

Mission Accomplished?

HTTPS Security after DigiNotar

Johanna Amann*

ICSI / LBL / Corelight

Oliver Gasser*

Technical University of Munich

Quirin Scheitle*

Technical University of Munich

Lexi Brent

The University of Sydney

Georg Carle

Technical University of Munich

Ralph Holz

The University of Sydney

* Joint First Authorship



THE UNIVERSITY OF
SYDNEY



TLS/HTTPS Security Extensions

- Certificate Transparency
- HSTS (HTTP Strict Transport Security)
- HPKP (HTTP Public Key Pinning)
- SCSV (TLS Fallback Signaling Cipher Suite Value)
- CAA (Certificate Authority Authorization)
- DANE-TLSA (DNS Based Authentication of Named Entities)

Methodology

- Active & passive scans
- Active measurements from 2 continents
 - Largest domain-based TLS scan so far
 - More than 192 million domains
- Passive measurements on 3 continents
 - More than 2.4 billion observed TLS connections

TLS/HTTPS Security Extensions

- **Certificate Transparency**
- HSTS (HTTP Strict Transport Security)
- HPKP (HTTP Public Key Pinning)
- SCSV (TLS Fallback Signaling Cipher Suite Value)
- CAA (Certificate Authority Authorization)
- DANE-TLSA (DNS Based Authentication of Named Entities)

Certificate Transparency

CA

Issues Certificates

CT Log

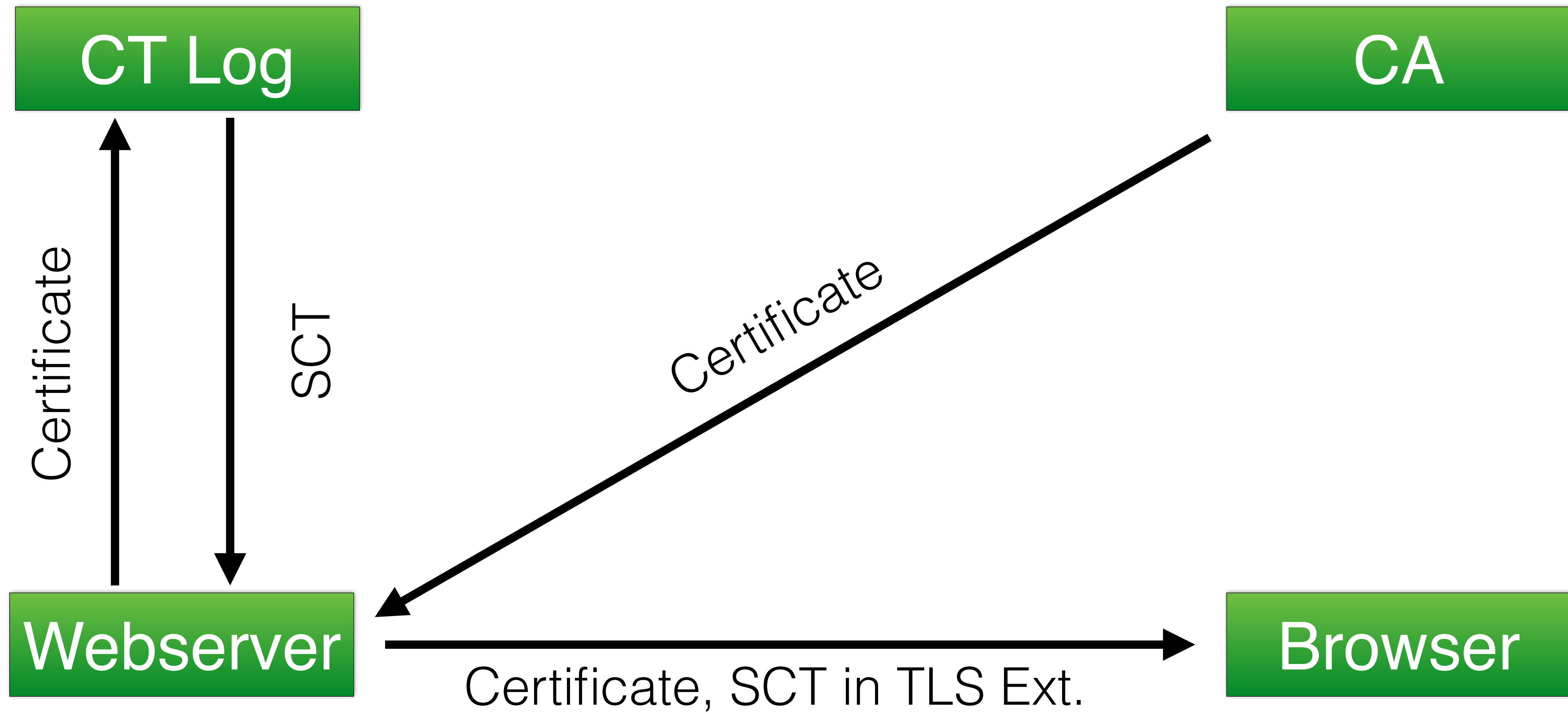
Provides publicly auditable, append-only Log of certificates

