

# Does Certificate Transparency Break the Web?

## Measuring Adoption and Error Rate

**Emily Stark**, Ryan Sleevi, Rijad Muminovic, Devon O'Brien,  
Eran Messeri, Adrienne Porter Felt, Brendan McMillion, Parisa Tabriz  
[estark@chromium.org](mailto:estark@chromium.org)



## Your connection is not private

Attackers might be trying to steal your information from **google.com** (for example, passwords, messages, or credit cards). [Learn more](#)

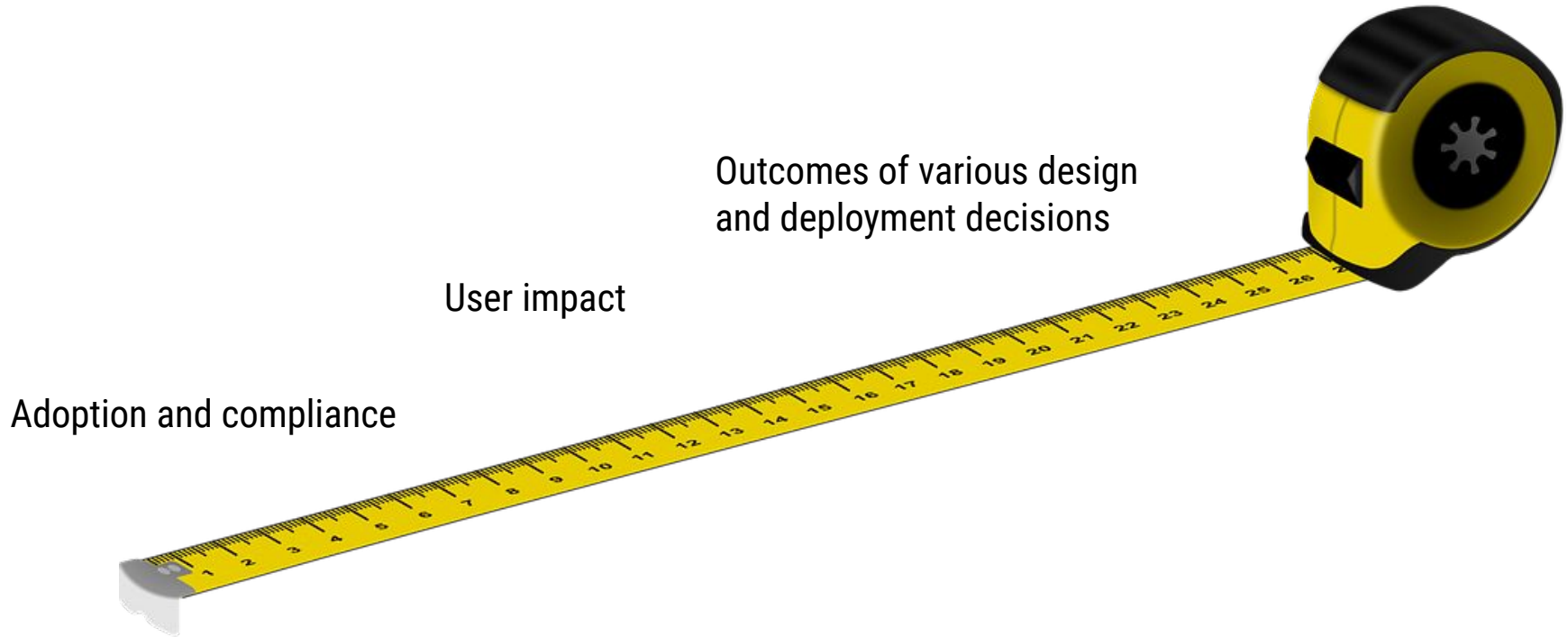
NET::ERR\_CERTIFICATE\_TRANSPARENCY\_REQUIRED

