

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

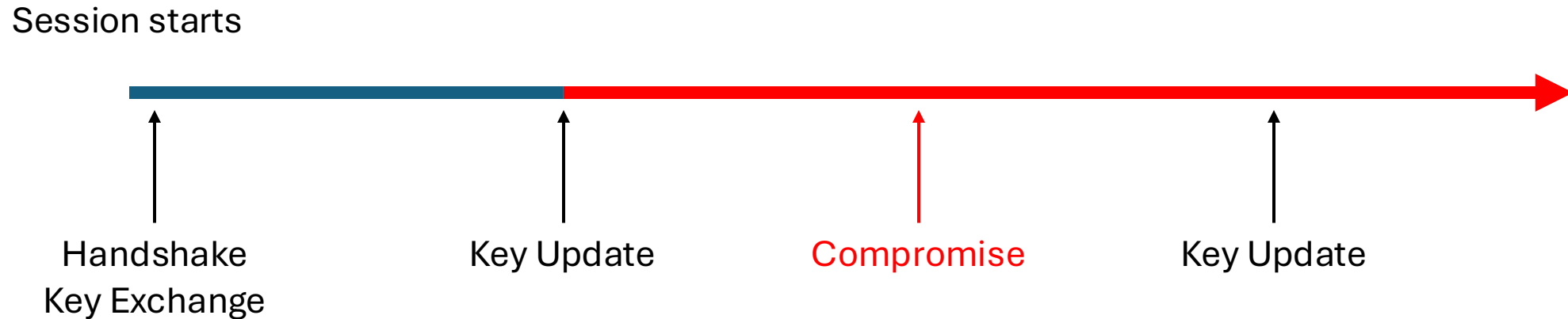
Yaroslav
Rosomakho

Hannes
Tschofenig

Tirumaleswar
Reddy

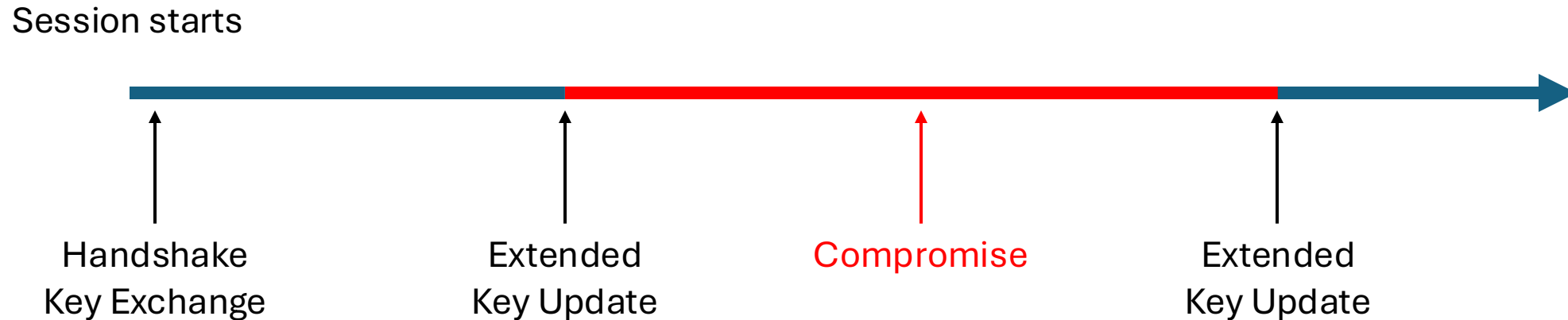
QUIC
IETF123, July 2025, Madrid

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 HKDF Expand
- Derive new exporter and resumption secrets in addition to application traffic secrets

```
Master Secret N
|
v
Derive-Secret(., "key derived", "")
|
v
(EC)DHE -> HKDF-Extract = Master Secret N+1
|
+-----> Derive-Secret(., "c ap traffic2",
|               ExtendedKeyUpdateRequest ||
|               ExtendedKeyUpdateResponse)
|               = client_application_traffic_secret_N+1
|
+-----> Derive-Secret(., "s ap traffic2",
|               ExtendedKeyUpdateRequest ||
|               ExtendedKeyUpdateResponse)
|               = server_application_traffic_secret_N+1
|
+-----> Derive-Secret(., "exp master2",
|               ExtendedKeyUpdateRequest ||
|               ExtendedKeyUpdateResponse)
|               = exporter_master_secret_N+1
|
+-----> Derive-Secret(., "res master2",
|               ExtendedKeyUpdateRequest ||
|               ExtendedKeyUpdateResponse)
|               = resumption_master_secret_N+1
```

Next Steps

- Implementations and interoperability testing
- Further refine wording

Thank you!