Also provides proof of inclusion

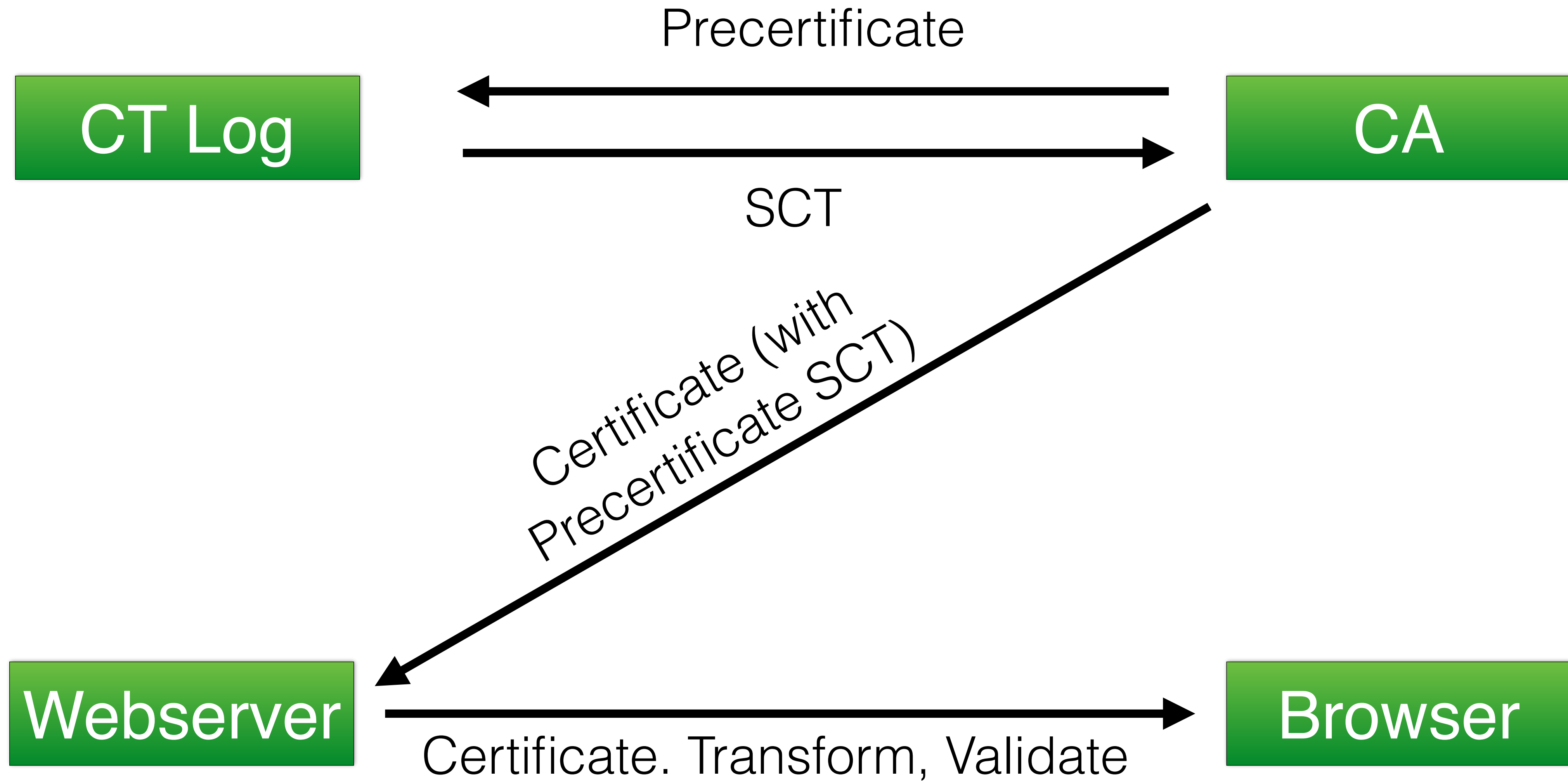
Browser