Advanced

Back to safety



# How successfully has CT been deployed?



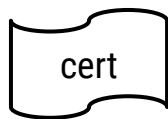
# Outline

- Background and data sources
- Analyzing CT compliance
- Deployment challenges

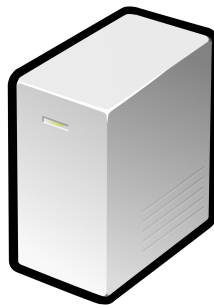
# Outline

- **Background and data sources**
- Analyzing CT compliance
- Deployment challenges

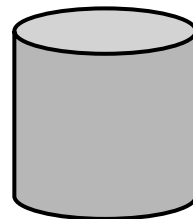
Root certificate authority



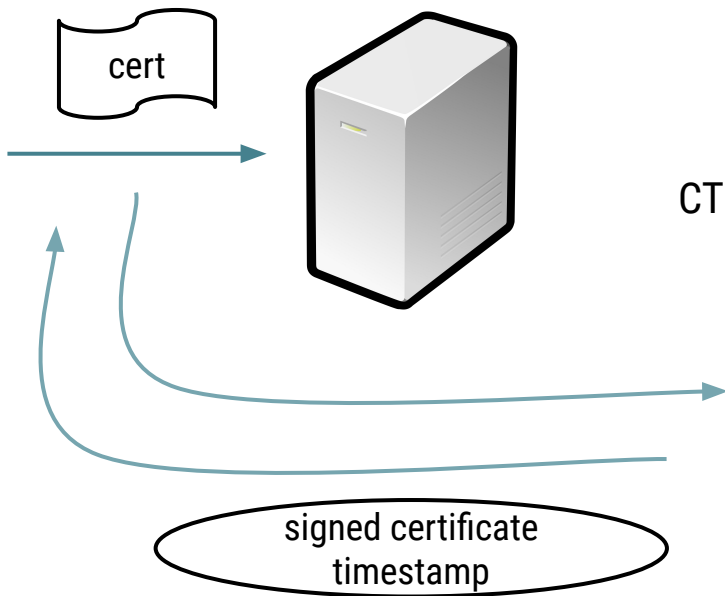
Web server

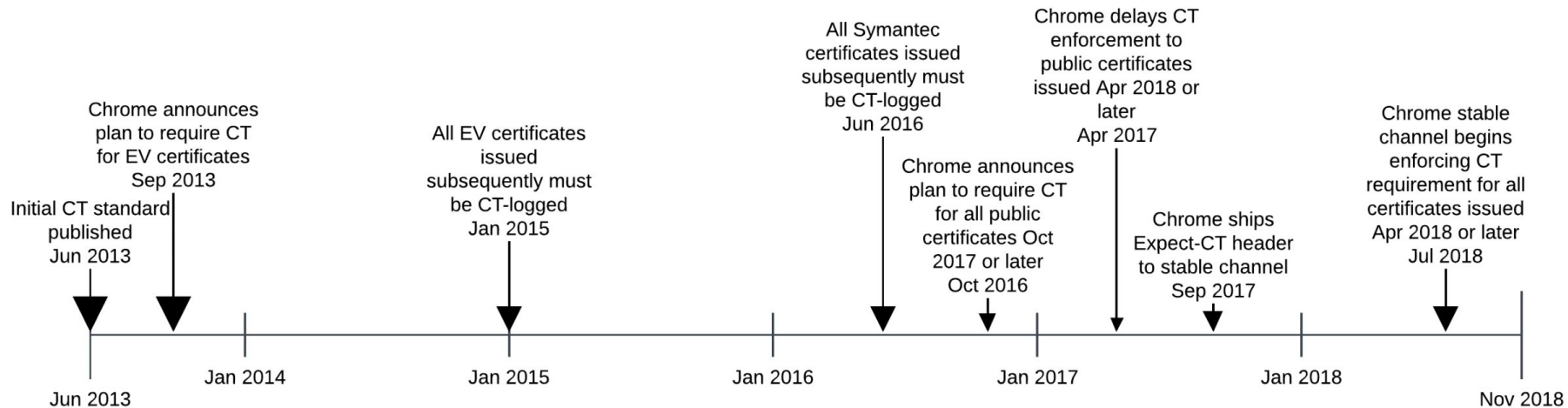


CT log: a public, auditable,  
append-only ledger



signed certificate  
timestamp







# Data sources

- Telemetry from Chrome
- Active scans of popular websites
- Qualitative analysis of Chrome help forum posts

