Attested TLS Token Binding

Giri Mandyam

draft-mandyam-tokbind-attest

https://datatracker.ietf.org/doc/draft-mandyam-tokbind-attest/

Recap

- Bearer tokens are still applicable, but client must prove possession of a private key on every TLS connection to a server
- Current specification requires signing of payload that includes
  - Exported Key Material (RFC 5705)
  - Tokbind.type and Tokbind.KeyParameters
- User agent (browser) could maintain private keys associated with TLS token binding
  - Problem: User agents are usually implemented in user space; private keys may be vulnerable
    - Attacker that obtains private key and bearer token can impersonate client
  - Problem not much better for native applications
    - Many OS's use open source libraries such as OpenSSL to implement secure socket connection
      - Private keys may still be stored in user space

https://datatracker.ietf.org/doc/draft-mandyam-tokbind-attest/

Remote Attestation (recap)

- Describes the process by which software executing on a device provides an assertion to a relying party about the integrity of its platform
  - The platform in question is the one controlling the tokbind private key
- The attestation can be based on several criteria, including 'health' measurements of platform
  - An assessment of the operating system kernel
  - Enumeration of 3rd-party applications installed in environment where credential is stored
  - Suspicious events such as protected memory access
- Attestation data is formed by combining these indications into a compact data structure that can be sent to a relying party
  - Attestation data is used to form an attestation statement, which is the actual message sent to the relying party
  - Attestation statement should be cryptographically-verifiable (signed and/or encrypted)

https://datatracker.ietf.org/doc/draft-mandyam-tokbind-attest/

Tokbind Impact

- Inclusion of an attestation in the tokbind message enabled through a protocol extension
  - Sec. 3.4, draft-ietf-tokbind-protocol: "One of the possible uses of extensions envisioned at the time of this writing is attestation …"
- Current I.-D. proposes a pairing of attestation type and attestation data for extension
- Initial types are currently
  - TCG – TPM v1.2 specifications
  - Android Keystore
  - Registry for future attestation extensions

https://datatracker.ietf.org/doc/draft-mandyam-tokbind-attest/

Tokbind Impact (cont.)

- All current proposed attestations involve signing of the EKM
- Verification procedures leverage heavily from Webauthn procedures
  - https://w3c.github.io/webauthn/#android-key-attestation
  - https://w3c.github.io/webauthn/#tpm-attestation
  - Primary differences
    - Webauthn attestation signature over clientData||AuthData
    - Webauthn requires transmission of signing algm. in addition to attestation data and cert
      - Current I.-D. leverages algm. field in certificate

https://datatracker.ietf.org/doc/draft-mandyam-tokbind-attest/

TLS Handshake Impact

- Current TokBind specs do not provide a means for client/server to advertise extension capabilities
  - Could allow for server to suppress client extensions for which it has no interest
- I.-D. now proposes new TLS extension codepoint “token_binding_with_extensions”
- Client Hello includes list of supported extensions
- Server Hello includes list that is a subset of Client Hello list
  - Client can only send extensions that Server lists in its Hello

https://datatracker.ietf.org/doc/draft-mandyam-tokbind-attest/

Open Questions

- Should there even be an extensions negotiation mechanism?
  - Can server just ignore tokbind.extensions that it doesn't support/care about?
- Should supported attestation types be advertised?
- Should supported attestation trust anchors be advertised?
- Are the current list of initial supported extensions sufficient?
- Are the verification procedures accurate?

https://datatracker.ietf.org/doc/draft-mandyam-tokbind-attest/

Recommendations to WG (in order)

- Answer open questions
- Adopt I.-D. as standards-track
- Co-editors are welcomed

https://datatracker.ietf.org/doc/draft-mandyam-tokbind-attest/