Verifies proof of inclusion

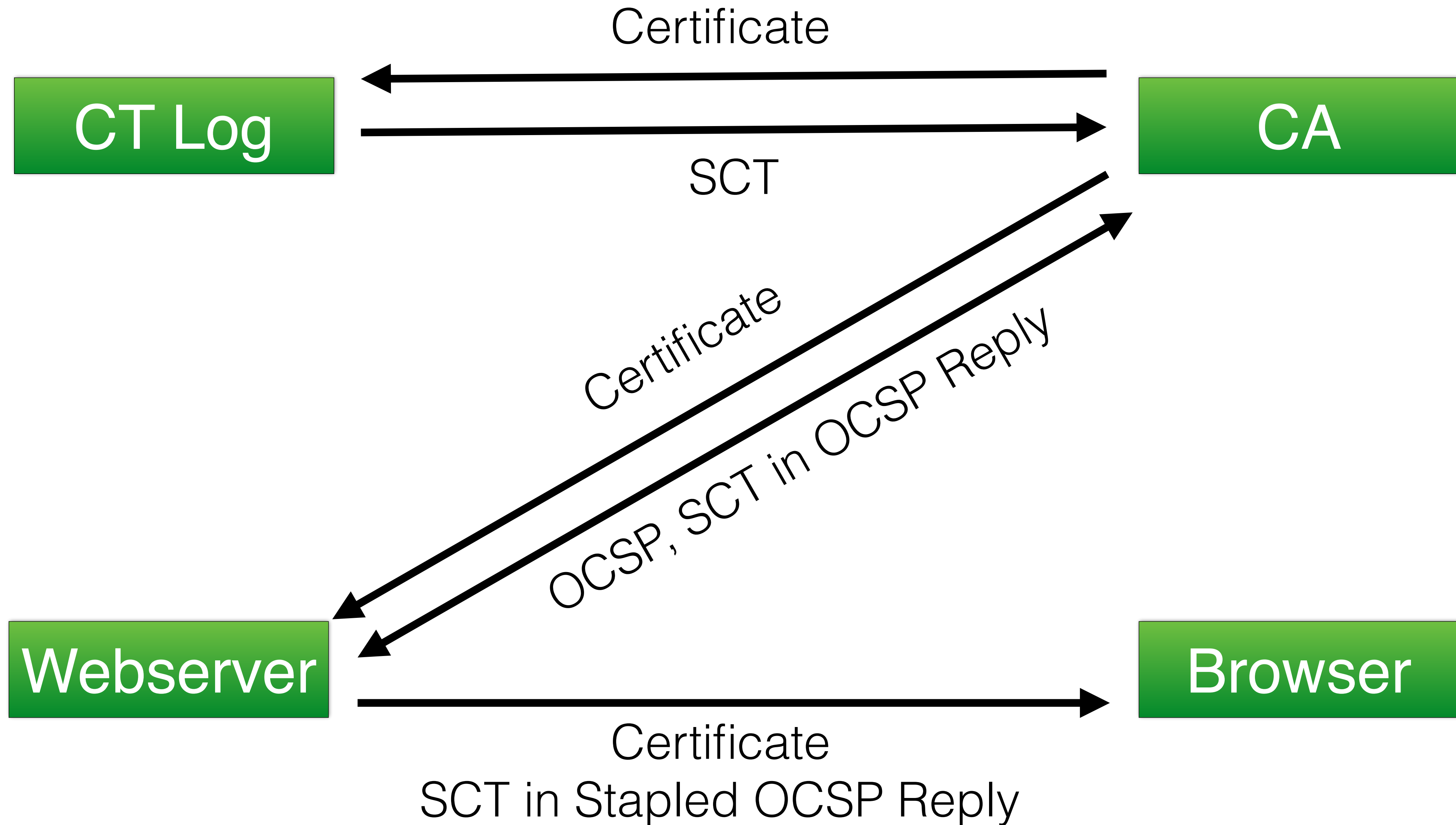
Certificate Transparency - TLS Ext.



