Source Tagging for Reserve Charging of Encrypted Traffic

Lingli Deng
China Mobile
denglingli@chinamobile.com

Dapeng Liu and Dacheng Zhang
Alibaba
{max.ldp, dacheng.zdc}@alibaba-in.com
Background

The Changing Lifestyle with E-Commerce

• E-commerce has been changing our lifestyle
  • On-line shopping has been replacing on-site shopping
    • Amazon
    • Alibaba
  • On-line promotions becomes national shopping festivals
    • Black Friday in the US
    • 11.11 in China (Alibaba)
    • 6.28 in China (Jingdong)

• E-commerce has been changing operator’s lifestyle
  • Vast volume of highly asynchronous traffic from a handful E-Commerce giants to its subscribers within a short time frame of days/hours duration
Appealing Business Model
Reverse Charging during E-festivals

• Idea: Have the ICP pay for the data traffic to its websites for the mobile subscribers to further promote customer participation.

• Implications
  • The charging GW sitting in the edge of operator’s core network needs to identify the traffic flows and do reverse charging for these traffic volume between its mobile subscribers to the intended ICP websites during a given period of time.

• Potential ways for Web traffic identification
  • Layer7 DPI (URL) based identification
  • Source/Target-IP-based identification
Problem Statement
Life Has been Changed Since Encryption

• There is NO way for the charging GW to differentiate an ICP traffic.

• Layer7 DPI (URL) based identification
  • Not applicable as Web traffic is end2end encrypted with TLS.

• Source/Target-IP-based identification
  • Not performant for the charging GW to be manually configured with the enormous IP address pools for the nation-wide private/rented CDN network of Alibaba.

• Potential Alternatives
  • Out-of-band tagging: TLS handshake piggybacking.
  • In-band tagging: Traffic tagging outside TLS encryption.
Summary

• To enable reverse charging for mobile web traffic to a specific ICP, the charging GW needs to differentiate the relevant traffic accurately even if it is actually encrypted with TLS.

• There may be two types of semantics that such a tag can carry
  • The charging model of the traffic and the entity to be charged

• There may be further security implications to consider in order to prevent malicious endpoints/middle-box from tampering/fraud with the traffic tagging.
Question

• Would ACCORD be interested in solving this use-case?