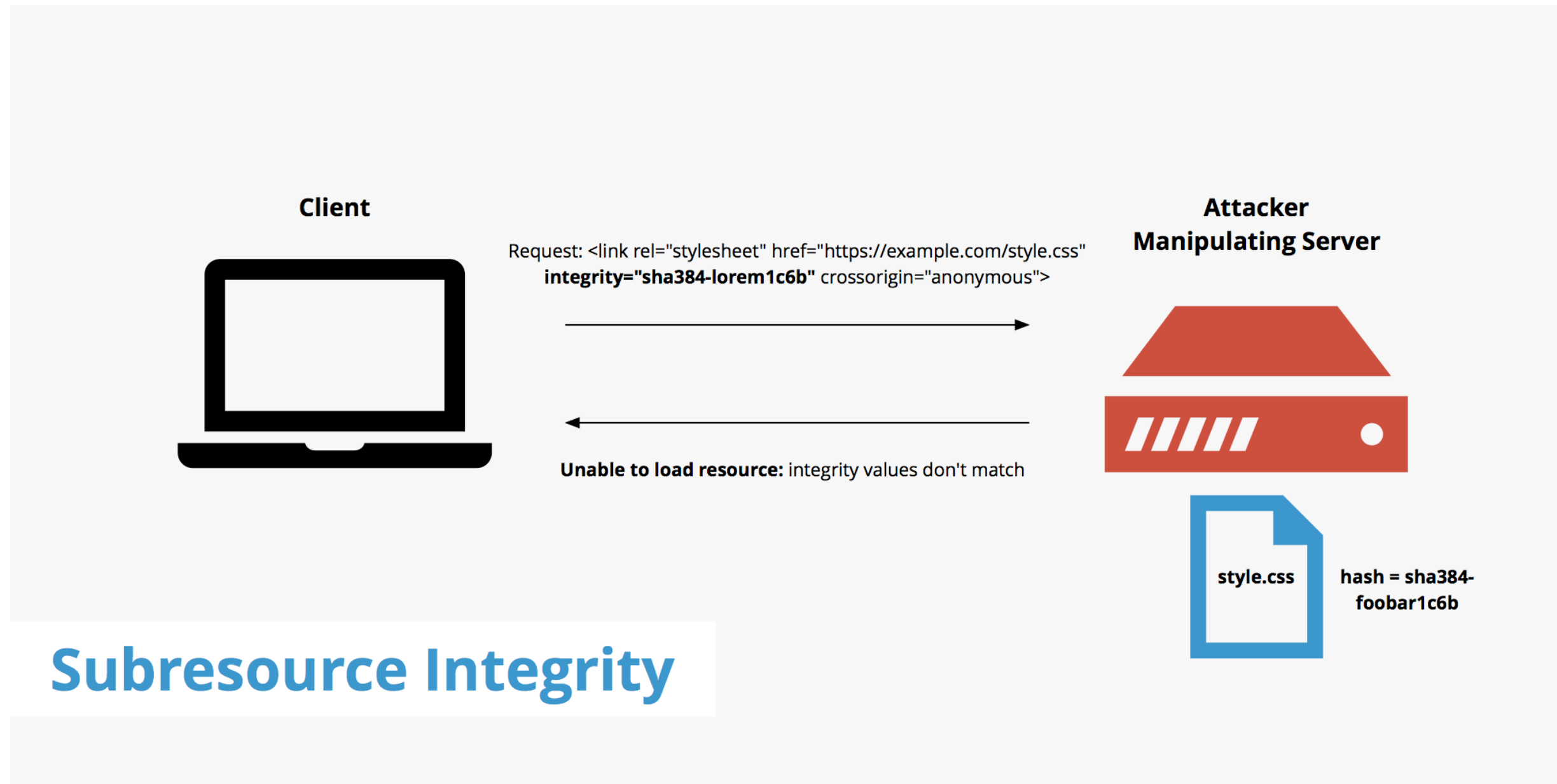
Source: <http://www.messynessychic.com/2015/07/17/colombias-beloved-jeeps-loaded-with-everything-but-the-kitchen-sink/>

Content Security Policy



- Restrict inline script, styles, and eval()
- Restrict resource loading
- Restrict framing
- Prevent mixed content

Subresource Integrity



Source: <https://www.keycdn.com/support/subresource-integrity/>

Subresource Integrity

```
<script  
src="//cdn.example.com/jquery.min.js"  
crossorigin="anonymous"  
integrity="sha256-[hash]">  
</script>
```


Same-site cookies

Cookie prefixes



- `__Host-`
- `__Secure-`
- `SameSite=Strict`
- `SameSite=Lax`

A few things I didn't have time to talk about...