Certificate Transparency - x509



Certificate Transparency - OCSP



SCT Statistics - Active

Sydney v4

Munich v4

Munich v6

Domains we could connect to

55.7M

58.0M

5.1M

Domains with SCT

6.8M

6.8M

357K

... via X509

6.7M

6.8M

344K

... via TLS Ext.

27.6K

27.2K

12.9K

... via OCSP

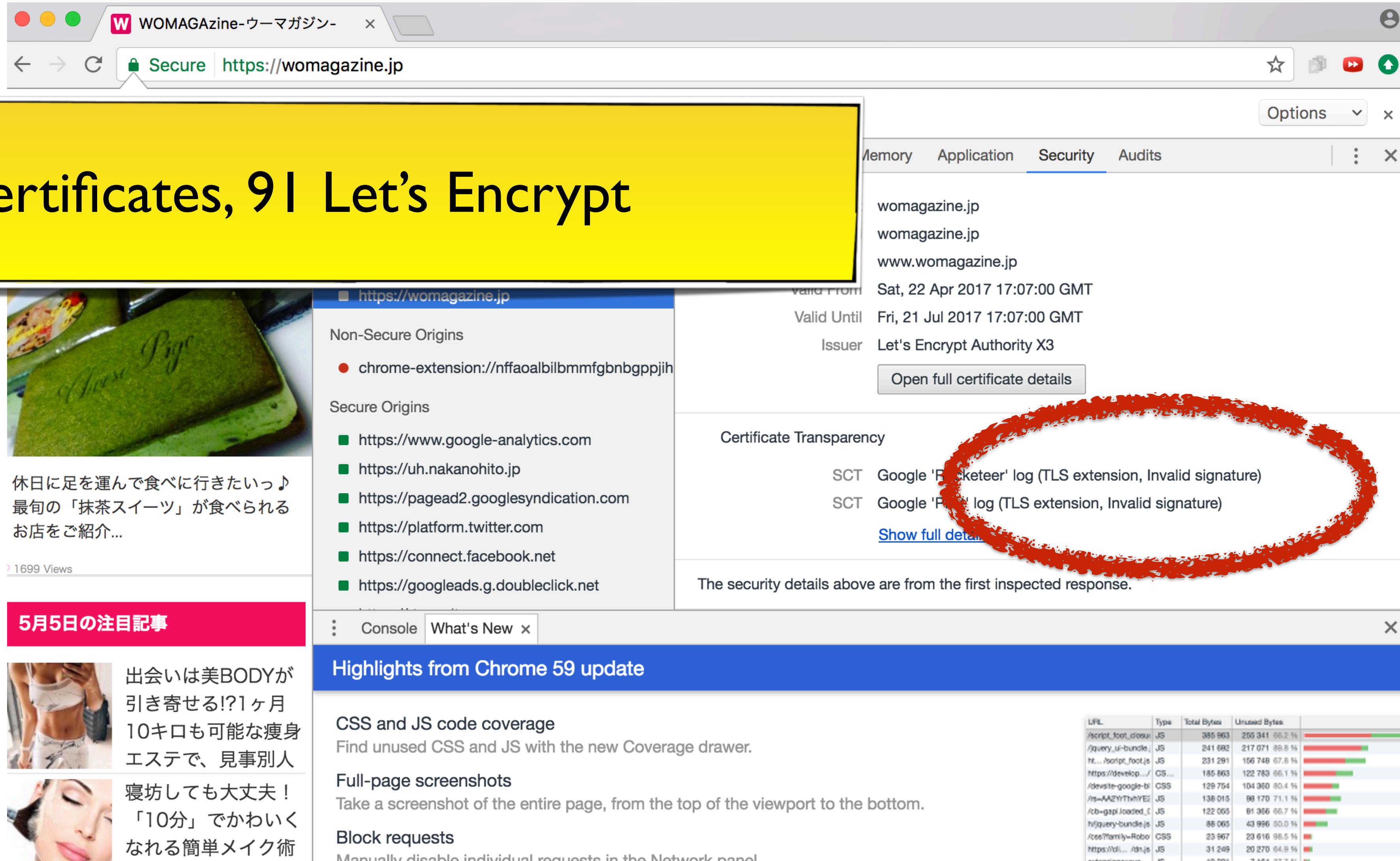
180

188

3

SCT via TLS Ext. is Error-Prone

105 Certificates, 91 Let's Encrypt



WOMAGazine-ウーマガジン- x

Secure https://womagazine.jp

Options x

Memory Application Security Audits

womagazine.jp
womagazine.jp
www.womagazine.jp

Valid From Sat, 22 Apr 2017 17:07:00 GMT
Valid Until Fri, 21 Jul 2017 17:07:00 GMT
Issuer Let's Encrypt Authority X3

