draft-ietf-quic-extended-key-update-01

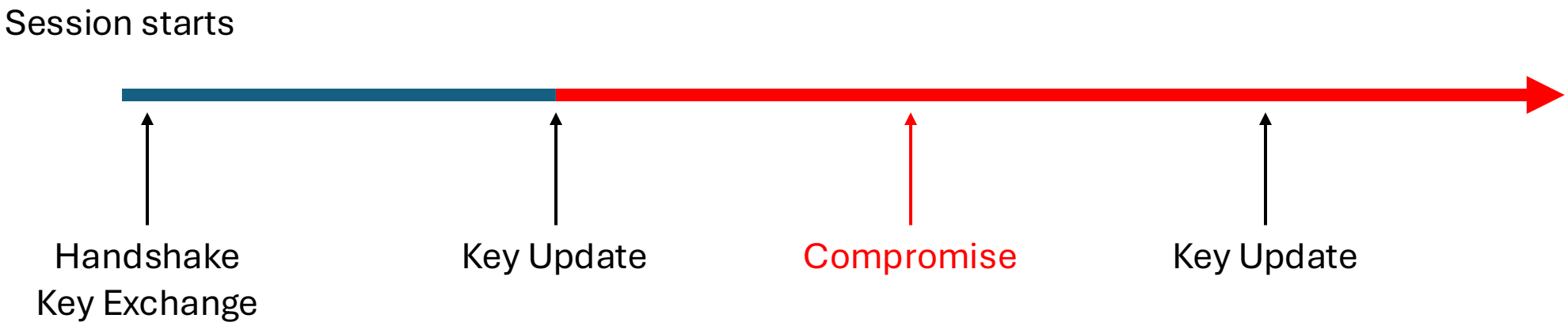
Yaroslav Rosomakho

Hannes Tschofenig

Tirumaleswar Reddy

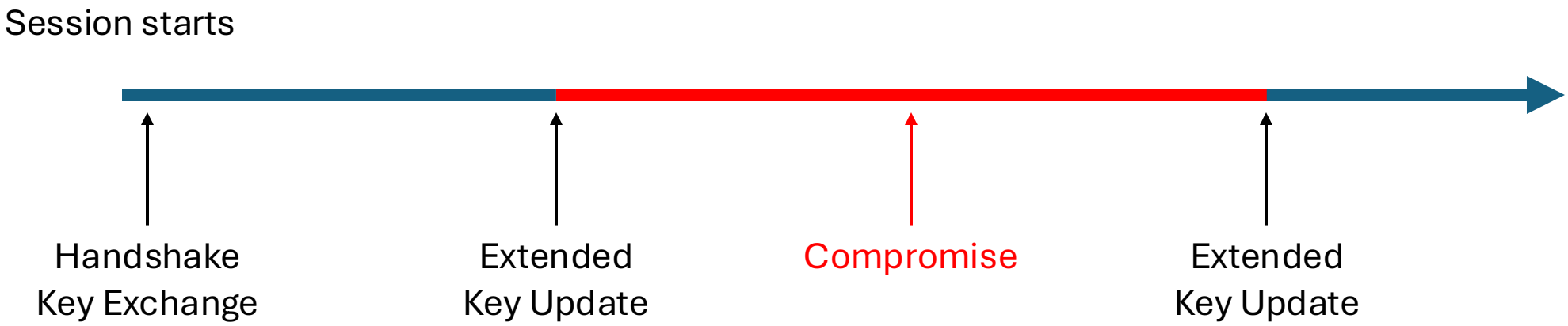
QUIC
IETF123, July 2025, Madrid

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

New in -01: sync with TLS extended key update changes

- Replaced single HDKF Expand
- Derive new exporter and resumption secrets in addition to application traffic secrets

Next Steps

- Implementations and interoperability testing
- Further refine wording

Thank you!