Using LURK for CDNI DNS Delegation for Video Streaming

Hackathon
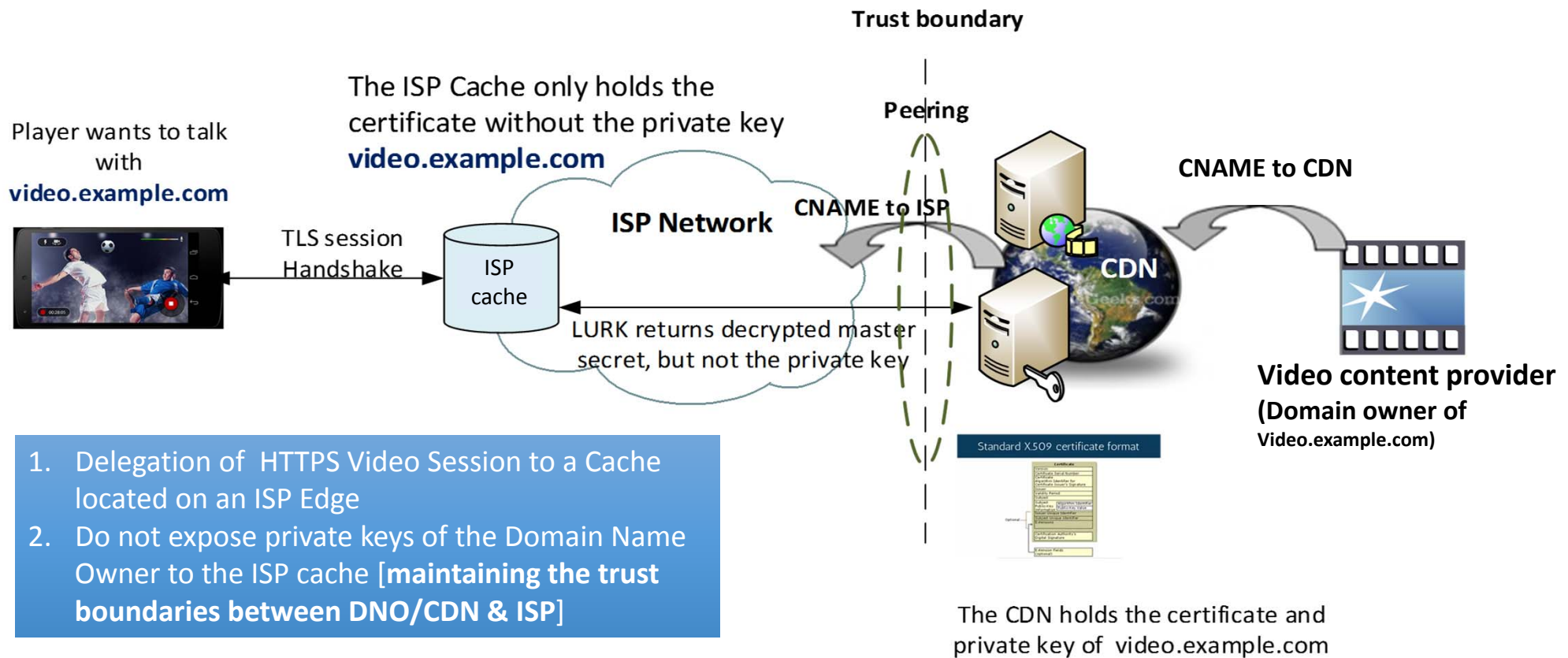
IETF101

London, UK

March 17-18, 2018
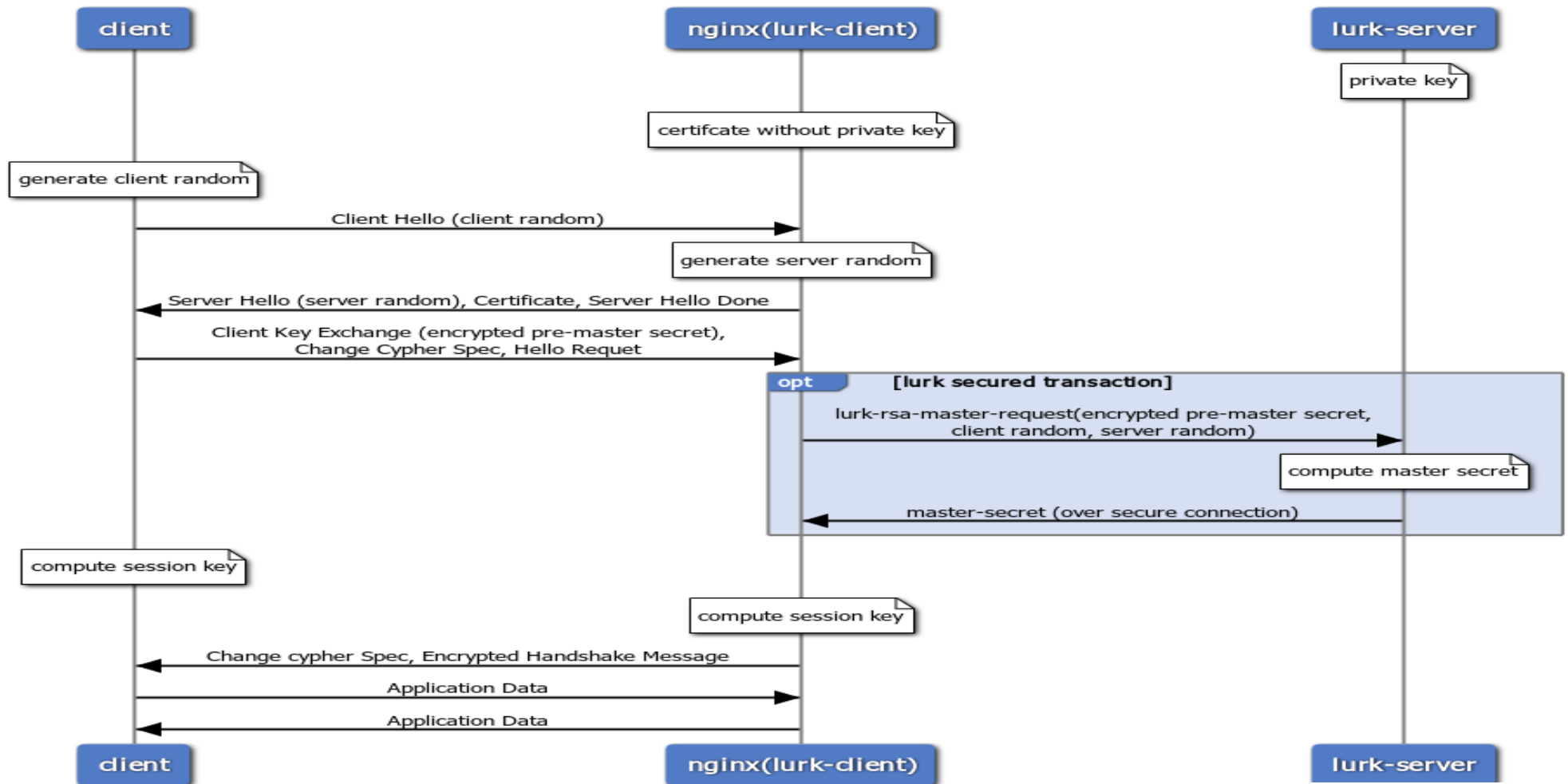
Delegation of HTTPS Video Session
CDNI Use case

Trust boundary

Peering

Player wants to talk with
video.example.com

The ISP Cache only holds the certificate without the private key
video.example.com

TLS session Handshake

ISP cache

ISP Network

CNAME to ISP

CNAME to CDN

CDN

LURK returns decrypted master secret, but not the private key

Standard X.509 certificate format

Video content provider
(Domain owner of
Video.example.com)

1. Delegation of HTTPS Video Session to a Cache located on an ISP Edge
2. Do not expose private keys of the Domain Name Owner to the ISP cache [**maintaining the trust boundaries between DNO/CDN & ISP**]

The CDN holds the certificate and private key of video.example.com

TLS Handshake over LURK

LURK TLS RSA handshake

Delegation Interoperability Test

- What did the Interoperability accomplished?
  - Established an HTTPS session between the client and the Edge Server (ISP cache)
  - Edge Server requested master secret creation from the LURK server. The LURK Server used private key of the Domain Name Owner residing on the LURK Key Server
  - Browser played-back user requested content hosted at the ISP Cache
    - (Barcelona vs Atletico Madrid)

- Interoperability Using:
  - Client Browser (Chrome/IE)
  - Edge Server (NGINX)
  - Made NGINX to use a patched OpenSSL
    - Integrated OpenSSL with LURK client RSA implementation
    - Used masterkey generated by LURK Key Server
  - Key Server (Python)
  - For Hackathon interoperability we tested RSA Handshake
    - Diffie Hellman is next on to-do list

IETF 101 LURK Hackathon Participants

- Daniel Migault (Ericsson)

- Ori Finkelman (Qwilt)

- Dmitry Kravkov (Qwilt)

- Frederic Fieau (Orange)

- Emile Stephan (Orange)

- Sanjay Mishra (Verizon)

LURK I-D:
1. https://datatracker.ietf.org/doc/draft-mglt-lurk-lurk/
2. https://datatracker.ietf.org/doc/draft-mglt-lurk-tls12/

Why LURK?

- Using LURK am I increasing load?
  - Video sessions are long persistent session
    - Single handshake can stay for the duration of Video Streaming session
    - TLS Session resumption can be used in case of connection disconnect
- Using LURK what is my Latency?
  - Impact limited to session establishment
  - Subsequent requests use persistent TLS session information
- What about key server scaling?
  - Within CDN interconnection (CDNI), uCDN holds key and no additional infrastructure specific to LURK request/response
    - Key server can be deployed to uCDN and scale naturally with uCDN growth
    - Overall, volume and per user transaction is reduced with dCDN delegation
- What about H/A considerations?
  - As above