Open full certificate details

Certificate Transparency

SCT Google 'P...sketeer' log (TLS extension, Invalid signature)
SCT Google 'P...sketeer' log (TLS extension, Invalid signature)

Show full details

The security details above are from the first inspected response.

Non-Secure Origins

- chrome-extension://nffaoalbilbmmfngbnbgppjih

Secure Origins

- https://www.google-analytics.com
- https://uh.nakanohito.jp
- https://pagead2.googlesyndication.com
- https://platform.twitter.com
- https://connect.facebook.net
- https://googleads.g.doubleclick.net

5月5日の注目記事

出会は美BODYが引き寄せる!?1ヶ月10キロも可能な痩身エステで、見事別人

寝坊しても大丈夫!「10分」でかわいくなれる簡単メイク術

Highlights from Chrome 59 update

CSS and JS code coverage
Find unused CSS and JS with the new Coverage drawer.

Full-page screenshots
Take a screenshot of the entire page, from the top of the viewport to the bottom.

Block requests
Manually disable individual requests in the Network panel

URL	Type	Total Bytes	Unused Bytes	Unused %
/script_foot_close.js	JS	385 963	255 341	66.2 %
/query_ui_bundle.js	JS	241 682	217 071	89.8 %
ht.../script_foot.js	JS	231 291	156 748	67.8 %
https://develop.../	CS...	185 663	122 783	66.1 %
/devsite-google-bi	CSS	129 754	104 360	80.4 %
/rs=AAZYThhYEg	JS	138 015	88 170	71.1 %
/cb-gapiLoaded.js	JS	122 065	81 366	66.7 %
h/jquery-bundle.js	JS	88 065	43 996	50.0 %
/ces?family=Robo	CSS	23 967	23 616	98.5 %
https://dl.../dn.js	JS	31 249	20 270	64.9 %
autofocus-mouse	JS	10 000	7 426	74.3 %

Invalid embedded SCT?

Folkehelseinstituttet - FHI

Secure | <https://www.fhi.no>

This page is in Norwegian Would you like to translate it? Nope Translate Options

folkehelse

MENY

Overview

Main Origin

- https://www.fhi.no

Secure Origins

- https://www.google-analytics.com
- https://www.googletagmanager.com
- https://www.googleadservices.com
- https://connect.facebook.net
- https://googleads.g.doubleclick.net
- https://www.google.com
- https://www.facebook.com

Unknown / Canceled

- https://code.jquery.com

Subject www.fhi.no

SAN www.fhi.no
admin.fhi.no
[Show more \(4 total\)](#)

Valid From Thu, 09 Jun 2016 12:32:36 GMT

Valid Until Sat, 09 Jun 2018 21:59:00 GMT

Issuer Buypass Class 3 CA 2

[Open full certificate details](#)

Certificate Transparency

- SCT Google 'Aviator' log (Embedded in certificate, Invalid signature)
- SCT Venafi log (Embedded in certificate, Invalid signature)
- SCT Symantec log (Embedded in certificate, Invalid signature)

[Show full details](#)

