Comparing content-origins and signer-origins

Jeffrey Yasskin and Martin Thomson

IETF 107 WPACK

2020-03-25

Recap

Signer origin

Content is given an origin based on who signed it.

Content origin

Content is given an origin based on (a hash of) its bytes,

And possibly “adopted” by an online origin later.

Shared risks

- Don’t adopt personalized content, including cookies.
- Bundle to avoid version skew.

Complementary approaches

- Each approach has upsides, some of which compensate for the other's downsides.

Liveness

- Sec-Content-Origin lets a server vouch for content in real time, reducing the need to expire signatures quickly.

Upgrades

- We can't let just anyone claim to be an upgrade of an existing site in order to get its state.
- To do an upgrade offline, the old version has to somehow identify the target of the upgrade before the upgrade happens.
- That's impossible when content is only identified by its hash.
- The old version could identify a signing key that authorizes updates to see its state.

URL display

- A content-origin’s target URL isn’t trustworthy enough to show in the URL bar.
- If the domain of that URL also signed the content, maybe it is trustworthy enough.

Summary

Liveness

- If content origins work, use them.

Upgrades

- Expose state to future updates signed with a particular key.

URL display

- Show the signer’s origin in the URL bar.