MTC experiment early results

Luke Valenta (Cloudflare)
PLANTS IETF 125

Merkle Tree Certificates experiment

Goal: evaluate feasibility and performance of MTCs

Merkle Tree Certificates experiment

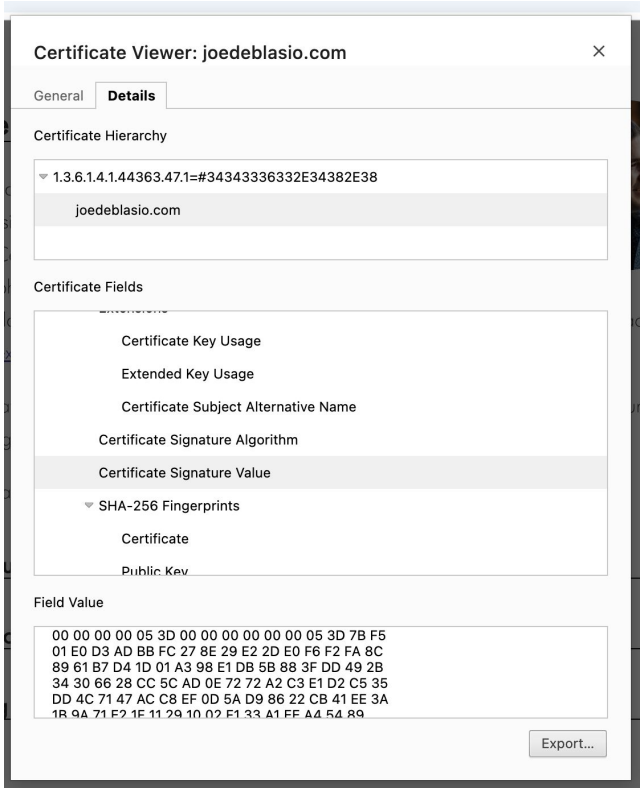
Goal: evaluate feasibility and performance of MTCs

Cloudflare runs

- TLS server — currently 1000 Cloudflare-proxied domains
- "bootstrap" MTC CA
  - Every MTC is backed by a traditional cert chain
  - Restricts experiment to classical signatures
  - Use 7 day cert validity
- Limit to landmark MTCs
  - Landmarks every hour
  - Largest proof size: 512 bytes (Web scale will be 700-800)

