Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 21, 2016

J. You
C. Xiong
Huawei

October 19, 2015

The Effect of Encrypted Traffic on the QoS Mechanisms in Cellular Networks
draft-you-encrypted-traffic-management-00

Abstract

This document provides a detailed description of the QoS mechanisms of the 3GPP network and why encrypted IP traffic makes current QoS management mechanisms almost useless. Finally, we propose some ideas to solve this conflict to allow QoS mechanisms to be applied to encrypted IP traffic whilst maintaining the confidentiality of the IP traffic.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 21, 2016.

Copyright Notice

Copyright (c) 2015 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Terminology 3
  2.1. Abbreviations and acronyms 3
  2.2. Definitions 4
3. The Influence of Encryption on the QoS Management 4
  3.1. IPsec/VPN Tunnel-based IP Layer Encryption Effect 5
  3.2. IMS/SIP Session Service Encryption Effect 6
  3.3. HTTP Encryption Effect 6
4. Potential Co-operative Information between Application and Network 7
  4.1. Application to Network 7
  4.2. Network to Application 8
5. Potential Bandwidth Optimization Methods 8
  5.1. Intelligent Heuristic Method 8
  5.2. Legacy Protocol Extension 9
  5.3. New Substrate Protocol 9
6. Conclusion 10
7. Acknowledgement 10
8. References 10
  8.1. Normative References 10
  8.2. Informative References 10
Authors' Addresses 11

1. Introduction

Encryption of internet traffic is to prevent pervasive monitoring and protect customer privacy. Historically, Secure Sockets Layer (SSL) / Transport Layer Security (TLS) were earlier used in financial services to encrypt a subset of Internet traffic, especially financial transactions. However, the shift away from unencrypted traffic towards encrypted traffic is accelerating in recent years [I-D.mm-wg-effect-encrypt] due to concerns about privacy. Google offered end-to-end encryption for Gmail since 2010, and switched all searches over to HTTPS in 2013. YouTube traffic is carried via HTTPS (or QUIC) since 2014. Also, the Snowden revelations [RFC7258] [RFC7624] seem to cause an upward surge in encrypted traffic. A

large number of operators began requiring encryption for all XMPP traffic in May 2014 [XMPP].

However, the prevalence of encryption impacts current network services, such as policy control, load balancing, etc. The network services may be less efficient or totally unavailable in the case of fully encrypted traffic. QoS handling is the most important part of the 3GPP radio resource management. 3GPP networks have limited radio and transmission resources and need to strictly schedule the utilization of radio and transmit resources using different granularity of bearers to provide and ensure Quality of Service (QoS) for the IP traffic. Different bearers with different QoS parameters will provide different QoS handling for the IP flows on each bearer. Different IP flows can share the same bearer; IP flows on the same bearer will receive the same QoS handling of the 3GPP network. With this binding mechanism, the 3GPP network can provide any IP flow with its required QoS handling. Therefore, the 3GPP network firstly needs to know the IP flow information and its QoS requirements. If this information is unknown, possibly as a result of encryption applied to the IP flow, the 3GPP network will discard this IP flow or handle the IP flow with default QoS.

2. Terminology

2.1. Abbreviations and acronyms

AF: Application Function

ARP: Allocation and retention priority

EPS: Evolved packet System

IMS: IP Multimedia Subsystem

PCRF: Policy and Charging Rules Function

QCI: QoS Class Identifier

QoS: Quality of Service

SDF: Service Data Flow

SIP: Session Initiation Protocol

SLA: Service-Level Agreement

URL: Uniform/Universal Resource Locator

2.2. Definitions

This section contains definitions for terms used frequently throughout this document. However, many additional definitions can be found in [3GPP 23.203]

ARP: The Allocation and Retention Priority for the service data flow consisting of the priority level, the pre-emption capability and the pre-emption vulnerability.

IP CAN bearer: An IP transmission path of defined capacity, delay and bit error rate, etc.

GBR bearer: An IP CAN bearer with reserved (guaranteed) bitrate resources.

Non-GBR bearer: An IP CAN bearer with no reserved (guaranteed) bitrate resources.

QoS class identifier: A scalar that is used as a reference to a specific packet forwarding behavior (e.g. packet loss rate, packet delay budget) to be provided to a SDF.

QoS: It contains the QoS class identifier and the data rate for a service data flow.

Service data flow: An aggregate set of packet flows that matches a service data flow template.

Service data flow template: The set of service data flow filters that contains a set of packet flow header parameter values/ranges used to identify one or more of the packet flows.

3. The Influence of Encryption on the QoS Management

EPS provides different levels of QoS guarantee for IP services. Any IP service can be identified by one or more Service Data Flows (SDFs) of the transfer data. A SDF can be identified by one or more IP Flow Filters, and a SDF is transferred through an EPS bearer. By implementing the QoS of EPS bearer, it can realize the QoS of SDF, and realize the QoS of IP services. The EPS bearer is one type of logical transport channel between the UE to Packet Gateway (PGW).

In general, if the cellular network cannot know the SDF of one IP service in advance or the content type of the transmission data and its QoS requirements, the SDF of the IP service is usually mapped to the Default Bearer with the Default QoS or is mapped to a poor ARP (Allocation and retention priority) dedicated EPS (Evolved packet

System) Bearer with default QCI or is discarded because of the unknown service information of the SDF based on the predefined operators rules.

