Signer origins

IETF 107 WPACK

Jeffrey Yasskin
draft-yasskin-http-origin-signed-responses-08

Goals

- Authenticity
- Continuity of Experience

Authenticity

User gets some content while offline.

Where did the content come from? Can they trust it?

Caveat: URLs aren't good at expressing authenticity to users.

Continuity of Experience

Users get a piece of content while offline. Use it, generating state.

Go online. Send bits of the state over the internet.

Get a new version while offline. Update existing state using the new version.

Go back online.

Solution: Assign content its signer's origin

If foo.example controls a private key,
and we know of that control with the same assurance as TLS,
and that key signs a file,
give that file an origin of https://foo.example.

Downsides

- Off-path attackers
- "Revoked" content
- Other security considerations of draft-yasskin-http-origin-signed-responses
- Signature updates

Downside: Off-path attackers

An attacker who obtains a TLS private key
still faces logistical challenges in exploiting users.

An attacker who obtains a Signed-Exchange private key
avoids these challenges.

Downside: Revoked content

A signature proves this **was** vouched for by the signer.
A TLS connection proves this **is** vouched for by the peer.

The 7-day validity limit isn't a complete fix
and introduces logistical problems.

Downside: Signature update infrastructure

All content must be re-signed every 3ish days.

URL structure for clients to fetch updated signatures

Questions