(from various points in 2015-2018)

# Outline

- Background and data sources
- **Analyzing CT compliance**
- Deployment challenges

CT was supported on  
**71%**  
of HTTPS requests in Chrome

(February 2018)

# CT compliance

When Chrome requires a site to support CT, how often does the site comply?

# CT compliance

When Chrome requires a site to support CT, how often does the site comply?

**99.7%**

of CT-required HTTPS requests were compliant

(September 2018)

# Outline

- Background and data sources
- **Analyzing CT compliance**
- Deployment challenges

# Outline

- Background and data sources
- **Analyzing CT compliance**
  - Low compliance would be bad
  - Compliance shouldn't be taken for granted
  - Contributing factors to high compliance
- Deployment challenges

# Outline

- Background and data sources
- Analyzing CT compliance
  - **Low compliance would be bad**
  - Compliance shouldn't be taken for granted
  - Contributing factors to high compliance
- Deployment challenges



Users proceeded ~2x  
more often than  
certificate errors overall  
(September 2018)



## Your connection is not private

Attackers might be trying to steal your information from **google.com** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR\_CERTIFICATE\_TRANSPARENCY\_REQUIRED

Hide advanced

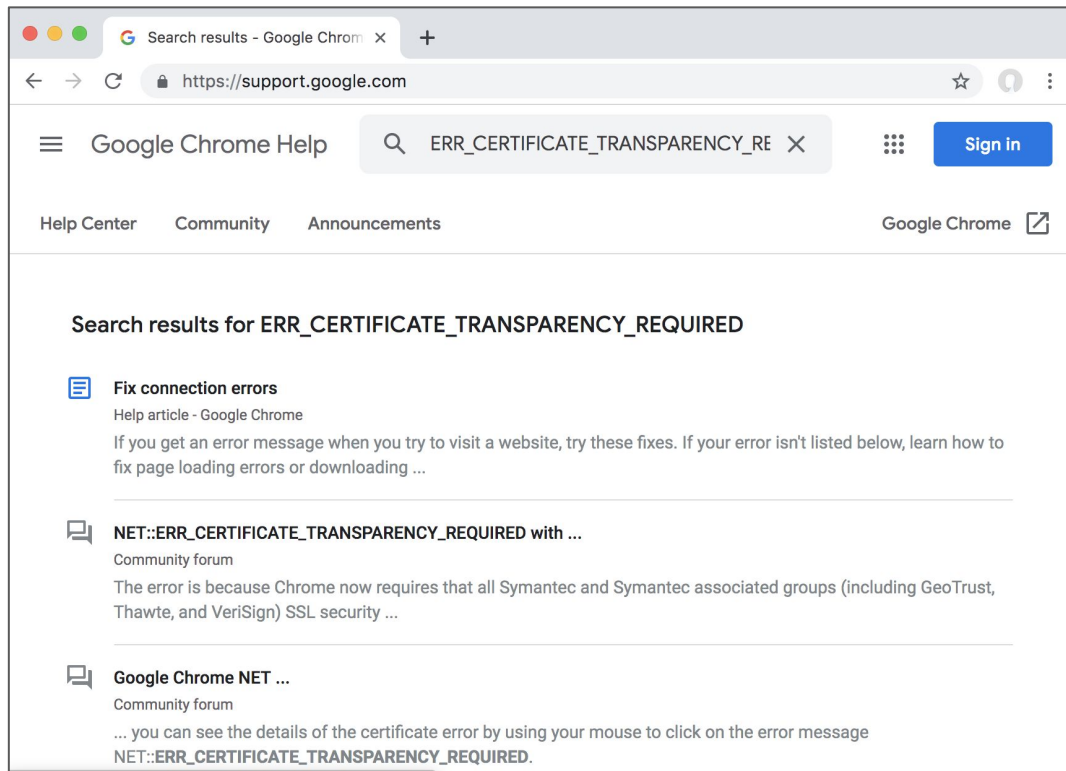
Back to safety

The server presented a certificate that was not publicly disclosed using the Certificate Transparency policy. This is a requirement for some certificates, to ensure that they are trustworthy and protect against attackers.

