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
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
  • Shared pipeline where possible

• 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
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

- CT Log
- CA
- Webserver
- Browser
Certificate Transparency

CT Log ----> CA

Certificate

Webserver ----> Browser
Certificate Transparency

CT Log \[\rightarrow\] Certificate \[\rightarrow\] Webserver

SCT \[\uparrow\] Certificate \[\downarrow\] Webserver

CA \[\rightarrow\] Certificate

Certificate, SCT in TLS Ext. \[\rightarrow\] Browser
Certificate Transparency

CT Log <- Precertificate -> CA

Webserver    Browser
Certificate Transparency

CT Log → Precertificate → SCT → CA

Webserver → Browser
Certificate Transparency

CT Log → Precertificate → CA → SCT → Certificate (with Precertificate SCT) → Webserver → Browser
Certificate Transparency

CT Log  \[\rightarrow\]  Precertificate

Precertificate  \[\rightarrow\]  SCT

SCT  \[\rightarrow\]  Certificate (with Precertificate SCT)

Certificate (with Precertificate SCT)  \[\rightarrow\]  Certificate. Transform, Validate

CA  \[\rightarrow\]  Webserver

Webserver  \[\rightarrow\]  Browser
Certificate Transparency

CT Log

CA

Webserver

Browser
Certificate Transparency

CT Log → Certificate → Webserver → Browser

CA
Certificate Transparency

CT Log → Certificate → CA

SCT

Webserver → Certificate → Browser
Certificate Transparency

CT Log → Certificate → CA

CA → SCT

Webserver → Certificate → Browser

Browser → OCSP, SCT in OCSP Reply
Certificate Transparency

CT Log — Certificate

CA — SCT

Webserver — Certificate

Browser — OCSP, SCT in OCSP Reply

Certificate

SCT in Stapled OCSP Reply
## SCT Statistics - Active

<table>
<thead>
<tr>
<th></th>
<th>Sydney v4</th>
<th>Munich v4</th>
<th>Munich v6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Domains we could connect to</strong></td>
<td>55.7M</td>
<td>58.0M</td>
<td>5.1M</td>
</tr>
<tr>
<td><strong>Domains with SCT</strong></td>
<td>6.8M</td>
<td>6.8M</td>
<td>357K</td>
</tr>
<tr>
<td>... via X509</td>
<td>6.7M</td>
<td>6.8M</td>
<td>344K</td>
</tr>
<tr>
<td>... via TLS Ext.</td>
<td>27.6K</td>
<td>27.2K</td>
<td>12.9K</td>
</tr>
<tr>
<td>... via OCSP</td>
<td>180</td>
<td>188</td>
<td>3</td>
</tr>
<tr>
<td><strong>Certificates (Total)</strong></td>
<td>10.62M</td>
<td>9.66M</td>
<td>549.98K</td>
</tr>
<tr>
<td><strong>Certificates with SCT Ext.</strong></td>
<td>799.9K</td>
<td>834.5K</td>
<td>193.9K</td>
</tr>
</tbody>
</table>
## SCT Statistics - Passive

<table>
<thead>
<tr>
<th></th>
<th>California</th>
<th>Munich</th>
<th>Sydney</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time</strong></td>
<td>4/4-5/2</td>
<td>5/12-5/16</td>
<td>5/12-5/16</td>
</tr>
<tr>
<td><strong>Conns</strong></td>
<td>2.6B</td>
<td>287M</td>
<td>196M</td>
</tr>
<tr>
<td><strong>Conns with SCT</strong></td>
<td>779M</td>
<td>73M</td>
<td>58M</td>
</tr>
<tr>
<td>… in Cert</td>
<td>520M</td>
<td>58M</td>
<td>44M</td>
</tr>
<tr>
<td>… in TLS</td>
<td>248M</td>
<td>14M</td>
<td>14M</td>
</tr>
<tr>
<td>… in OCSP</td>
<td>156K</td>
<td>38K</td>
<td>31K</td>
</tr>
<tr>
<td><strong># v4 IPs</strong></td>
<td>737K</td>
<td>344K</td>
<td>226K</td>
</tr>
<tr>
<td><strong># SCT v4 IPs</strong></td>
<td>222K</td>
<td>102K</td>
<td>66K</td>
</tr>
</tbody>
</table>
CERTIFICATE TRANSPARENCY

Main Origin:
https://www.wsgyet.com

Non-Secure Origins:
- chrome-extension://nftsoabibnmffglnbggj

Secure Origins:
- https://pagead2.googlesyndication.com
- https://www.google-analytics.com
- https://www.google-analytics.com
- https://pixe1.esm1.net
- https://adwc.elsem1.net
- https://ad.doubleclick.net

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 enable individual requests in the Network panel.
休日に足を運んで食べに行きたいっつ
最初の「味茨スイーツ」が食べられる
お店をご紹介です。

### 5月5日の注目記事

1. **出会いは典BODYが引き寄せ!?**
   - 1ヶ月
   - 10キロも可能な痩身エクセントで、見事別人
   - 痩せるのも大丈夫！
   - 「10分」でかわいくなる簡単メイク術

---

### Highlights from Chrome 59 update

<table>
<thead>
<tr>
<th>Subject</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSS and JS code coverage</td>
<td>Find unused CSS and JS with the new Coverage drawer.</td>
</tr>
<tr>
<td>Full-page screenshots</td>
<td>Take a screenshot of the entire page, from the top of the viewport to the bottom.</td>
</tr>
<tr>
<td>Block requests</td>
<td>Manage blocked requests in the Network panel.</td>
</tr>
</tbody>
</table>
105 Certificates, 91 Let’s Encrypt
This page is in Norwegian
Would you like to translate it?

