draft-kampanakis-tls-scas-latest-00  (was draft-thomson-tls-sic)

https://github.com/csosto-pk/tls-suppress-intermediates

Martin (Mozilla)

Panos (AWS)

Cameron (AWS)

Bas (Cloudflare)
Problem: TLS is heavy in auth data

- TLS includes a few Sigs & PKs
  - $(x+1)$ Sigs + $(x+1)$ Public Keys, where $x$ is the # of ICAs in the chain
  - 1 CertificateVerify signature
  - 2+ SCT signatures (WebPKI)
  - 1 OCSP signature (sometimes)

- Issues
  - Post-quantum Signature and Public Key sizes
    - can lead to 10+ KB auth data size increases
    - will introduce at least one round-trip in QUIC
  - Wi-SUN Field Area Networks, IEEE 802.15.4 mesh networks
ICA suppression in TLS 1.3

- Pre-acquire a “fresh” (TBD3-time) ICAs list and
- Ask the peer to not send ICAs by using `tlsflag` TBD1 in
  - `ClientHello` (server auth)
  - `CertificateRequest` (mutual auth)

Why
- TLS (including Web) PQ auth data stay within acceptable levels
  - Saves ~3.2 / 1.6 KB for 1 ICA with NIST Round 3’s two leanest PQ Sig finalists
  - Saves ~6.4 / 3.1 KB for 2 ICAs with NIST Round 3’s two leanest PQ Sig finalists
- Low hanging fruit
About ICA lists

• WebPKI: Total <1,500 ICAs / ~1-2 MBs compressed
• In some (non WebPKI) usecases, the ICA list can be built dynamically.

• Send ICAs regardless of tlsflag to prevent failures, if your ICAs are not
  • published (constrained) (MSRP 2.8 may change that)
  • in the list hosted by a public repo (e.g. CCADB)

• Similar Precedents
  • Mozilla already uses an ICA Pre-load list
  • Browsers build and distribute revocation lists
  • draft-ietf-tls-ctls defines a compression certificate dictionary
Open Questions

• What is the recommended TBD3-time?

• Who maintains the list of ICAs?
  • Client / browser vendor
  • CCADB or other public repo.

• What if there is a failure
  • Connection re-try and its impact on security and privacy
    • Could the fallback logic allows for downgrade style of attacks?
    • Active attack analysis.
  or can we assume no failure?
Closing Comment & Asks

• Challenges for WebPKI
  • We believe addressing them is possible
  • But also, let’s not forget, TLS is not just for the Web

• Discussion on the draft in the WG or git repo
  https://github.com/csosto-pk/tls-suppress-intermediates

• Consider it for WG adoption after NIST announces its Round 3 picks.