- CORS/ACAO
- XCTO
- XFO
- XDO
- XXP
- SPF
- DKIM
- DMARC
- SMTP STS
- Mixed-Content



How do we solve this?

Let's take a look

Hardenize

Continuous monitoring and assessment



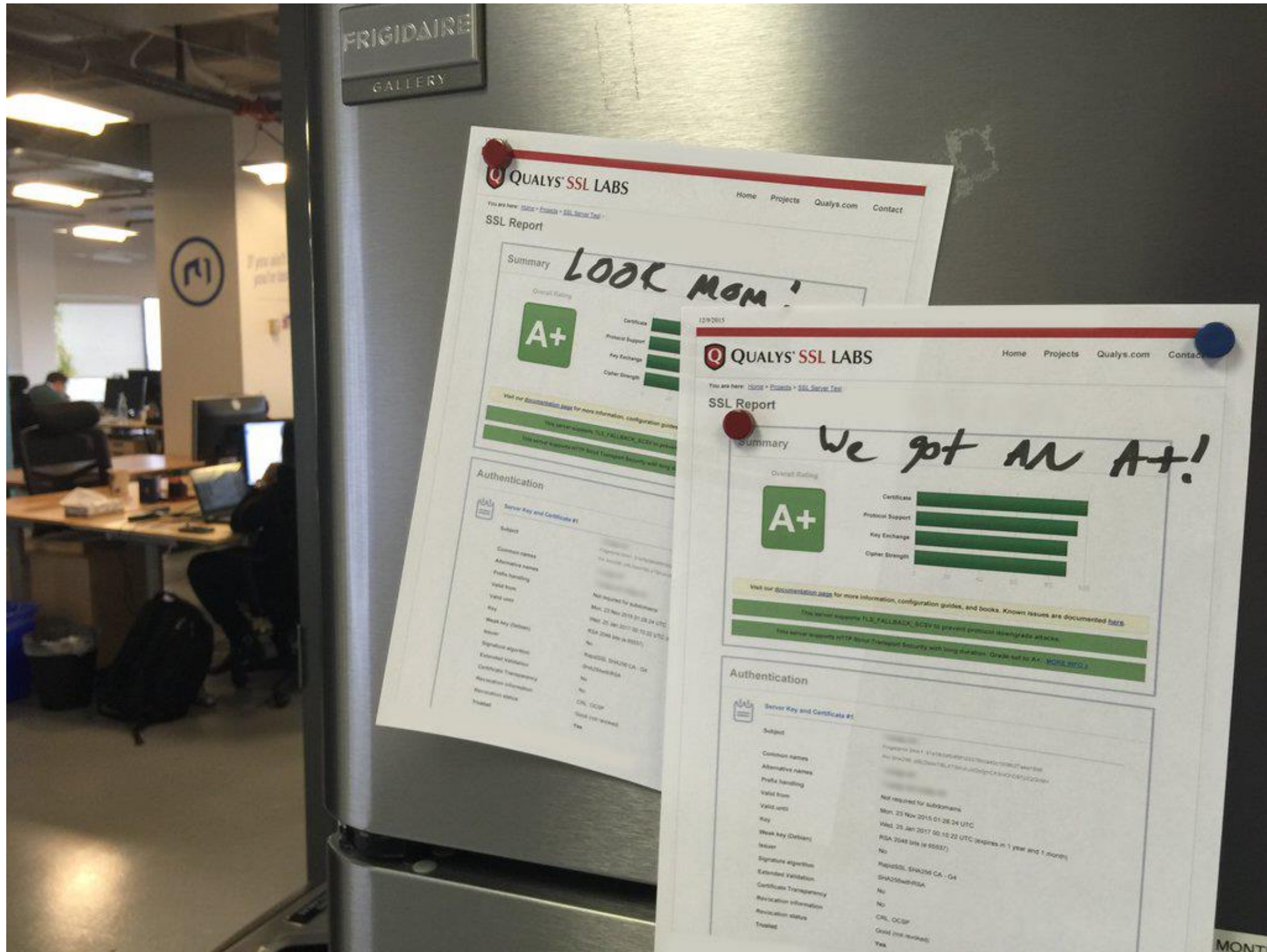
**Less than 1% of top
web sites use modern
security features**

**WHOIS, DNS, DNSSEC, DANE, CAA, SMTP,
STARTTLS, CAs, X.509, SPF, DKIM,
DMARC, IPv4, IPv6, HTTP/2, SSL, TLS,
HSTS, CSP, HPKP, RC4, SHA, Cookies,
Mixed content, SRI,
Privacy, and many more...**

**The future [of security] is already here, but
it's not evenly distributed yet**

William Gibson, adapted

**Make security
easy and fun!**





Follow

Thanks to [@Scott_Helme](#)'s eye opening talk, I made it from grade F to grade A with just a few lines of .htaccess. [#fronteers](#) ›

securityheaders.io

HomeAbout

Scan your site now

Scan

Hide results Follow redirects

Security Report Summary

F

Site: (Scan again over https)