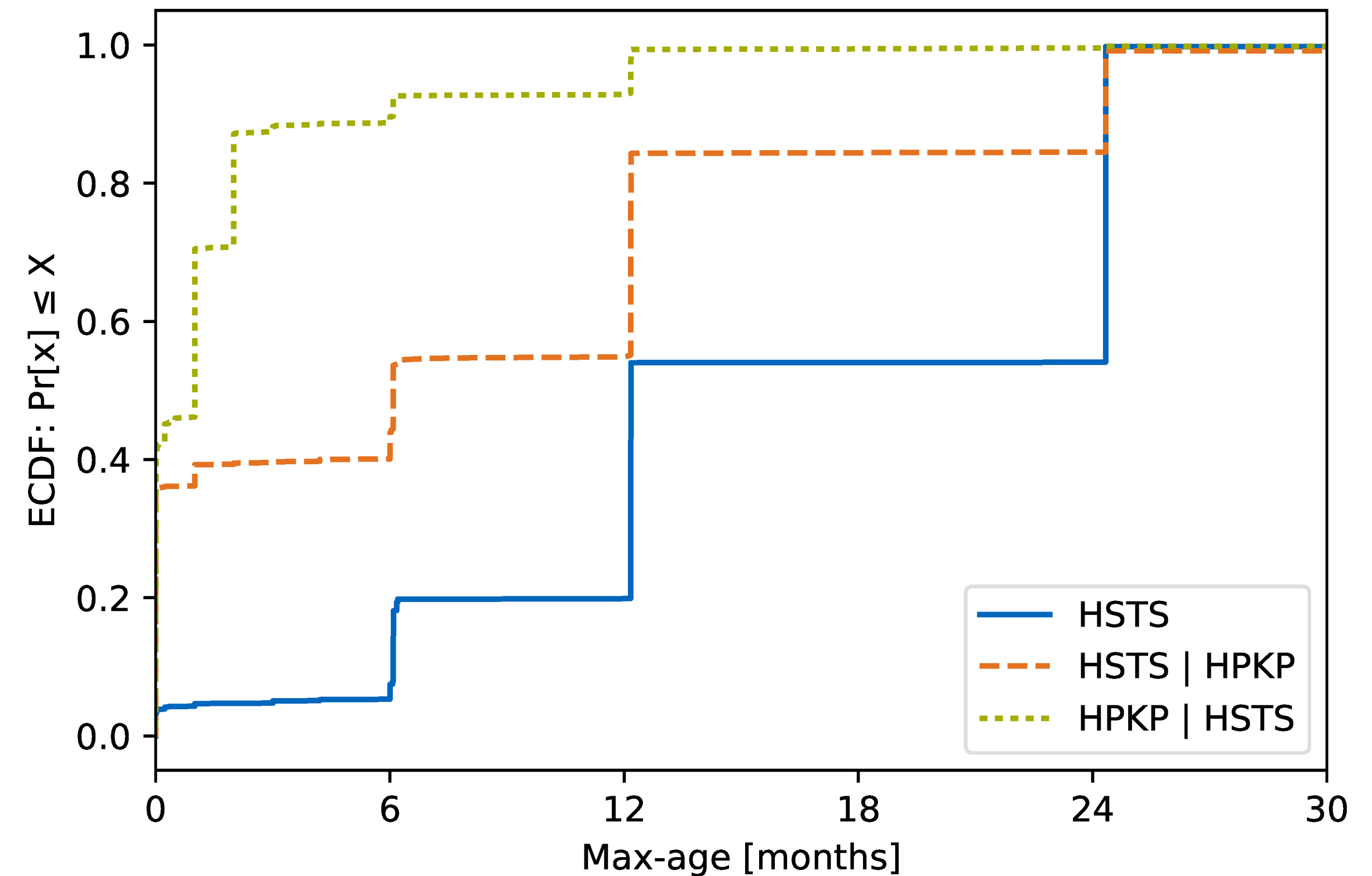
The security details above are from the first inspected response.

TLS/HTTPS Security Extensions

- Certificate Transparency
- **HSTS (HTTP Strict Transport Security)**
- **HPKP (HTTP Public Key Pinning)**
- SCSV (TLS Fallback Signaling Cipher Suite Value)
- CAA (Certificate Authority Authorization)
- DANE-TLSA (DNS Based Authentication of Named Entities)

HSTS, HPKP: Much longer max-age values for HSTS

- HSTS: ~3.5% of domains
- 0.2% send incorrect headers (misspellings, wrong attributes, ...)
- HPKP: ~0.02% of domains (6,181)
- 41 invalid



TLS/HTTPS Security Extensions

- Certificate Transparency
- HSTS (HTTP Strict Transport Security)
- HPKP (HTTP Public Key Pinning)
- **SCSV (TLS Fallback Signaling Cipher Suite Value)**
- CAA (Certificate Authority Authorization)
- DANE-TLSA (DNS Based Authentication of Named Entities)

