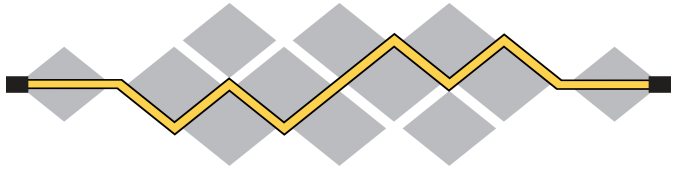
WebRtcEndpoint: improving establishment connection time



IETF®

IETF 96 Hackathon

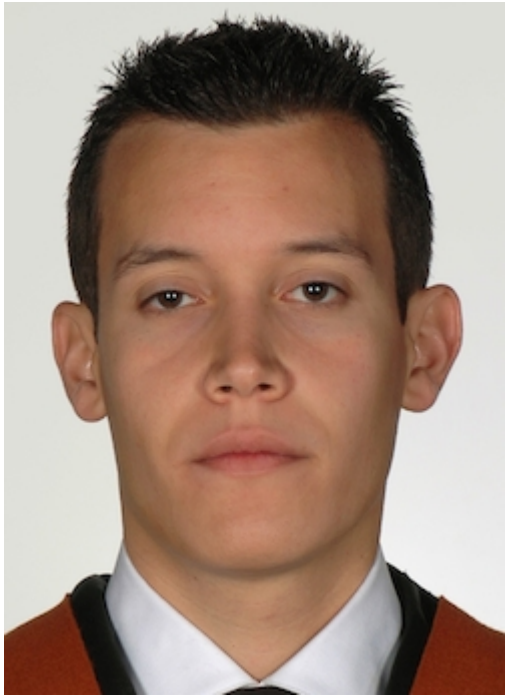
July 16-17, 2016
Berlin, Germany

Miguel París
mparisdiaz@gmail.com

Who I am

Miguel París

- Software Engineer
- Telematic Systems Master's
- Researcher at Universidad Rey Juan Carlos (Madrid, Spain)
- Kurento real-time responsible
- mparisdiaz@gmail.com
- Twitter: @mparisdiaz



Goals

- Support ECDSA in Kurento Media Server
  - [rtcweb] Security architecture: Making ECDSA mandatory
    - https://www.ietf.org/mail-archive/web/rtcweb/current/msg14754.html
- Verifying DTLS handshake
  - Chrome – KMS
  - Firefox – KMS
  - KMS - KMS
- Profiling
  - RSA vs ECDSA
  - Relate saved CPU to SRTP (protect/unprotect)

KURENTO

Implementation

- Use libssl 1.0.2d (OpenSSL)
- Generate EC private key
- Generate EC parameters from EC group
- Generate self-signed certificate
- Add configuration to use RSA or ECDSA

Verifying

- At the beginning it didn't work because we missed the next line, but thanks to David Benjamin's help we could fix it :D

```
EC_GROUP_set_asn1_flag (group, OPENSSL_EC_NAMED_CURVE);
```

- Then everything worked fine
  - Chrome – KMS 
  - Firefox – KMS 
  - KMS - KMS 

Profiling types

- Only time
  - Could be indicative
  - But it is not a good idea for precise comparatives
  - Depends on the CPU load, locks, number of context switchings, etc.
- CPU cycles per function
  - Deterministic measure
  - callgrind

KURENTO

Profiling results

CPU cycles/call	RSA	ECDSA
KEY GENERATION	~420M (RSA_generate_key)	~250k EC_GROUP_new_by_curve_name (110k) EC_KEY_generate_key (140k)
SIGN	~12.9M (RSA_sign)	~400k (ECDSA_sign)

