Origin-Signed Exchanges

draft-yasskin-http-origin-signed-responses-03

Jeffrey Yasskin, Chromium

IETF 101

March 2018

Use Cases

From draft-yasskin-webpackage-use-cases-01:

- Privacy-preserving prefetch
  - This, with other changes, lets Google Search treat AMP and non-AMP content alike.
- Avoiding Slashdot effect
- Censorship evasion
- Cross-CDN Push (*P)
- Offline P2P site sharing (*B)

(*P) If privacy concerns are solved

(*B) With bundling.

Structure

- HTTP exchange
- Signature HTTP header (Section 3.1)
  - URL for certificate chain
  - SHA-256 hash of the leaf certificate
  - Timestamp range the signature is valid
  - Signature-update URL ("validityUrl"), same-origin with exchange
  - Name of header that guards payload's integrity
  - Sign(cert-pub-key, cert-hash||timestamps||update-url||integrity-header||exchange-headers)
- 3 ways to transfer (Section 5)
  - Normal response
  - Push
  - New envelope format

Privacy is the same as HTTPS

- Victim must have gotten a link to the exchange somehow.
- Whoever provided the link can track clicks on it.
- Trying to discover cached exchanges through a side channel, perhaps provided by an ISP, would break this property.
- One change: The link source gets a guarantee of the target's content instead of high probability. Does this matter?

Architectural risks?

- Unlike client's HTTP cache, users can load a resource without ever connecting to its origin server.
  - Same as old HTTP caching proxies.
  - Same as CDN business model.
- New proxy model, where the proxy is configured by the link source.
- Does this privilege folks like Google who can afford to run their own caches?
  - CDNs can provide caches with privacy promises for smaller sites.

Security risks

- All risks of CERTIFICATE frame.
- Replay attacks: 0RTT allows replaying requests;
  signed-exchanges allow replaying responses.
- Downgrade attacks: Within an exchange's signature's validity, attacker can push an old, vulnerable version.
- Signing oracles can sign future packages.

Mitigations

- Replay
  - Cookie and authentication headers are blocked.
  - Servers are advised to strip request authentication before processing a to-be-signed exchange, and to only sign Cache-Control:public responses.
  - Could enforce Cache-Control:public but currently don't.
- Downgrade
  - Signature validity capped to 7 days (=OCSP validity). Servers can choose shorter expirations.
  - Clients could fetch validityUrl aggressively in the non-prefetch case.
- Signing Oracles
  - New X.509 extension.
  - Could sign over stapled OCSP response but currently don't.

Chrome plans

Chrome is implementing a subset of the current draft behind a flag, described by draft-yasskin-httpbis-origin-signed-exchanges-impl.

Working with Google Search, Baidu, AMP, and publishers to prefetch both AMP and non-AMP signed exchanges from the search results pages.

Hoping to find another hub website to also prefetch their link targets.

If the above goes well, Origin Trial by the end of the year.
(https://www.chromium.org/blink/origin-trials)

Discussion

Backup Slides

Use Cases for non-origin signed exchanges

- Subresource Integrity
- Presence in a Binary Transparency log (*B)
- Appstore-like static analysis (*B)

(*B) With bundling.

Signed exchanges vs	draft-cavage-http-signatures
Algorithm determined by key type	Attacker specifies algorithm
Specifies how to look up key	Opaque keyId
Specifies payload integrity	Assumes client enforces Digest header
Signs hostname	Doesn't
Expires signatures	Vulnerabilities require key revocation