SCSV

Automatically deployed when servers/libraries update

> 96% deployment

TLS/HTTPS Security Extensions

- Certificate Transparency
- HSTS (HTTP Strict Transport Security)
- HPKP (HTTP Public Key Pinning)
- SCSV (TLS Fallback Signaling Cipher Suite Value)
- **CAA (Certificate Authority Authorization)**
- **DANE-TLSA (DNS Based Authentication of Named Entities)**

Basically no deployment of CAA and TLSA as of April 2017

	SYD	MUC	Intersection	Top1M
CAA	3,243 (100%)	3,509 (100%)	3,057 (100%)	340 (100%)
signed	674 (21%)	899 (26%)	621 (20%)	53 (16%)
TLSA	1,697 (100%)	1,364 (100%)	1,246 (100%)	100 (100%)
signed	330 (78%)	1,042 (76%)	973 (78%)	89 (89%)

Deployment

Mechanism	Standard- ized	Deployment		Effort	Availability Risk
		Overall	Top 10K↓		
SCSV	2015	49.2M	6789	none	low
CT-x509	2013	7.0M	1788	none ²	none
HSTS	2012	0.9M	349	low	low
CT-TLS	2013	27,759	171	high	none
HPKP	2015	6616	156	high	high
HPKP PL.	2012 ¹	479	150	high	high
HSTS PL.	2012 ¹	23,539	144	medium	medium
CAA	2013	3057	20	medium	low
TLSA	2012	973	3	high	medium
CT-OCSP	2013	191	0	low	none

1: Preloading list first added to Chrome in 2012

2: Requires deployment effort on CA side and a new site certificate.

Deployment

Mechanism	Standard- ized	Deployment		Effort	Availability Risk
		Overall	Top 10K↓		
SCSV	2015	49.2M	6789	none	low
CT-x509	2013	7.0M	1788	none ²	none
HSTS	2012	0.9M	349	low	low
CT-TLS	2013	27,759	171	high	none
HPKP	2015	6616	156	high	high
HPKP PL.	2012 ¹	479	150	high	high
HSTS PL.	2012 ¹	23,539	144	medium	medium
CAA	2013	3057	20	medium	low
TLSA	2012	973	3	high	medium
CT-OCSP	2013	191	0	low	none

1: Preloading list first added to Chrome in 2012

2: Requires deployment effort on CA side and a new site certificate.

[blink-dev](#) ›

Intent To Deprecate And Remove: Public Key Pinning

31 posts by 14 authors  



Chris Palmer

Oct 27



Primary eng (and PM) emails

palmer@chromium.org, rsleeve@chromium.org, estark@chromium.org, agl@chromium.org

Summary

Deprecate support for public key pinning (PKP) in Chrome, and then remove it entirely.

This will first remove support for [HTTP-based PKP](#) (“dynamic pins”), in which the user-agent learns of pin-sets for hosts by HTTP headers. We would like to do this in Chrome 67, which is estimated to be released to Stable on 29 May 2018.

Finally, remove support for built-in PKP (“static pins”) at a point in the future when Chrome requires Certificate Transparency for all publicly-trusted certificates (not just newly-issued publicly-trusted certificates). (We don’t yet know when this will be.)