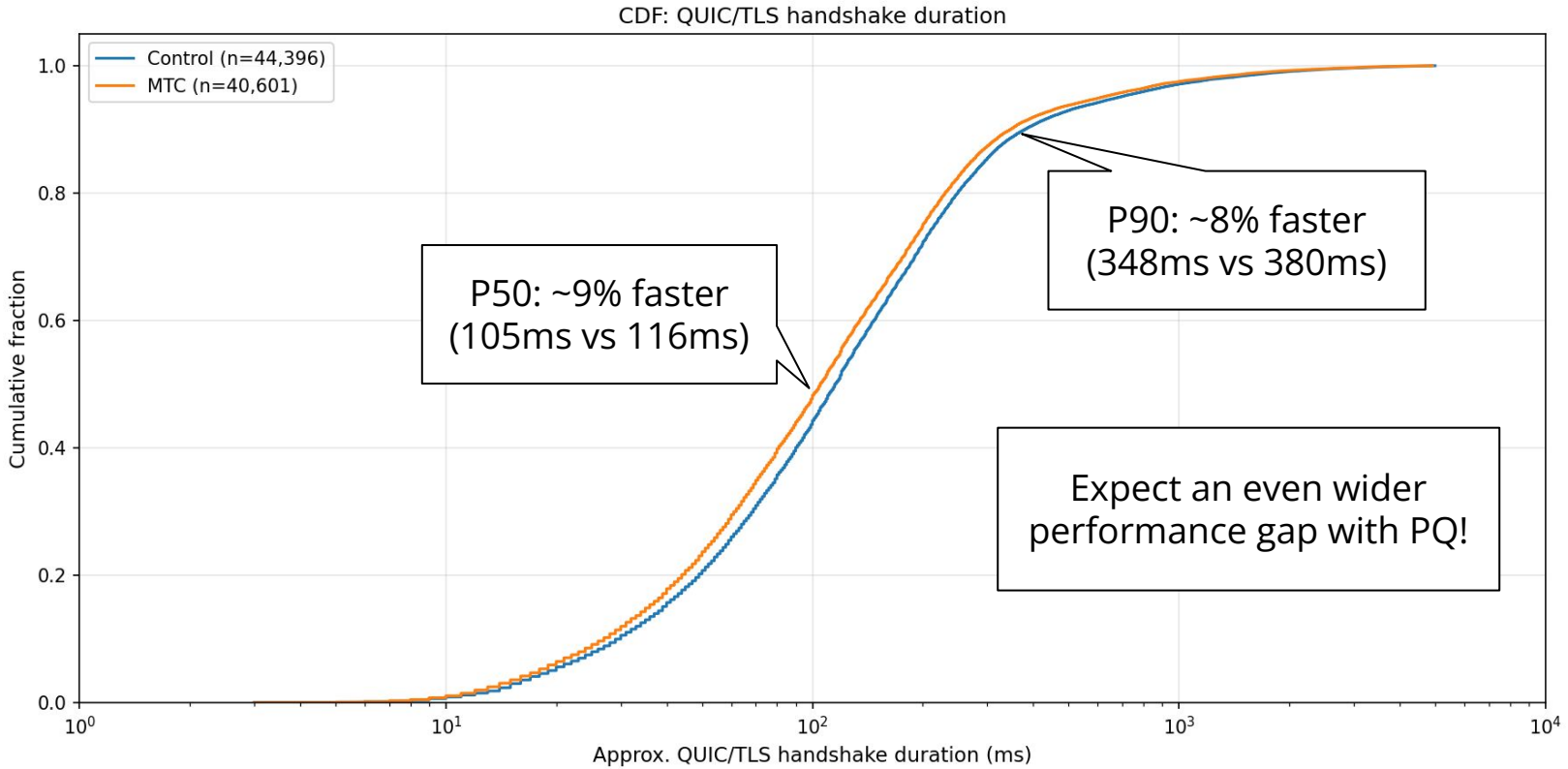
Chrome runs

- TLS client — currently 50% of Chrome Beta 146+
- Update service to validate and distribute landmarks
  - Client state for landmarks: ~10KB

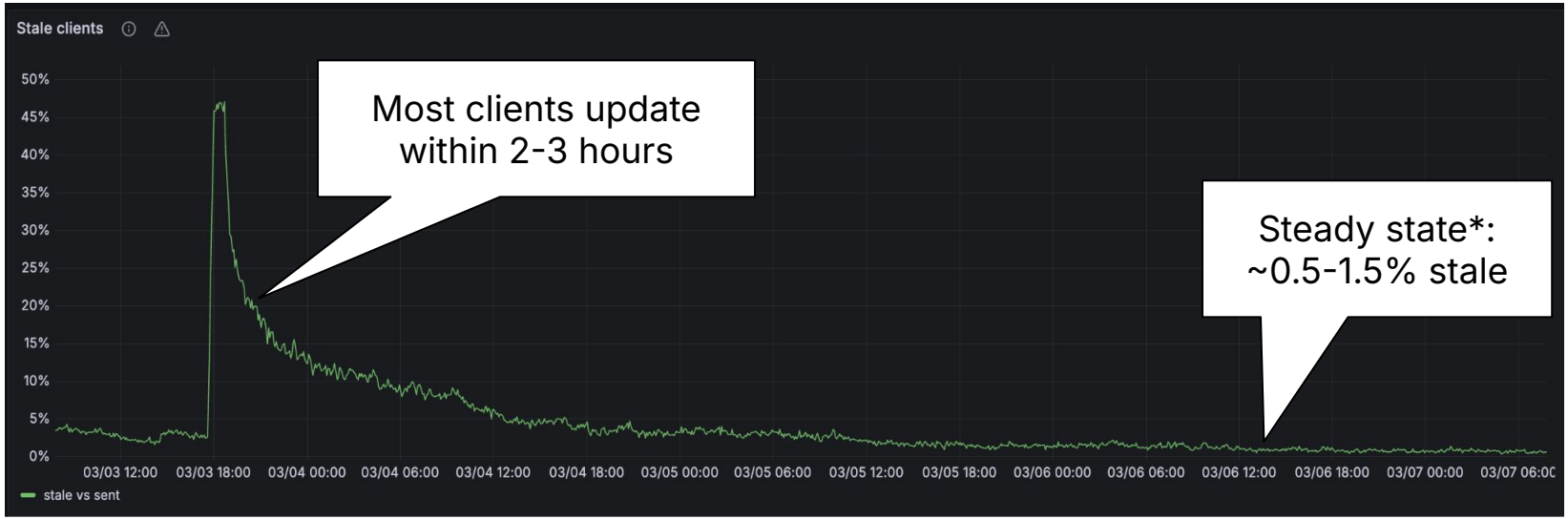


MTC in Chrome Beta

Are landmark MTCs faster than *classical*?



How quickly do clients get landmarks?



*This is an *upper bound* due to experimental quirks

What we’ve learned (so far)

MTCs work (!), and are used to secure real Internet traffic today.

What we've learned (so far)

MTCs work (!), and are used to secure real Internet traffic today.

How do MTCs perform?

- Significant latency improvements in TLS, *even over classical* signatures
- Generally not a problem for clients to stay up-to-date with landmarks

What we've learned (so far)

MTCs work (!), and are used to secure real Internet traffic today.

How do MTCs perform?

- Significant latency improvements in TLS, *even over classical* signatures
- Generally not a problem for clients to stay up-to-date with landmarks

Operational experience

- We've had to shake out a few bugs on both client and server side
- Middlebox interference thus far is a non-factor (TLS 1.3 encrypts server cert)