New Adventures in PKI

Jeremy Rowley

DigiCert, Inc.
Overview

- Deprecation of SHA-1
- Certificate Transparency (CT)
- Certificate Lifecycles
- Internal Name Deprecation
- Certificate Authority Authorization (CAA)
- Heartbleed Bug
SHA-1 Transition

Microsoft SHA-1 Deprecation Timeline
  – January 1, 2016: Cease issuance and deprecation for code signing certificates
  – January 1, 2017: Deprecation of SSL

Mozilla SHA-1 Deprecation Timeline
  – Early 2015: Security warning for 2017 certificates
  – Firefox 2016 release: “Untrusted Connection” for new SHA-1 certificates
  – Firefox 2017 release: “Untrusted Connection” for all SHA-1
SHA-1 Transition

Google SHA-1 Deprecation Timeline

- September 2014: Mixed content warning for SHA-1 expiring in 2017
- November 2014: Mixed content warning for SHA-1 expiring after June 1, 2016
- Q1 2015: Mixed content warning for all certificates expiring in 2016 and interstitial for 2017 and non-secure indicator for 2017
SHA-1 Sunset Tool

SHA-1 certificates expiring after January 1, 2016 will receive a security warning beginning with Google Chrome v39 and on future Microsoft platforms.

Find all of the SHA-1 certificates on a given domain and replace them for free with an equivalent SHA-256 DigiCert certificate to avoid browser warnings.

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Expiration</th>
<th>Chrome 39 (November)</th>
<th>Chrome 40 (After holidays)</th>
<th>Chrome 41 (Q1 2015)</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.twitter.com</td>
<td>2017-10-29</td>
<td><img src="https://" alt="" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="" /></td>
<td>Replace with SHA-2 »</td>
</tr>
<tr>
<td>api.twitter.com</td>
<td>2016-12-31</td>
<td><img src="https://" alt="" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="" /></td>
<td>Replace with SHA-2 »</td>
</tr>
<tr>
<td>stream.twitter.com</td>
<td>2016-12-30</td>
<td><img src="https://" alt="" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td>Replace with SHA-2 »</td>
</tr>
<tr>
<td>ms1.twitter.com</td>
<td>2016-10-18</td>
<td><img src="https://" alt="" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td>Replace with SHA-2 »</td>
</tr>
<tr>
<td>syndication.twitter.com</td>
<td>2016-08-12</td>
<td><img src="https://" alt="" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td>Replace with SHA-2 »</td>
</tr>
<tr>
<td>tnn.twitter.com</td>
<td>2016-04-05</td>
<td><img src="https://" alt="" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td>Replace with SHA-2 »</td>
</tr>
<tr>
<td>upload.twitter.com</td>
<td>2016-04-01</td>
<td><img src="https://" alt="" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td>Replace with SHA-2 »</td>
</tr>
<tr>
<td>api.twitter.com</td>
<td>2016-04-01</td>
<td><img src="https://" alt="" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td>Replace with SHA-2 »</td>
</tr>
<tr>
<td>support.twitter.com</td>
<td>2016-04-01</td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td>Replace with SHA-2 »</td>
</tr>
<tr>
<td>mobile.twitter.com</td>
<td>2016-04-01</td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td>Replace with SHA-2 »</td>
</tr>
<tr>
<td>urls-realapi.twitter.com</td>
<td>2016-04-01</td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td>Replace with SHA-2 »</td>
</tr>
<tr>
<td>s10.twimg.com</td>
<td>2016-03-01</td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td><img src="https://" alt="https://" /></td>
<td>Replace with SHA-2 »</td>
</tr>
</tbody>
</table>

Legend:
- ![https://](https://): No security warnings
- ![https://](https://): Secure, but with minor errors
- ![https://](https://): Neutral, lacking security
- ![https://](https://): Affirmatively insecure

DigiCert®
Your success is built on trust®
Certificate Transparency

• Goals
  – Provide insight into issued SSL certificate
  – Provide faster remediation
  – Ensure CAs are aware of what they issue