Summary

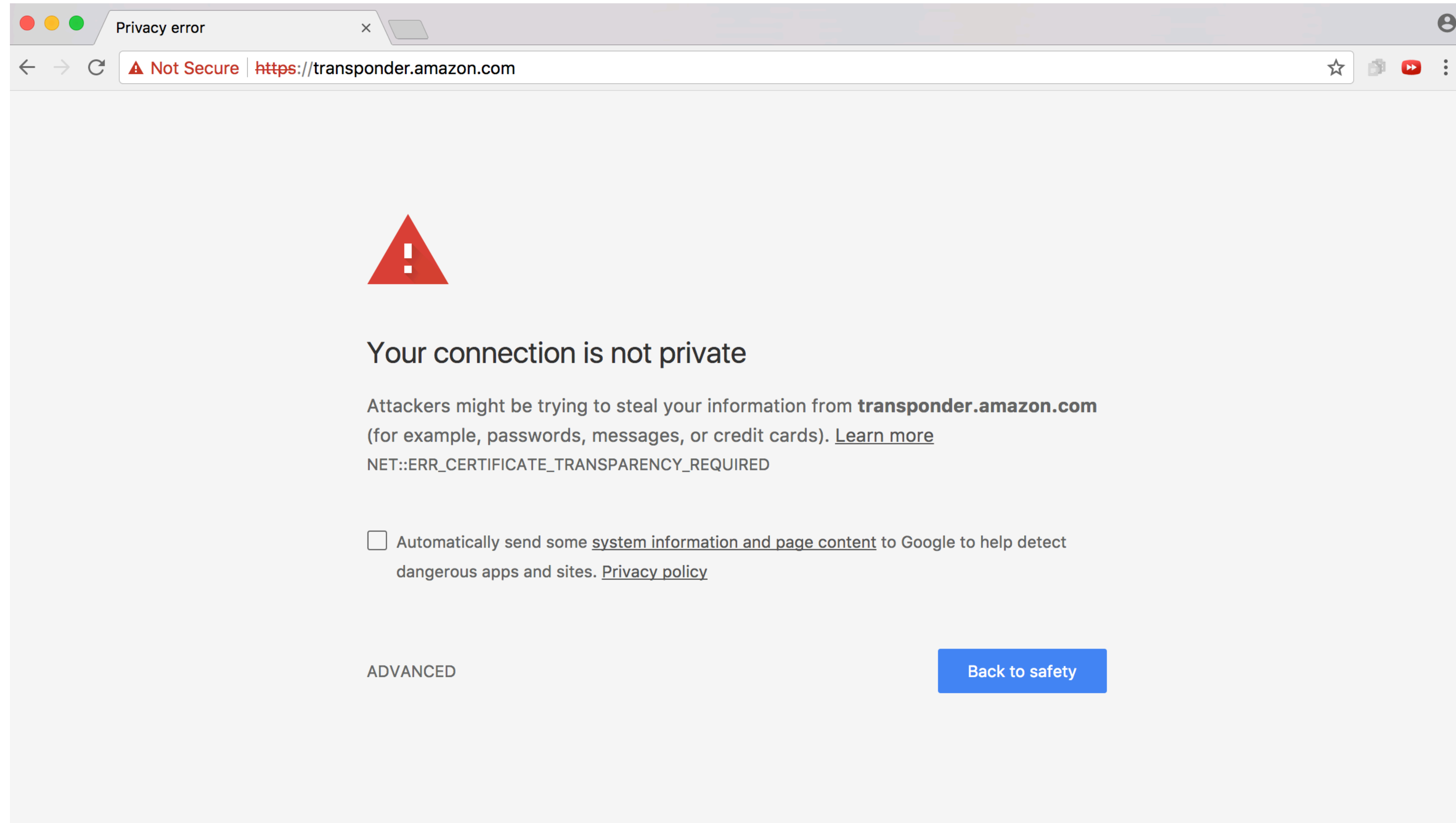
- Deployment status correlates with:
 - Configuration effort
 - Risk
 - Default deployment / settings work best
- Measurements from several sites have very similar results
 - One measurement location probably good enough in most cases

Community Contributions

- PCAPs of active scans
- Active scan results, CT database dumps
- Analysis Scripts (primarily Jupyter notebooks)
- Datasets: <https://mediatum.ub.tum.de/1377982>
- Software:
 - goscanner (HTTPS scanner): <https://github.com/tumi8/goscanner>
 - extended Bro TLS support (in master): <https://bro.org>

Backup

Log Operators



Log Operators

Active	Passive
Symantec log (81.26%)	Symantec log (62.78%)
Google 'Pilot' log (79.9%)	Google 'Rocketeer' log (58.6%)
Google 'Rocketeer' log (31.72%)	Google 'Pilot' log (58.48%)
DigiCert Log Server (26.96%)	Google 'Icarus' log (14.37%)
Google 'Aviator' log (25.67%)	Google 'Aviator' log (9.39%)
Google 'Skydiver' log (8.32%)	Vena log (7.47%)
Symantec VEGA log (3.98%)	WoSign ctlog (4.64%)
StartCom CT log (1.49%)	DigiCert Log Server (4.07%)
WoSign ctlog (0.67%)	Google 'Skydiver' log (1.7%)

SCT Statistics - Passive

	California	Munich	Sydney
Time	4/4-5/2	5/12-5/16	5/12-5/16
Conns	2.6B	287M	196M
Conns with SCT	779M	73M	58M
... in Cert	520M	58M	44M
... in TLS	248M	14M	14M
... in OCSP	156K	38K	31K
# v4 IPs	737K	344K	226K
# SCT v4 IPs	222K	102K	66K