[Proceed to google.com \(unsafe\)](#)

60% of help forum threads have an incorrect solution or explanation

e.g., *“I have tried resetting to default settings (so disabling all extensions).”*



# Outline

- Background and data sources
- **Analyzing CT compliance**
  - **Low compliance would be bad**
  - Compliance shouldn't be taken for granted
  - Contributing factors to high compliance
- Deployment challenges

# Outline

- Background and data sources
- **Analyzing CT compliance**
  - Low compliance would be bad
  - **Compliance shouldn't be taken for granted**
  - Contributing factors to high compliance
- Deployment challenges

Malformed SCT designed  
to hide domain name  
from CT logs

Criteria

ID = '27896132'

crt.sh ID	27896132																																				
Summary	Precertificate																																				
Certificate Transparency	<table><tr><th>Timestamp</th><th>Entry #</th><th>Log Operator</th><th>Log URL</th></tr><tr><td>2016-08-10 19:25:02 UTC</td><td>8339</td><td>DigiCert</td><td>https://deneb.ws.symantec.com</td></tr><tr><td>2016-08-12 17:59:47 UTC</td><td>24765341</td><td>Google</td><td>https://ct.googleapis.com/aviator</td></tr><tr><td>2018-09-10 20:40:01 UTC</td><td>368625407</td><td>Google</td><td>https://ct.googleapis.com/pilot</td></tr></table>	Timestamp	Entry #	Log Operator	Log URL	2016-08-10 19:25:02 UTC	8339	DigiCert	https://deneb.ws.symantec.com	2016-08-12 17:59:47 UTC	24765341	Google	https://ct.googleapis.com/aviator	2018-09-10 20:40:01 UTC	368625407	Google	https://ct.googleapis.com/pilot																				
Timestamp	Entry #	Log Operator	Log URL																																		
2016-08-10 19:25:02 UTC	8339	DigiCert	https://deneb.ws.symantec.com																																		
2016-08-12 17:59:47 UTC	24765341	Google	https://ct.googleapis.com/aviator																																		
2018-09-10 20:40:01 UTC	368625407	Google	https://ct.googleapis.com/pilot																																		
Revocation	<table><tr><th>Mechanism</th><th>Provider</th><th>Status</th><th>Revocation Date</th><th>Last Observed in CRL</th><th>Last Checked (Error)</th></tr><tr><td>OCSP</td><td>The CA</td><td>Check</td><td>?</td><td>n/a</td><td>?</td></tr><tr><td>CRL</td><td>The CA</td><td>Revoked</td><td>2016-08-16 15:45:31 UTC</td><td>2017-08-16 22:07:25 UTC</td><td>2019-05-08 04:07:14 UTC</td></tr><tr><td>CRLSet/Blacklist</td><td>Google</td><td>Not Revoked</td><td>n/a</td><td>n/a</td><td>n/a</td></tr><tr><td>disallowedcert.stl</td><td>Microsoft</td><td>Not Revoked</td><td>n/a</td><td>n/a</td><td>n/a</td></tr><tr><td>OneCRL</td><td>Mozilla</td><td>Not Revoked</td><td>n/a</td><td>n/a</td><td>n/a</td></tr></table>	Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)	OCSP	The CA	Check	?	n/a	?	CRL	The CA	Revoked	2016-08-16 15:45:31 UTC	2017-08-16 22:07:25 UTC	2019-05-08 04:07:14 UTC	CRLSet/Blacklist	Google	Not Revoked	n/a	n/a	n/a	disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a	OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a
Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)																																
OCSP	The CA	Check	?	n/a	?																																
CRL	The CA	Revoked	2016-08-16 15:45:31 UTC	2017-08-16 22:07:25 UTC	2019-05-08 04:07:14 UTC																																
CRLSet/Blacklist	Google	Not Revoked	n/a	n/a	n/a																																
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a																																
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a																																
SHA-256(Certificate)	B0A0584F9A79F73C17DBC153A02D535468600DFE629DF2206AEA9C1F9AA341F																																				
SHA-1(Certificate)	241E4EE4517D80184E63A1574782308677B3CAF4																																				
Certificate   ASN.1	<p>Certificate:</p> <p>Data:</p> <p>Version: 3 (0x2)</p> <p>Serial Number:</p> <p>19:82:2f:8c:8f:b1:ff:b7:ef:f6:b7:9f:d3:95:b3:2a</p> <p>Signature Algorithm: sha256WithRSAEncryption</p> <p>Issuer: (CA ID: 1466)</p> <p>commonName = GeoTrust SHA256 SSL CA</p> <p>organizationName = GeoTrust Inc.</p> <p>countryName = US</p> <p>Validity</p> <p>Not Before: Aug 10 00:00:00 2016 GMT</p> <p>Not After : Aug 10 23:59:59 2017 GMT</p> <p>Subject:</p> <p>commonName = ?.united.com</p> <p>organizationalUnitName = Technology</p> <p>organizationName = United Airlines Inc</p> <p>localityName = Chicago</p> <p>stateOrProvinceName = Illinois</p> <p>countryName = US</p>																																				