- Key generation improvement: ~1680x
- Sign improvement: ~32x

KURENTO

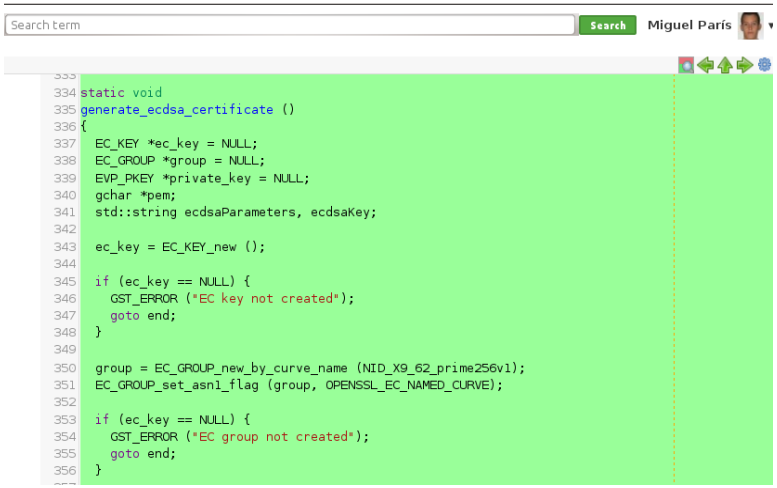
Comparing to SRTP

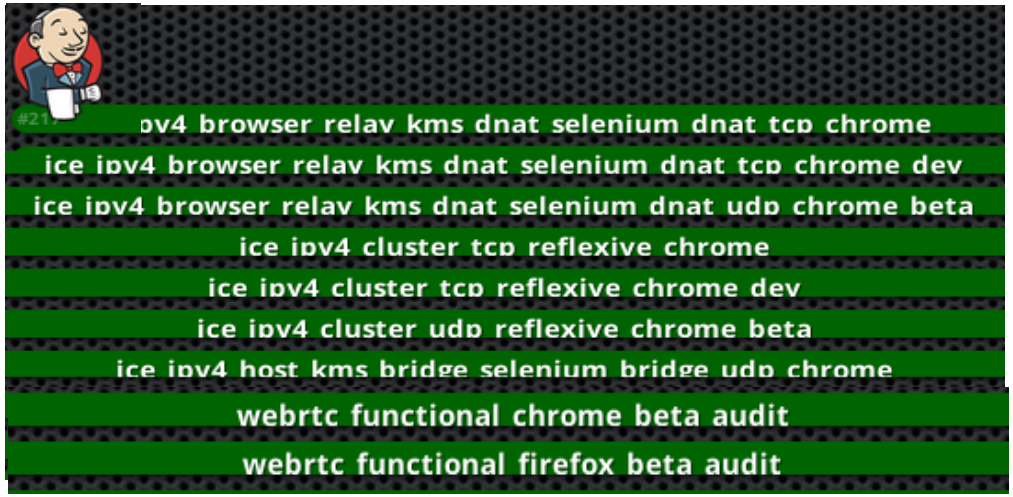
CPU cycles/call	RSA –> ECDSA (saving)	SRTP audio	SRTP video
KEY GENERATION	~420M	~9k (150-200 Bytes/packet)	~22k (~1200 Bytes/packet)
SIGN	~12.5M		

	Number audio packets	Audio seconds	Number video packets	Video (500kbps) seconds
KEY GENERATION	~46.5k	~920	~19k	~320
SIGN	~1400	~30	~570	~10

Future work

- Finish landing this improvements into Kurento Media Server
  - Code review (Gerrit)
  - Continuous Integration verifying (Jenkins)





  - Update KMS automatic profiling
- Contribute to GStreamer community
  - gst-plugins-bad: dtlsenc/dtlsdec elements
  - Also used by OpenWebRTC (Ericsson)

Thank you

http://www.kurento.org
http://www.github.com/kurento
info@kurento.org
Twitter: @kurentoms

http://www.nubomedia.eu

http://www.fi-ware.org

http://ec.europa.eu

Miguel París
mparisdiaz@gmail.com