Extended Key Update for QUIC

`draft-rosomakho-quic-extended-key-update-00`

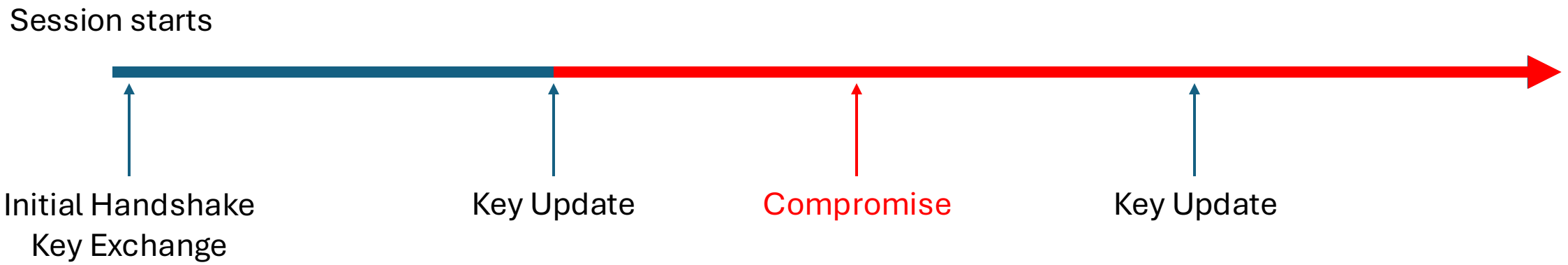
Yaroslav Rosomakho*

Hannes Tschofenig

Traditional Key Update

- There is only one Key Exchange event for the whole duration of QUIC session
- Traditional Key Update (Key Phase bit flip) derives new traffic secrets from the previous ones
- Good enough to:
  - Overcome AES-GCM confidentiality limit (2^{23} according to RC9001)
  - Keep confidentiality of historic packets encrypted with previous keys

Traditional Key Update security

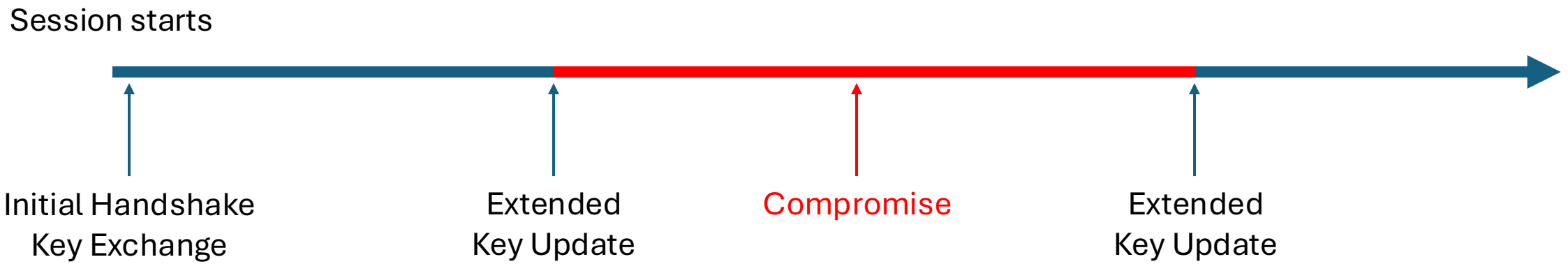


Attacker can decrypt all packets since the previous Key Update until the end of the session

Extended Key Update for QUIC

- Based on Extended Key Update for TLS 1.3 (draft-ietf-tls-extended-key-update)
- Extended Key Update triggers a fresh Key Exchange
  - Same TLS Group is used as during initial TLS handshake
- Extended Key Update support is negotiated in TLS handshake (through a TLS flag)
- New Key Exchange uses TLS 1.3 messages in CRYPTO stream
- Unlike TLS 1.3 Extended Key Update confirmed with a Key Phase bit swap
- Unlike TLS 1.3 Extended Key Update replaces traditional Key Update in QUIC

Extended Key Update security

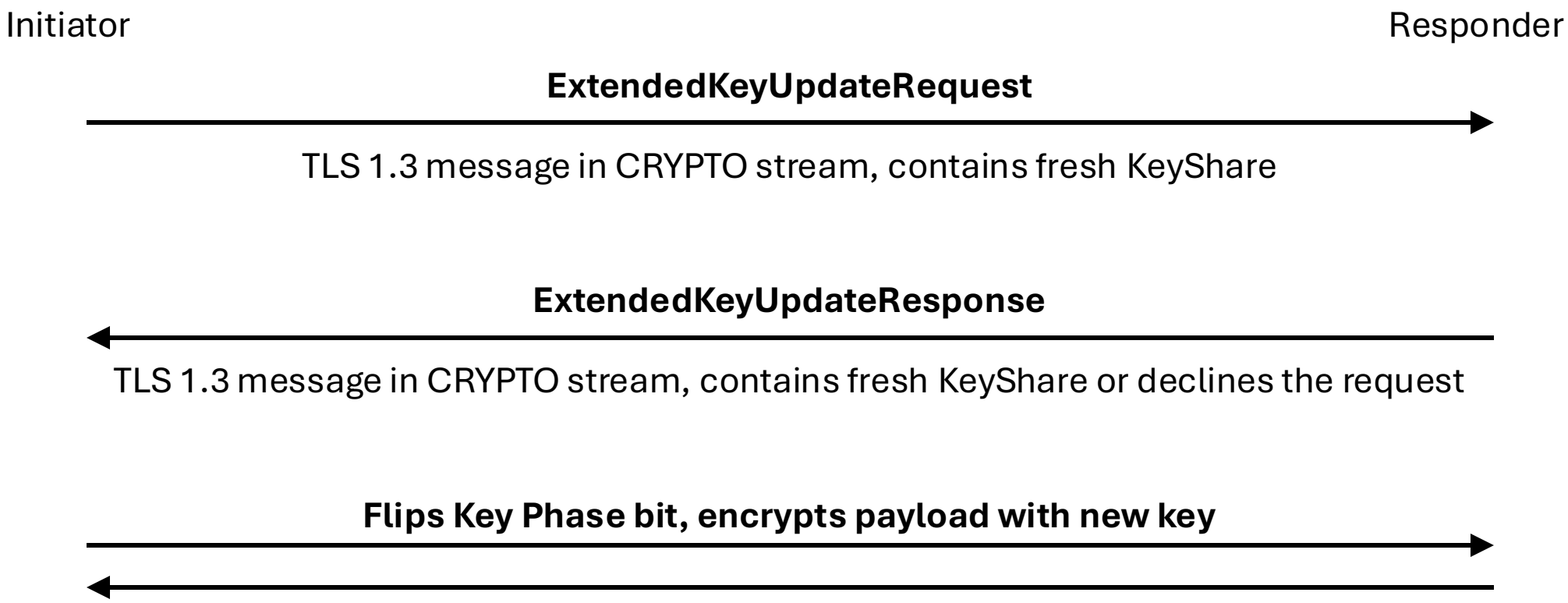


Attacker can decrypt only packets between Extended Key Updates

Why does it matter?

- Long-lived sessions (actually, QUIC is really good for those)
  - Telco Signaling
  - Industrial IoT
  - MASQUE/VPN
- IKE / SSH / TLS 1.2 / DTLS 1.2 displacement
  - Protocols listed above support periodic key exchange
- TLS 1.3 adopting it

Extended Key Update flow



Thank you!

- Is this use case (security of long-term sessions) relevant for you?
- Do you have opinions on the solution design?
- Would WG like to adopt this work?