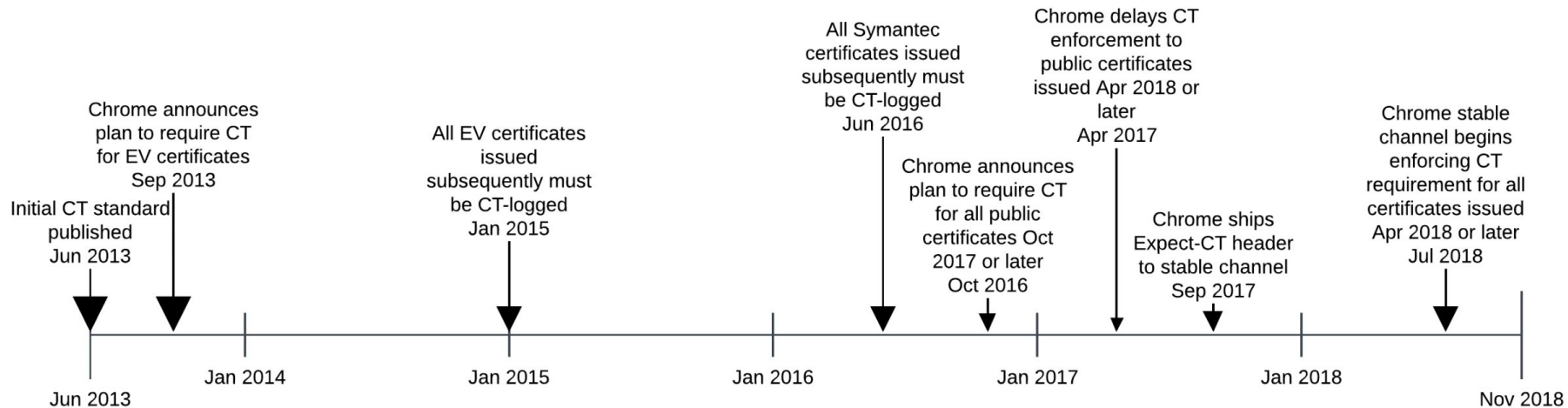
# Top 10 websites causing CT errors

(July/September 2018)

	Name stripping	Buggy CA implementation	CA lacking CT support
Chrome 67	8	2	
Chrome 68			10

