0-RTT with Token Binding

Nick Harper
IETF 103

Overview

- Problem statement
- Assumptions
- Options
- Security properties
- Implementation considerations

Problem statement

Some clients and servers may wish to support both 0-RTT and Token Binding on the same connection.

To send a TokenBindingMessage in early data requires using early_exporter_master_secret (instead of exporter_master_secret) for deriving the signed exporter value.

Assumptions

Token Binding keys are non-extractable/hardware protected.

An attacker that “has access to” a Token Binding key can sign arbitrary payloads.

An attacker will not substitute a hardware-backed keystore with an attacker-controlled software-backed keystore.

An attacker with access to a client’s session cache also has access to Token Binding keys.

Options

Can both 0-RTT and Token Binding be negotiated on the same connection?

> If no, this looks like draft-ietf-tokbind-tls13.

Can a TokenBindingMessage be sent in early data?

> If no, we only ever use exporter_master_secret for the signed exporter value. If yes, the early_exporter_master_secret needs to be used at least for the TokenBinding in early data.

Which exporter?

- Always use early_exporter_master_secret
  - As described in expired draft-ietf-tokbind-tls13-0rtt
- Have client switch to using exporter_master_secret “as soon as possible”
  - Requires application level signal to ask client to retry using exporter_master_secret (similar to HTTP 425 Too Early), or it degrades to the above
- Use early_exporter_master_secret for TokenBinding in early data, and exporter_master_secret for TokenBinding post handshake
  - This is unimplementable

Security differences in exporter secrets used

A signature over the exporter from exporter_master_secret proves that the sender had access to the Token Binding key at the point in time when the TLS handshake finished.

A signature over the exporter from early_exporter_master_secret proves that the sender had access to the Token Binding key after the NewSessionTicket was received —OR— the ClientHello and early data were replayed verbatim.

Implementation considerations

Switching exporters requires a signal in the TokenBinding struct of which exporter was used. (Or the server needs to try both exporters when verifying the signature.)

Define a new TLS extension for negotiating use of both Token Binding and 0-RTT on same connection.