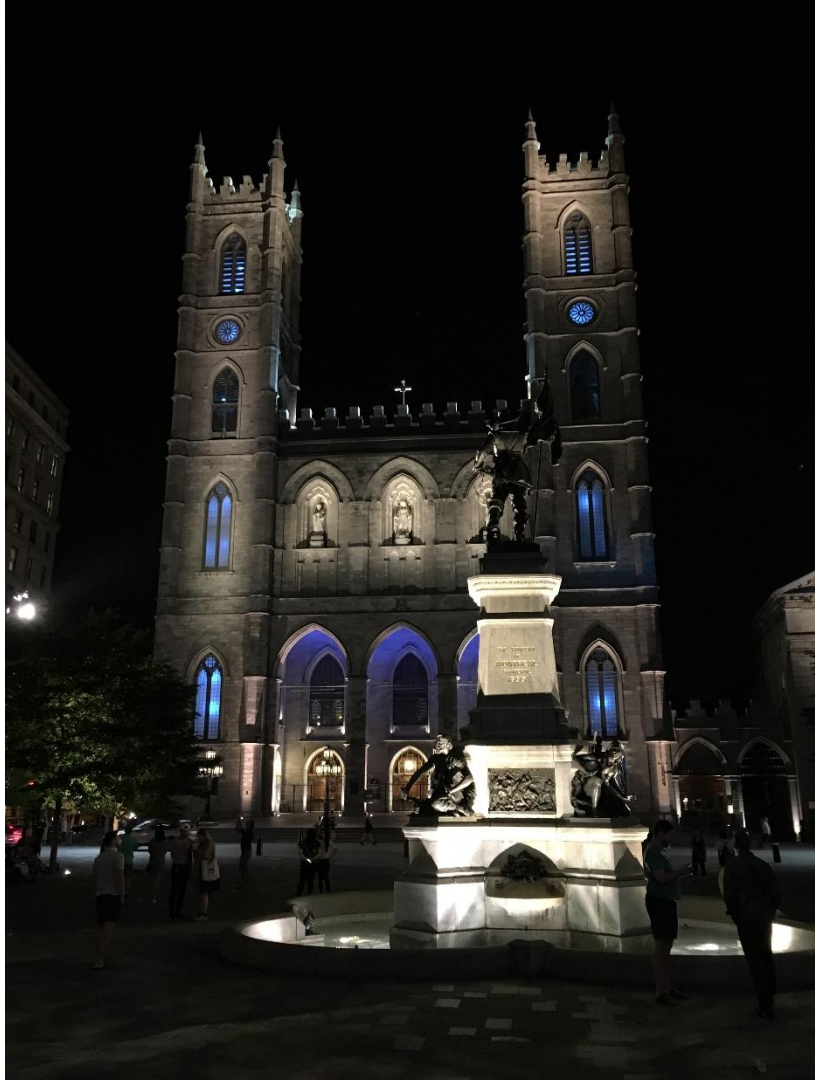
IETF Hackathon: LURK

IETF 102

14-15 July, 2018

Montreal



LURK – IETF 102 Hackathon

- What we aim to address:
  - Protect security credentials of a security service
  - Isolate operations associated to these credentials into specific cryptographic services

- Use Case:
  - Enable delegation of video sessions from one domain, such as a Content Delivery Network (CDN) to another domain such as an Internet Service Provider (ISP) hosted “caches”, where a CDN can securely store content but without sharing of private keys
- Relevant RFC’s:
  - https://datatracker.ietf.org/doc/draft-mglt-lurk-lurk/
  - https://datatracker.ietf.org/doc/draft-mglt-lurk-tls12/
  - https://tools.ietf.org/pdf/draft-mglt-lurk-tls13-00.pdf

What got done

- What we achieved?
  - Two running implementations: cLURK and pyLURK
- What the team agreed?
  - Proverif implementation to formally verify the LURK protocol
- Links to github
  - https://github.com/mami-project/KeyServer
  - https://github.com/mglt/pylurk
  - https://github.com/jesusalber1/clurk
- New design?
  - ECDHE implemented in pyLURK
  - Disabling non-secure configurations (LURK TLS 1.2 draft)

