draft-ietf-tls-extended-key-update-06

Hannes Tschofenig

Michael Tüxen

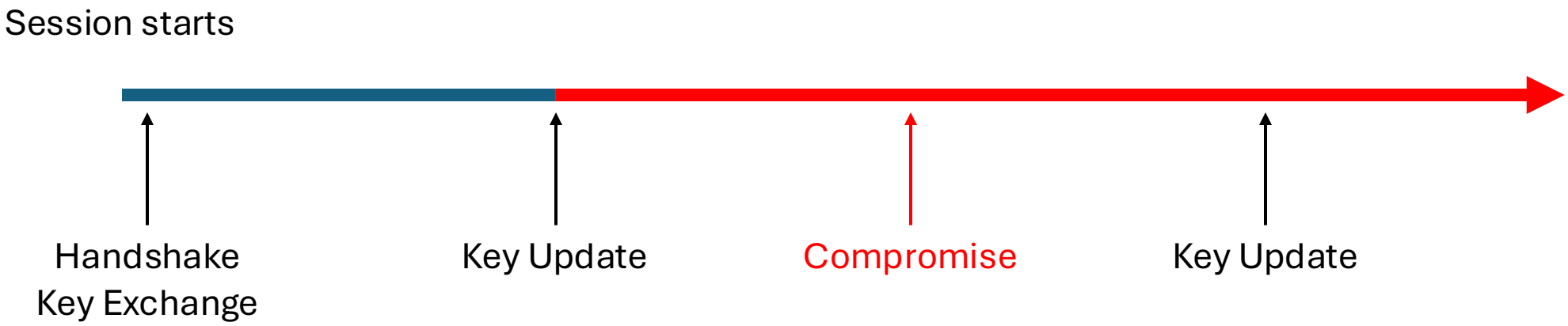
Tirumaleswar Reddy

Steffen Fries

Yaroslav Rosomakho

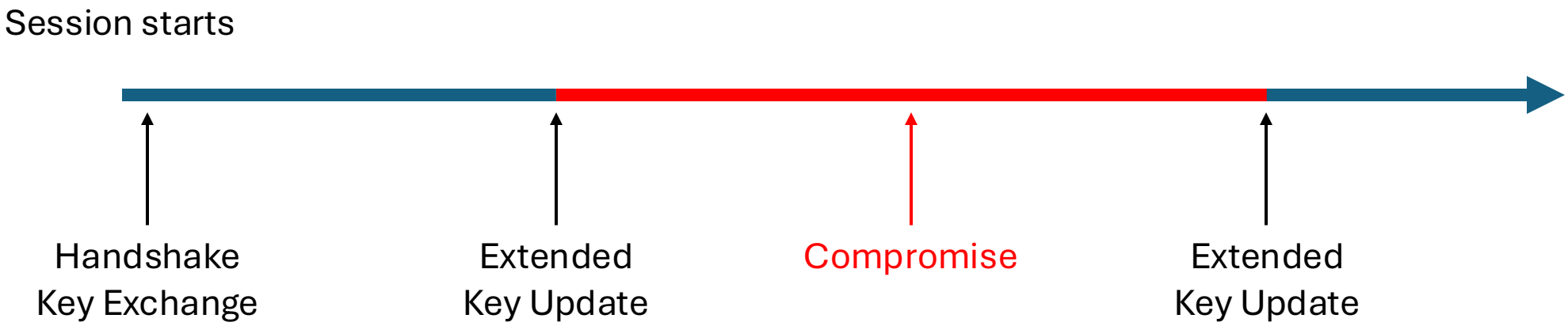
TLS
IETF124, November 2025, Montreal

Recap: Standard Key Update Security



Attacker can decrypt all packets since the previous Key Update until the end of the session

Recap: **Extended** Key Update Security



Attacker can decrypt only packets between Extended Key Updates

Updated in -06: terminology

Converge on “post-compromise security” with a reference to IEEE paper “On Post-compromise Security” (2016) by Katriel Cohn-Gordon, Cas Cremers and Luke Garratt.

Updated in -06: converge to a single message

ExtendedKeyUpdate (EKU) with uint8 message subtype.

Three subtypes defined:

- key_update_request (0)
- key_update_response (1)
- new_key_update (2)

IANA registry will be requested for potential future extensions

Updated in -06: no more failures

- Extended Key Update is always expected to (eventually) succeed.
- No more error codes.
- If responder is too busy, it MAY delay response
  - If requester runs out of patience it terminates the connection
  - DTLS consideration – responder sends ACK so that requester won't keep retransmitting

Added in -06: security considerations

- Scope of key compromise
- Post-compromise security
- Denial of Service
- Operational Guidance

Added in -06: TLS/DTLS state machines

Practical guidance for implementers

Next Steps

- Align labels and key naming with TLS 1.3 - #79 (already in editor's copy)
  - There does not seem to be any value in changing HKDF labels
- More clarification around impact on exporter APIs - #74
- Finish non-normative state diagrams in appendices - #78
- Clarify security goals - #77
- Clarify threat model - #76
- More implementations and interoperability testing (we have two prototypes – based on Rustls and mbedtls)
- More reviews and further refine wording

Thank you!