# Outline

- Background and data sources
- **Analyzing CT compliance**
  - Low compliance would be bad
  - Compliance shouldn't be taken for granted
  - **Contributing factors to high compliance**
- Deployment challenges





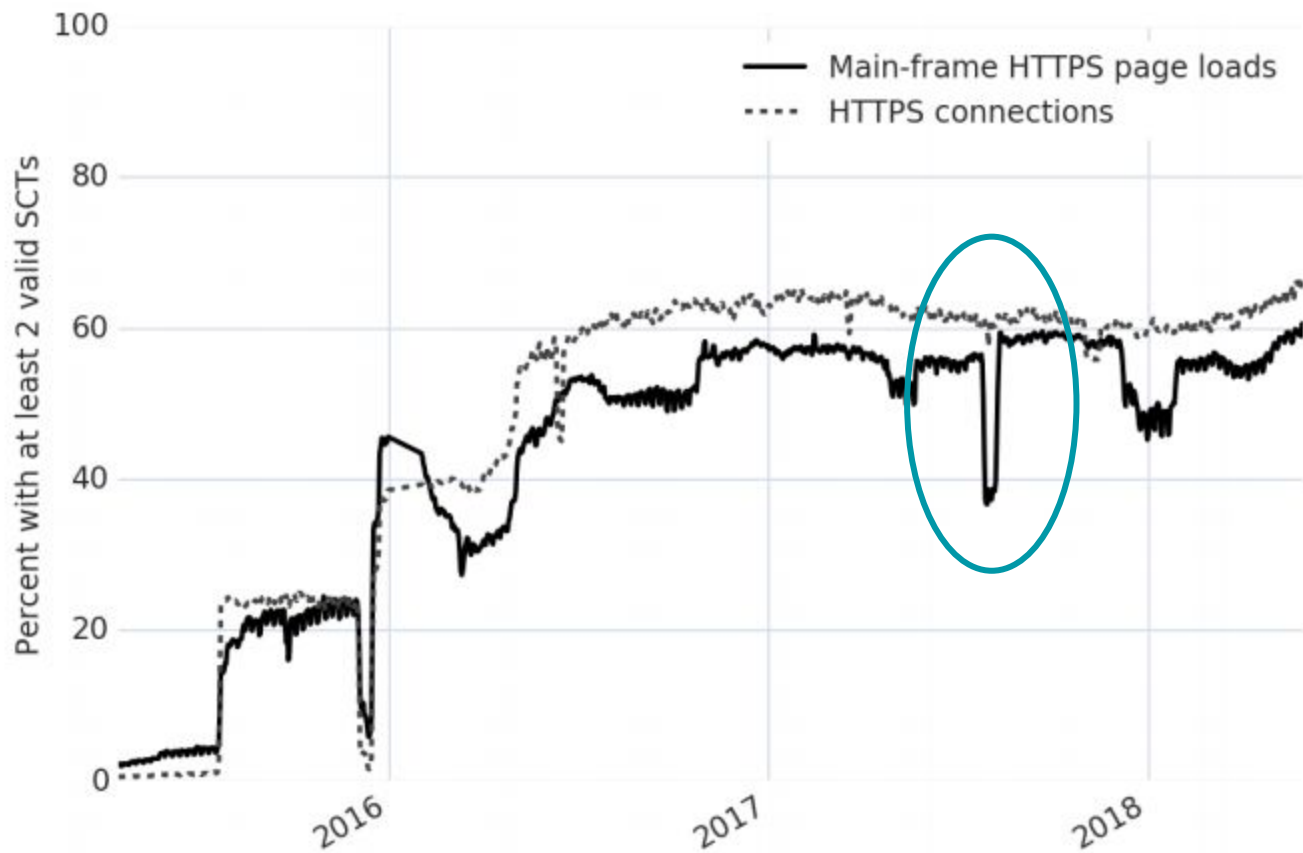
 PayPal, Inc. [US] | <https://www.paypal.com>