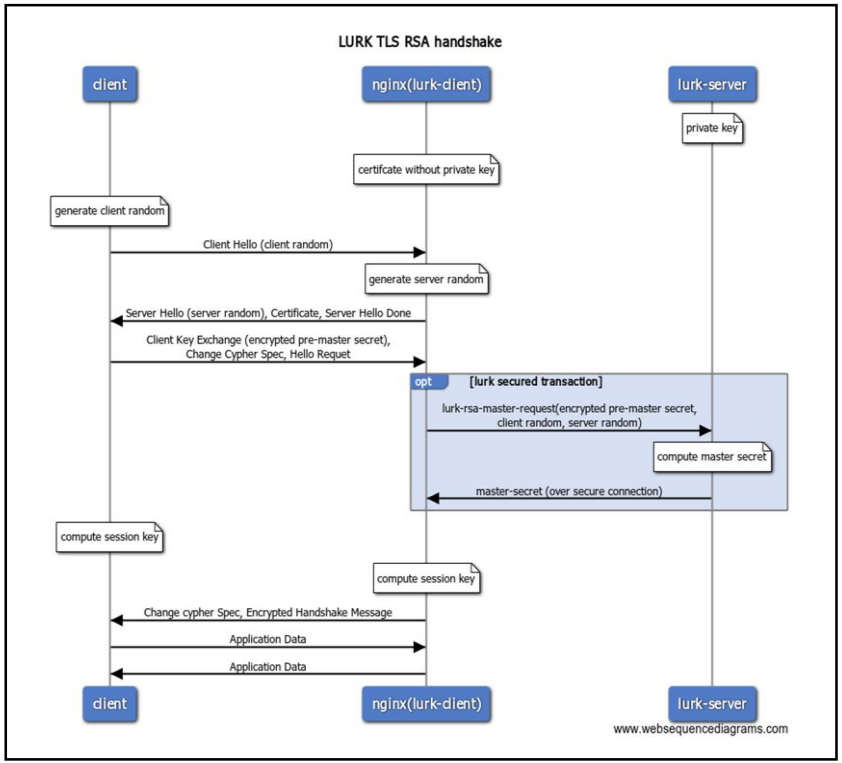
What we learned

- Lessons learned from this hackathon?
  - Integrate with NGNIX OpenSSL
  - Trusted environment
- Issues with existing draft
  - Fully implement LURK extensions for TLS 1.2
- Future implementation Plans
  - Formal verification for LURK extension for TLS 1.3 (using Proverif)

Wrap Up

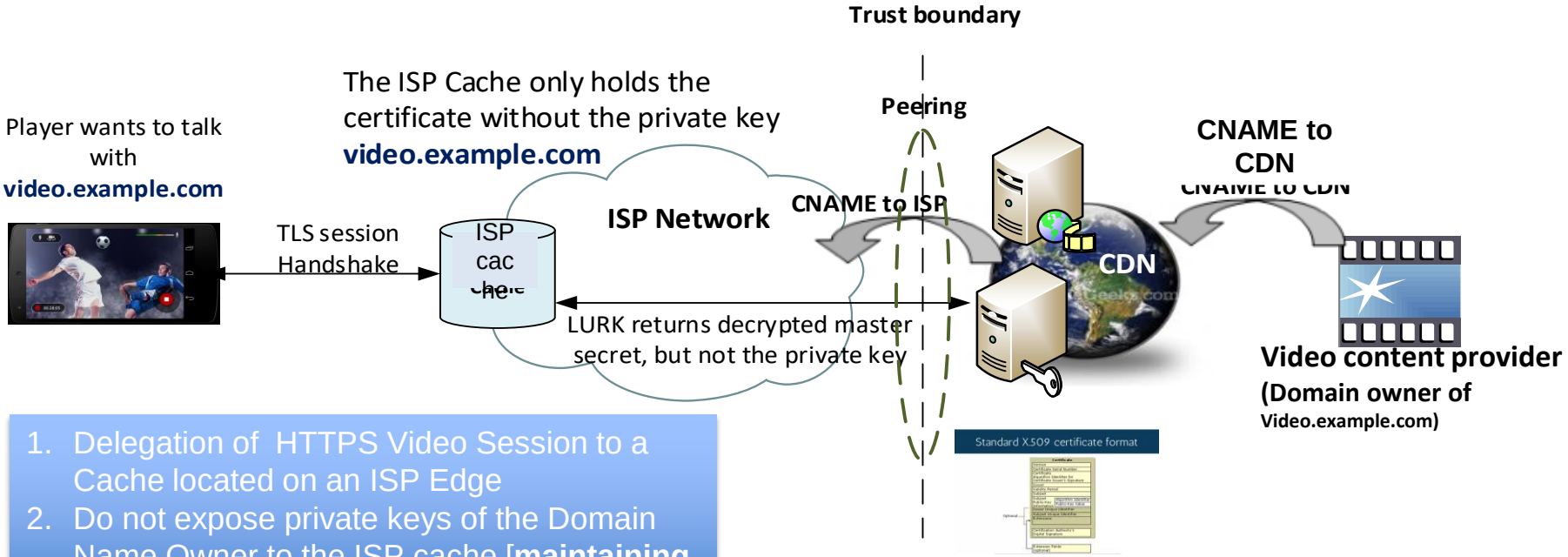
Team members:

- Daniel Migault (Daniel.Migault@ericsson.com)
- Sanjay Mishra (sanjay.Mishra@verizon.com)
- Ori Finkelman (orif@qwilt.com)
- Dmitry Kravkov (dmitryk@qwilt.com)
- Frederic Fieau (Frederic.fieau@orange.com)
- Emile Stephane (emile.stephan@orange.com)
- Jesús Alberto Polo (ietf@jesusalberto.me)



Delegation of HTTPS Video Session

CDNI Use case



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