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
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
How successfully has CT been deployed?

Adoption and compliance

User impact

Outcomes of various design and deployment decisions
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

cert

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
# Top 10 websites causing CT errors

(July/September 2018)

<table>
<thead>
<tr>
<th></th>
<th>Name stripping</th>
<th>Buggy CA implementation</th>
<th>CA lacking CT support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chrome 67</td>
<td></td>
<td>8</td>
<td>2</td>
</tr>
<tr>
<td>Chrome 68</td>
<td></td>
<td></td>
<td>10</td>
</tr>
</tbody>
</table>
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
EV UI requires CT

<= 4% of connections with EV certificates lost EV UI due to CT
<table>
<thead>
<tr>
<th>Issuing organization</th>
<th>EV certificates w/o SCTs</th>
<th>Total EV certificates</th>
<th>% w/o SCTs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verizon Cybertrust Security</td>
<td>8550</td>
<td>8556</td>
<td>99.9%</td>
</tr>
<tr>
<td>Symantec Corporation</td>
<td>1923</td>
<td>495528</td>
<td>3.9%</td>
</tr>
<tr>
<td>SwissSign AG</td>
<td>1719</td>
<td>1908</td>
<td>90.1%</td>
</tr>
<tr>
<td>Certplus</td>
<td>1391</td>
<td>1391</td>
<td>100.0%</td>
</tr>
<tr>
<td>Cybertrust Japan Co., Ltd</td>
<td>1373</td>
<td>24748</td>
<td>5.5%</td>
</tr>
</tbody>
</table>
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?

Why have popular websites adopted CT?

What is the client-side performance cost of CT?

Open problems
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