Expect-CT

Emily Stark
estark@chromium.org
IETF 97

Background

Certificate Transparency (CT): a framework for publicly logging certificates and proving that they’ve been logged. Standardization in TRANS WG.

Background

Today, domain owners can monitor logs for misissued certificates... but how do they defend against unlogged misissuances?

Expect-CT

Allow site owners to opt in to CT enforcement.

Expect-CT

```
HTTP/1.1 200 OK

...

Expect-CT: require; report-uri="https://..."; max-age: 31536000
```

Asks the UA to refuse and report connections that violate the UA's CT policy (e.g. two Signed Certificate Timestamps from two different logs).

Expect-CT

```
HTTP/1.1 200 OK

...

Expect-CT: report; report-uri="https://..."; max-age: 31536000
```

Allows the site owner to discover misconfigurations before turning on enforcement.

Expect-CT

- HTTP header for deployability.
- Syntax/semantics familiar to site operators (from HSTS).
- Allows site operators to ensure that all certificates in use for their domains are publicly logged.

Upcoming CT requirement

- Chrome plans to require CT for all new certificates starting Oct 2017.
- Value added by Expect-CT:
  - Protect against backdating or old misissuances.
  - Let sites get security benefit of CT before all browsers require CT.
  - Let sites see how they will fare before CT requirement date hits.

Questions/issues

- Separate header vs new HSTS directives
- Behavior of report-only mode (cached?)
- Defining a header to enforce CT without defining what it means to enforce CT