IP Address:

Report Time: 07 Oct 2016 10:10:47 UTC

Report Short URL:

Headers: Content-Security-Policy X-Frame-Options X-XSS-Protection X-Content-Type-Options

securityheaders.io

HomeAbout

Scan your site now

Scan

Hide results Follow redirects

Security Report Summary

A

Site:

IP Address:

Report Time: 07 Oct 2016 10:21:50 UTC

Report Short URL:

Headers: X-Frame-Options Content-Security-Policy Strict-Transport-Security X-XSS-Protection X-Content-Type-Options Public-Key-Pins

RETWEETS

7

LIKES

26



11:30 AM - 7 Oct 2016




7



26






HOMEFEATURESABOUTSIGN IN


We'll help you deploy the latest security standards


With so many security features to deploy and services to configure, most organisations struggle to understand where they are and where they need to be. Our continuous monitoring and assessment service cuts through the fluff and enables you to have exactly the security you want.

We are currently in early stages of development. To gain early access and stay informed about our progress, request an invite below.

REQUEST INVITE >

© 2016 Hardenize / hello@hardenize.com / [Twitter](#)

REPLAY INTRO

**www.feistyduck.com**

7 Jul 2016 10:41 UTC ↺[Tweet](#)[Email](#)

Domainfeistyduck.com

✓ WHOIS

✓ Name servers

✗ DNSSEC

⚠ CAA

Emailfeistyduck.com

SECURE TRANSPORT

✓ TLS

✓ Certificates

✗ DANE



AUTHENTICATION AND POLICY

✓ SPF

Preview

Easy to
understand and
communicate

The report is
broken down to
show key areas

**longdomainname.com**
Test time: 14 Jan 2016 12:41:45 UTC  [Tweet](#)


Poor93/125


2 ERRORS


3 WARNINGS


4 IMPROVEMENT OPPORTUNITIES

Domain Name

 Locked


 Name Server Configuration


 DNSSEC


 Certification Authority Authorization

Email


SECURE TRANSPORT


 Encryption


 Certificate

 TLS Configuration

AUTHENTICATION AND POLICY

 SPF

 DKIM

 DMARC



Deceptively
simple

More detail
available on
demand

Hundreds of
complex tests
under the hood

⚠️ TLS Configuration



AUTHENTICATION AND POLICY

✓ SPF



✓ DKIM



✓ DMARC



WWW

PROTOCOLS

✓ HTTP/2



✓ IPv6



SECURE TRANSPORT

✓ Certificate



⚠️ TLS Configuration



✓ Secure Cookies



✗ Mixed Content



MODERN SECURITY FEATURES

✓ Strict Transport Security



✓ Public Key Pinning



✓ Content Security Policy



✓ DANE



APPLICATION SECURITY

✓ Third Party Trust



✓ Privacy



✓ Security Headers



Hardenize Community Dashboard

Home

[HOW TO CONTRIBUTE](#)

Hardenize Community Dashboards are Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus finibus luctus massa, eu ultricies diam rutrum at. Sed pretium pretium tempus. Vestibulum imperdiet risus sit amet rutrum venenatis. Vivamus et odio porta, varius lectus a, viverra elit. Cras dolor nunc, porta vel nulla finibus, congue pulvinar purus. Quisque fringilla magna in nunc efficitur dapibus. Vivamus sit amet nulla arcu.

**Online gaming
websites**

45 sites

UK Internet Providers

18 sites

**US Telecom
Companies**

9 sites

Webmail Providers

45 sites

Social Network Sites

27 sites

Google Web Services

57 sites

SaaS Providers

45 sites

Banks in the UK

34 sites

Top 50 Websites

Online gaming

Insurance companies

Daily Newspapers in

Hardenize Community Dashboard

Banks in the UK

[HOW TO CONTRIBUTE](#)

Website	DOMAIN NAME			EMAIL		WWW					Score
	Domain name locked	DNSSEC	Certification Authority Authorisation	Encryption	Certificate	HTTP/2 protocol	Certificate	Strict Transport Security	Content Security Policy	Security Headers	
Beautiful Pillows www.domainname.com	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	Good
Super Something www.domainname.com	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	Good
C Company Name www.domainname.com	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	Poor
Guacamole Xtreme Sportz www.domainname.com	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	Good
Papillon un Pomme de terre www.domainname.com	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	Poor
Four Potatoe Consulting www.domainname.com	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	Good
Errorsoft Security Plc www.domainname.com	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	Good
Legitimate Evasion Co. www.domainname.com	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	Poor



www.hardenize.com