EV UI requires CT

$\leq 4\%$  of connections with EV certificates lost EV UI due to CT

<b>Issuing organization</b>	<b>EV certificates w/o SCTs</b>	<b>Total EV certificates</b>	<b>% w/o SCTs</b>
Verizon Cybertrust Security	8550	8556	99.9%
Symantec Corporation	1923	495528	3.9%
SwissSign AG	1719	1908	90.1%
Certplus	1391	1391	100.0%
Cybertrust Japan Co., Ltd	1373	24748	5.5%

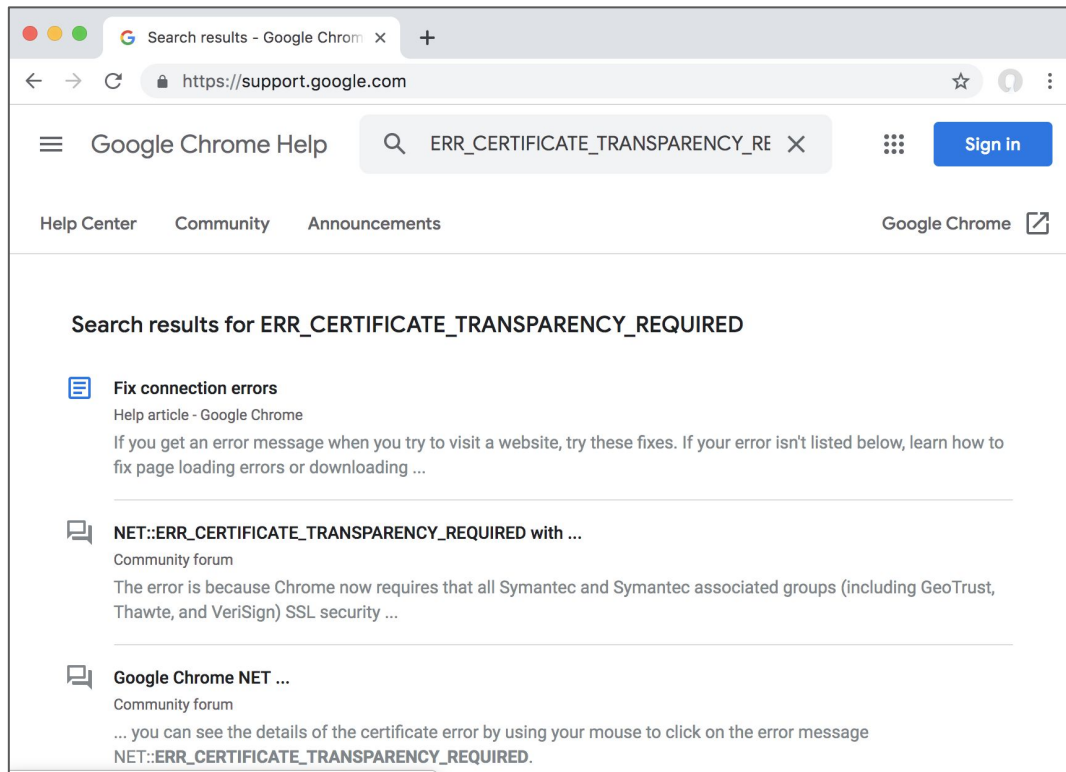


# Outline

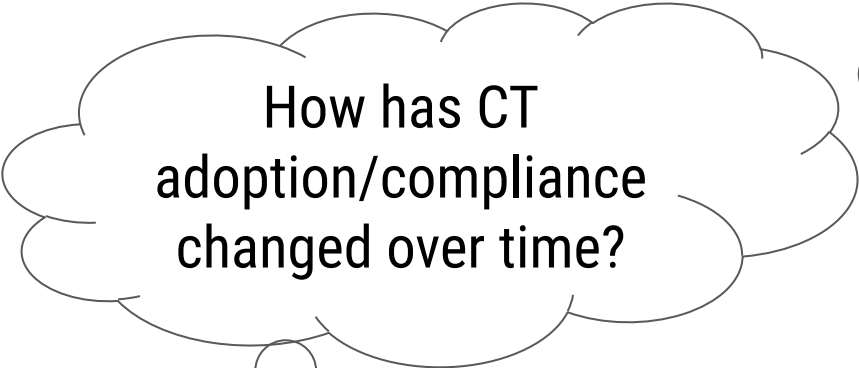
- Background and data sources
- Analyzing CT compliance
  - Low compliance would be bad
  - Compliance shouldn't be taken for granted
  - Contributing factors to high compliance
- **Deployment challenges**