- 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

SAN

- www.fhi.no
- admin.fhi.no

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

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

Issuer
Bypass Class 3 CA 2

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)

The security details above are from the first inspected response.
## Log Operators

<table>
<thead>
<tr>
<th>Active</th>
<th>Passive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec log (81.26%)</td>
<td>Symantec log (62.78%)</td>
</tr>
<tr>
<td>Google 'Pilot' log (79.9%)</td>
<td>Google 'Rocketeer' log (58.6%)</td>
</tr>
<tr>
<td>Google 'Rocketeer' log (31.72%)</td>
<td>Google 'Pilot' log (58.48%)</td>
</tr>
<tr>
<td>DigiCert Log Server (26.96%)</td>
<td>Google 'Icarus' log (14.37%)</td>
</tr>
<tr>
<td>Google 'Aviator' log (25.67%)</td>
<td>Google 'Aviator' log (9.39%)</td>
</tr>
<tr>
<td>Google 'Skydiver' log (8.32%)</td>
<td>Vena log (7.47%)</td>
</tr>
<tr>
<td>Symantec VEGA log (3.98%)</td>
<td>WoSign ctlog (4.64%)</td>
</tr>
<tr>
<td>StartCom CT log (1.49%)</td>
<td>DigiCert Log Server (4.07%)</td>
</tr>
<tr>
<td>WoSign ctlog (0.67%)</td>
<td>Google 'Skydiver’ log (1.7%)</td>
</tr>
</tbody>
</table>
Certificate:

Data:

- Version: 3 (0x2)
- Signature Algorithm: sha256WithRSAEncryption
- Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4 Validity
  - Not Before: May 30 00:00:00 2016 GMT
  - Not After: May 30 00:00:00 2018 GMT
- Subject: C=US, ST=Washington, L=Seattle, O=Amazon.com, Inc., CN=* cloudfront.net

X509v3 extensions:

- Subject Alternative Name:
  - DNS: cloudfront.net, DNS:*.cloudfront.net
- Basic Constraints:
  - CA: FALSE
- Authority Information Access:
  - OCSP - URI: http://ss.symcd.com
  - CA Issuers - URI: http://ss.symcb.com/ss.crt
- CT Precertificate SCTs:
  - Random string goes here
Certificate:

Data:

Subject:

Serial Number:

Signature Algorithm:

Serial Number:

Not Before: May 30 00:00:00 2016 GMT

Not After: May 30 00:00:00 2018 GMT

Subject: CN=US, O=Symantec Corporation, OU=Symantec Trust Network, CN=Symantec Class 3 Secure Server CA - G4

Validity

X509v3 Subject Alternative Name:

DNS:cloudfront.net, DNS:* .cloudfront.net

X509v3 Basic Constraints:

Authority Information Access:

OCSP - URI:http://ss.symcd.com

CA Issuers - URI:http://ss.symcb.com/ss.crt

CT Precertificate SCTs:

..Random string goes here
HSTS, HPKP

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

Automatically deployed when servers/libraries update

> 96% deployment
# Deployment

<table>
<thead>
<tr>
<th>Mechanism</th>
<th>Standardized</th>
<th>Deployment Overall</th>
<th>Top 10K</th>
<th>Effort</th>
<th>Availability Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCSV</td>
<td>2015</td>
<td>49.2M</td>
<td>6789</td>
<td>none</td>
<td>low</td>
</tr>
<tr>
<td>CT-x509</td>
<td>2013</td>
<td>7.0M</td>
<td>1788</td>
<td>none²</td>
<td>none</td>
</tr>
<tr>
<td>HSTS</td>
<td>2012</td>
<td>0.9M</td>
<td>349</td>
<td>low</td>
<td>low</td>
</tr>
<tr>
<td>CT-TLS</td>
<td>2013</td>
<td>27,759</td>
<td>171</td>
<td>high</td>
<td>none</td>
</tr>
<tr>
<td>HPKP</td>
<td>2015</td>
<td>6616</td>
<td>156</td>
<td>high</td>
<td>high</td>
</tr>
<tr>
<td>HPKP PL.</td>
<td>2012¹</td>
<td>479</td>
<td>150</td>
<td>high</td>
<td>high</td>
</tr>
<tr>
<td>HSTS PL.</td>
<td>2012¹</td>
<td>23,539</td>
<td>144</td>
<td>medium</td>
<td>medium</td>
</tr>
<tr>
<td>CAA</td>
<td>2013</td>
<td>3057</td>
<td>20</td>
<td>medium</td>
<td>low</td>
</tr>
<tr>
<td>TLSA</td>
<td>2012</td>
<td>973</td>
<td>3</td>
<td>high</td>
<td>medium</td>
</tr>
<tr>
<td>CT-OCSP</td>
<td>2013</td>
<td>191</td>
<td>0</td>
<td>low</td>
<td>none</td>
</tr>
</tbody>
</table>

1: Preloading list first added to Chrome in 2012
2: Requires deployment effort on CA side and a new site certificate.
Primary eng (and PM) emails

palmer@chromium.org, rsleevi@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.)
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
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