• Benefits
  – Fast detection means better mitigation
  – Greater visibility means better accountability
  – Visible trust in operations
  – Easier evaluation of certificate use

• Deployment
  – Number of logs dependent on lifecycle
  – Required for EV starting Jan 2015
  – Nothing required from server operators
  – Two logs approved, two pending
Certificate Lifecycles

• **Short lived Certificates**
  – Issued with a 48 hour validity period
  – Used for remote location
  – Alternative form of revocation
  – Mozilla discussion:
    [https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/T11up58JkFc](https://groups.google.com/forum/#!topic/mozilla.dev.security.policy/T11up58JkFc)

• **3-year Maximum Lifecycle**
  – Required April 2015
  – Permits “rapid” changes in standards
  – Ensures revalidation is occurring
Internal Name Deprecation

CAs may no longer issue certificates that contain Internal Names and expire after November 1, 2015.

All certificates are revoked within 120 days of the contract signing date.

Finding Internal Names
- Gather all Certificates
- Look at each common name
- Look at each SAN
- Evaluate if there is an internal name

Certificate Inspector Tool
- Scans a network range and port range
- Evaluates each Certificate to determine if any internal names exist
- Compares against the latest policy changes
- Lists all internal name Certificates
www.examplecompany10.com
Certificate found by agent on Thu Feb 27 15:36:57 MST 2014.

Issuing CA: Booktrust Inc.
Valid From: Jan 23, 2014 8:27:02 AM
Expires: Jan 23, 2015 11:27:49 AM
Certificate Grade: 60/100
DigiCert Product Match: SSL Plus

*Note: This is your certificate grade. Click your SSL endpoint grade below.

Subject
Common Name: examplecompany.com
SANs: *digicert.com
digicert.com
Organization Name: DigiCert, Inc
Organization Unit: Lindon
Thumbprint: 19ED06C43945C4DFEB109E2ADFD5DC16BA3E5073
Serial number: 01000000000143C411D598DD01883
Validation Type: Domain Validation
Publicly Trusted: true
Self-signed: False
Signing algorithm: SHA1withRSA

SHA1 Hashing Algorithm Notice
The SHA1 hashing algorithm could be prone to collision based attacks. It is recommended to move to SHA2 if your infrastructure will support it.
How can I fix this?

Missing AIA
Certificate is missing AIA Information. The AIA fields are required under the CA/B Forum baseline requirements
How can I fix this?

SSL Endpoint Analysis
The following services are using this certificate:

<table>
<thead>
<tr>
<th>Hostname</th>
<th>IP Address</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.examplecompany11.com">www.examplecompany11.com</a></td>
<td>10.0.0.8443</td>
<td>F</td>
</tr>
</tbody>
</table>
Certification Authority Authorization (CAA)

• **Advantages**
  – Reduces risk of unintended certificate mis-issuance
  – Simple way to express your preference of CAs
  – Add CAA information to DNS and change it when you wish

• **Disadvantages**
  – Compliance is voluntary
  – Not uniformly applied
  – Partial solution
  – May slow certificate issuance

• **Deployment**
  – CAs required to list policy and interpretation in CP
  – CAs may elect not to check CAA
Advanced SSL analysis examines common problems and weaknesses including:

- Vulnerability to Heartbleed Bug, CRIME, BEAST, or BREACH attacks
- Certificates with weak private keys
- Expiring certificate dates
- Internal names
- Missing fields and values
- Certificate name mismatch
- Weak cipher suites
- SHA1 vs SHA2
- Broken chains
Tools

SSL Analysis Tools

- [https://www.digicert.com/cert-inspector.htm](https://www.digicert.com/cert-inspector.htm)
- [https://www.digicert.com/sha1-sunset/](https://www.digicert.com/sha1-sunset/)
- [https://www.ssllabs.com](https://www.ssllabs.com)
- [http://www.whynopadlock.com/](http://www.whynopadlock.com/)

Jeremy Rowley

[jeremy.rowley@digicert.com](mailto:jeremy.rowley@digicert.com)

801-701-9676