In 19% of help forum threads, users circumvented error by switching browsers

e.g., *"I had to download another browser, which im starting to like."*

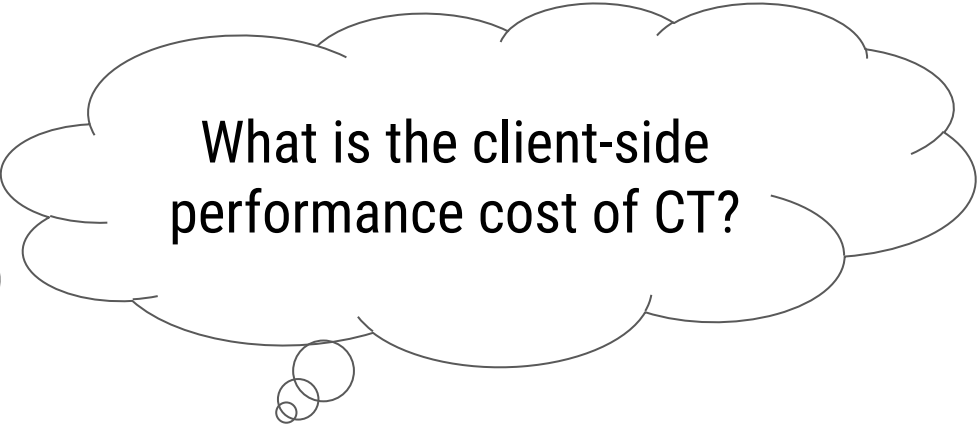


# Concluding tidbits



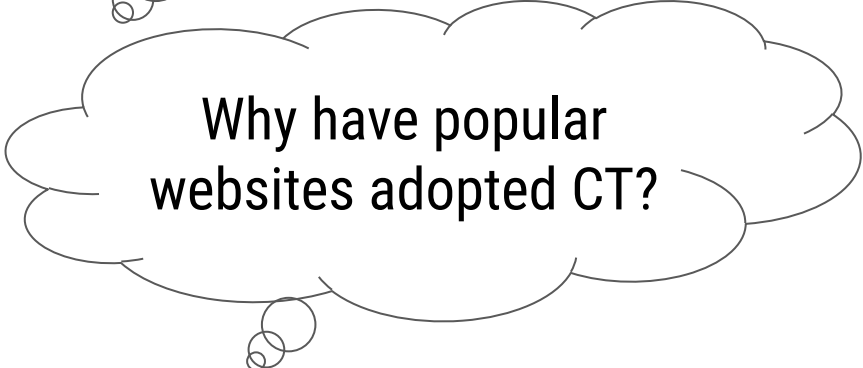
How has CT  
adoption/compliance  
changed over time?

A thought bubble with a scalloped border and a small tail at the bottom left.



What is the client-side  
performance cost of CT?

A thought bubble with a scalloped border and a small tail at the bottom left.



Why have popular  
websites adopted CT?

A thought bubble with a scalloped border and a small tail at the bottom left.



Open problems

A thought bubble with a scalloped border and a small tail at the bottom left.

# Does Certificate Transparency Break the Web?

## Measuring Adoption and Error Rate

**Emily Stark**, Ryan Sleevi, Rijad Muminovic, Devon O'Brien,  
Eran Messeri, Adrienne Porter Felt, Brendan McMillion, Parisa Tabriz  
[estark@chromium.org](mailto:estark@chromium.org)