Managing Radio Networks in an Encrypted World (MaRNEW) Workshop

24^{th} –25^{th} September, 2015

Atlanta, GA

https://www.iab.org/activities/workshops/marnew/

Orange

(Mohammed Dadas, Emile Stephan, Mathilde Cayla, Iuniana Oprescu)

In an encrypted environment, some of the useful information, needed by the operators to manage their networks are no longer accessible; this has negative impacts on all the involved entities (network operators, content providers, end users, ...).

As an example, the enforcement of HTTP streams' priorities according to their type, e.g. a streaming service and a non-real time service like a file download, is inefficient because the MIME Type of each stream needed for network management is not shared with the network. Hence prioritization cannot be achieved and the services will not operate in a correct way.

The encryption of flow types and of flow control information and the multiplexing at application layer also impacts all possibilities of dynamic network dimensioning as the network operator has no information to predict the traffic evolution in real time.

In Orange services, we often have the case where we use the MIME Types for prioritizing the streams and dynamically adjust the network dimensioning.
One common situation occurs when a user is watching a video online (streaming) and downloading an on-demand content (to use later). The MIME Types are transported as a field of the HTTP request.
With the HTTP[1][2][3][4] encryption this information cannot be retrieved at the network level, hence the two streams will be dealt with the same priority while one needs a real time delivery and will suffer a decrease of quality and this will impact the end user's service quality.

Another case is when for a some reasons, a specific content is downloaded or watched online by an increasing number of users, not being able to identify the content impacts not only the possibilities of caching it but also the possibility of providing more bandwidth to absorb the traffic increase needs.

One possible way to solve (or reduce the impact) if this issue could be to put some of the meta

data (needed for network management) in the transport layer (ie TCP) and to keep the other meta data (more user related) at the application layer (ie http); in this case, both the users will benefits from the advantages of a good network management and an improved privacy.

This evolution needs a cooperation framework between the application layer and the transport layer were we could investigate the needed evolutions of the protocols and identify (and hopefully agree) on the meta data which could be put in clear and those which should be kept encrypted. This work should be made at the technical level and avoid any interference with the business aspects.

[1] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners Lee, "Hypertext Transfert Protocol – HTTP/1.1, RFC 2616, IETF, June 1999.

[2] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, IETF, August 2008.

[3] E. Rescorla, "HTTP Over TLS", RFC 2818, IETF, May 2000.

[4] M. Belshe, R. Peon, M. Thomson (Ed.) and A. Melnikov (Ed.), "Hypertext Transfer Protocol version 2.0", draft-ietf-httpbis-http2, IETF, December 2013.