Securing AMP with Signed Exchanges (SXG)

Gabbi Fisher (Cloudflare), Frances Liu (Cloudflare), Zack Bloom (Cloudflare)

To create a faster browsing experience for mobile users, many content publishers use aggregators such as Google AMP to pre-fetch and serve their content from a cache hosted by the aggregator. Even though this provides significant speed advantages, it grants the platforms overreaching power over publisher-generated content. Aggregators could decide at any moment to change the content of millions of websites without visitors having any way to discover it.

It is clear that these aggregators have been successful at gaining adoption throughout the web, and that adoption is not likely to decline in the immediate future. Cloudflare views signed exchanges (SXG), the authenticity component of web packaging, as a means of restoring publisher power over the content they create. With signed exchanges, it's no longer possible for any external party to add, remove, or modify the publisher content. Web packaging makes it possible for a publisher to trust that their content is being served without modification which restores a critical check on aggregator power and maintains the veracity of the open-web.

As a CDN, one of Cloudflare's foremost responsibilities is to ensure that internet users receive authentic content securely. Publishers place their trust in CDNs to deliver their content with no changes; SXG provides a formal mechanism for verifying the integrity and authenticity of what content is delivered by stakeholders across the Internet, even when content is served by a CDN they do not have an existing trust relationship with. We are also supportive of marrying increased web performance with security, which SXG accomplishes for the AMP ecosystem.

One of the core outcomes of web packaging, origin substitution, allows for the faster delivery of trusted content to mobile (and potentially remote) internet users. Knowing that origin substitution introduces a paradigm shift in how we deliver content, we are keen to ensure this SXG practice is robust against bad actors.

A concern about SXG is the potential for attackers to use another domain's mis-issued or leaked certificate and private key pairs to impersonate that domain in TLS handshakes. In effect, SXG certs become more powerful than TLS ones, able to perform both SXG and TLS handshakes. We would like to see the SXG extension in certificates become critical, such that browsers would be forced to acknowledge SXG-only certs and prohibit their use in TLS handshakes.

Additionally, compromised certificate and private key pairs can be used to sign a fraudulent web packaged response from a website, and poison AMP caches with spoofed content that doesn't actually come from the victim's website. If such an attack happens, OCSP stapling will limit the scope of compromise to up to 7 days from certificate revocation. To Cloudflare, this isn't enough;

to ensure that SXG content only comes from its true origin, we also suggest adding a non-critical field to SXG certificates, which lists the only origins from which an AMP cache crawler could pull content packaged with a SXG certificate.

These changes require input from both Certificate Authorities and browsers, which is why we are keen to advance discussion at the IAB about approaches to further secure web packaging and improve its utility.