Improving the Security of EV Certificates

Ben Laurie (benl@google.com)

8 December~~19 March~~ 2014

In order to improve the security of Extended Validation (EV) certificates, Google Chrome intends to require Certificate Transparency (CT) for all EV certificates issued after 1 Jan~~Feb~~ 2015.

Once we have gained experience with EV certificates we will publish a plan to bring CT to all certificates.

We are pleased to announce the following plan.

1. Google is already running two geographically diverse ~~pilot~~ CT logs.
2. By Jan 2015 Google will deploy three geographically diverse production CT logs which will accept all certificates issued by CAs accepted by any major browser.
3. Google invites other organisations to deploy CT logs in order to improve robustness.
4. All EV certificates (including already issued certificates) with validity periods beyond Jan 2015 should be logged in at least one qualifying log. These logged certificates will determine what is in the whitelist created in step ~~5~~6.
5. On 1 Jan 2015 Chrome will create a whitelist of certificates that contain EV policy OIDs included or pending inclusion in Chrome, that have been logged in a qualifying log, and that would not qualify via SCTs embedded in the certificate (see below)~~valid EV certificates already issued without an embedded SCT issued by CAs participating in CT[1] from all qualifying logs~~.
6. On or after (depending on Chrome release schedule) 1 Feb 2015 Chrome for desktop platforms will cease to show the EV indicator for certificates not in the whitelist and not CT qualified according to the criteria below. Chrome for mobile platforms will cease to show EV indicators for certificates that are not CT qualified according to the criteria below.

Qualifying Logs

A log is qualified if its URL, public key and Maximum Merge Delay (MMD) are known to and accepted by Chrome.

In outline, Chrome will accept a log's URL, public key and MMD if

1. The log has not been shown to have acted in bad faith (e.g. it has in fact logged every certificate it has claimed to log, and has not ever violated the append-only property).
2. The log is up at least 99% of the time[2] and no single outage lasts longer than the MMD.
3. The log has an MMD of no more than 24 hours.
4. The log conforms to RFC 6962.

We will publish precise guidelines in due course.

Google will publish the set of qualified logs every six months at http://www.chromium.org/Home/chromium-security/certificate-

[1] "Participating in CT" means that the CA is issuing qualifying certificates by this date.

[2] That is, reachable and responsive as measured by Google.

transparency~~root-ca-policy~~ and to the CA/B Forum public mailing-list. Each list takes effect three months after publication. Special publications will be made in the event that a log is revoked.

Qualifying Certificate

A certificate is CT qualified if the TLS handshake it is presented in satisfies at least one of

1. At least the number of SCTs shown in Table 1, each from an independent log[3] that is either qualified or pending qualification at ~~was qualifying at the~~ time of certificate issuance, with all logs accepted as qualified prior to the TLS handshake~~issue~~, are embedded in the certificate.
2. Two or more SCTs from independent qualifying logs[4] are embedded in a stapled OCSP response as specified in RFC 6962.
3. Two or more SCTs from independent qualifying logs[5] are sent via the RFC 6962 TLS extension.

And at least one SCT for the certificate validates and was issued by a log that is qualifying at the time of check.

Lifetime of certificate	Number of SCTs
<15 months	2
>= 15, <= 27 months	3
> 27, <= 39 months	4[6]
> 39 months	5

Table 1

Note that, so long as the above conditions are met by some combination of SCTs presented in the handshake, additional SCTs, regardless of origin, are permitted.

Important note: most TLS servers do not support OCSP Stapling or the RFC 6962 TLS extension, so CAs should be prepared to insert SCTs into issued certificates to maintain the EV indication.

Temporary Relaxation of Independence

[3] An independent log is one that does not share infrastructure or administrative access with another log used for the same certificate.
[4] Note that in this case SCTs can be updated without modifying the certificate and are therefore expected to be from logs that are qualifying at the time of presentation.
[5] Note that in this case SCTs can be updated without modifying the certificate and are therefore expected to be from logs that are qualifying at the time of presentation.
[6] EV certificates should never have a lifetime over 27 months.

> For certificates issued before 1 July 2015, no matter how many SCTs are required, the logs they come from need not be independent. However, at least one must come from a log operated by Google.

Timeouts

The list of qualifying and once qualifying logs will be periodically refreshed during regular Chrome releases. If the installed version of Chrome has not applied security updates for a significant amount of time then CT checking will be disabled and the client will cease to show EV indications.