Through our analysis of impacted services in the case of encrypted traffic, we find that the impacted services can be categorized into three types based on the level of dependence to content visibility:

A: Low-level dependence

A service that is low-level dependent on the content visibility means the service can be effective providing with flow type (e.g. stream ID) rather than parsing the content itself. The typical services of low-level dependence are IPsec/VPN tunnel, load balancing, etc.

B: Middle-level dependence

A service that is middle-level dependent on the content visibility means the service can be effective providing with access metadata (e.g. domain name, URI) besides flow type rather than parsing the content itself entirely. Through the metadata different access features can be distinguished, thus appropriate actions could be enforced based on these features. For example, illegal websites can be filtered. The typical services of middle-level dependence are IMS/SIP service, parental controls, etc.

C: High-level dependence

A service that is high-level dependent on the content visibility means the service can be effective requiring analysis of content itself, even interaction procedure. The typical services of high-level dependence are web acceleration, video caching, which usually requires user access behavior and detailed video content (e.g. encoding format). In the case of encrypted traffic, this kind of service will not be available.

3.1. IPsec/VPN Tunnel-based IP Layer Encryption Effect

In this case, the internal real port number is invisible to cellular network and the tunnel-based IP traffic is usually mapped to the Default Bearer with Default QoS or to a dedicated EPS bearer with poor ARP and the same default QCI. If the VPN is from a big customer, the special tunnel-based IP traffics are mapped to a special dedicated EPS bearer with special QoS according the predefined rules and SLA (Service-Level Agreement). This might result in more dedicated EPS bearers with different QoS used to

transport the different tunneled-IP traffic with different QoS requirements.

3.2. IMS/SIP Session Service Encryption Effect

The cellular network can beforehand obtain the IP 5-tuple information of SDF of the voice, video and data parts and the content type of each SDF during the Offer/Answer signalling interaction if the signalling connection between the IMS/SIP UA (User Agent) and IMS/SIP server is plaintext without encryption. Alternatively, the IMS/SIP Server or the AF (Application Function) in the server can actively tell the cellular network via the Rx interface to the PCRF (Policy and Charging Rule Function) [3GPP 23.203] all the voice, video and data SDF information even when the signalling connection is encrypted. Even if the transmission of voice, video media above the transport layer is encrypted, such as using SRTP (Secure Real-time Transport Protocol), the cellular network can realize SDF detection and further can guarantee the SDF with the correct ARP and QoS control because the IP Flow information is known by the cellular network beforehand.

If the cellular network cannot obtain prior SDF information on the voice, video and data part of the session because the signalling connection is encrypted and the server/AF does not provide the SDF information, if the voice and video use different IP flows, the cellular network still can identify the SDF type through using intelligent heuristic algorithms which can identify the difference content type by the transmission span of two successive packets, packet size and other information. After the cellular network identifies the SDF information of voice, video and other (data) parts, the cellular network can realize the corresponding QoS control and ARP and ensure the whole session's QoS.

3.3. HTTP Encryption Effect

Currently HTTP 1.1 is the most widely used service/application protocol and it is expected to be widely replaced by HTTP 2 in the near future. HTTP supports transport of various types of data in a single TCP connection. Due to a single TCP connection corresponding to a single SDF, and different types of data and services are transmitted on the same TCP connection, the result is traditional SDF-based mapping SDFs transmitting different types of content/data to different EPS Bearers with different QoS and ARP no longer works well or is applicable for the cellular network. Instead, cellular network operators evolve and adopt new types of QoS-related acceleration technologies to realize and improve the user's experience. Therefore, Mobile CDN technology, Mobile Video Optimization technology, Mobile Web Optimization, Anti-Virus, Anti-

Spoofing, Parent Control technology and all kinds of value-added technologies emerge and are widely used. These technologies can reduce the transport cost of cellular network and at the same time can greatly improve mobile user video and web browsing experience.

When HTTP2 and HTTP1.1 use TLS to encrypt the TCP connection, the widely used Web acceleration and value-added technologies no longer work well. The usual result is the HTTPS connection is mapped to the Default Bearer with Default QoS or dedicated EPS bearer with default QCI and poor ARP. Therefore, there is no guarantee for the different services provided by HTTPS websites. One exception is if there is a SLA/cooperation agreement, then the cellular network can map the TCP connection of the HTTPS website to a dedicated EPS bearer with special QoS, then the QoS for the HTTS website may be improve respectively with the special dedicated EPS Bearer and the specific QoS.

4. Potential Co-operative Information between Application and Network

4.1. Application to Network

A SDF is mapped to a specific QoS EPS Bearer, and SDFs associated with different IP services can be mapped to the same EPS Bearer with the same QoS parameters (namely QCI (QoS Class Identifier) and ARP (Allocation and retention priority)) [PCC].

So application could provide the service level (i.e. per SDF) QoS parameters such as QCI and APR to indicate how certain service/ application traffic shall be treated in the operator's network. For example, given that the categories in table 1 map to GBR and non-GBR resources, with a priority level, it seems cleaner to reveal just the resource type and priority. This also seems possible to encode in a space similar to the QCI.

Table 1: Standardized QCI characteristics

QCI	Resource Type	Priority Level
1	GBR	2
2		4
3		3
4		5
65		0.7
66		2
5	Non-GBR	1
6		6
7		7
8		8
9		9
69		0.5
70		5.5

4.2. Network to Application

The network could provide the application with the real time information about the throughput estimated to be available at the radio downlink interface between a UE and the base station the UE connects to, which is discussed in [I-D.flinck-mobile-throughput-guidance].

5. Potential Bandwidth Optimization Methods

5.1. Intelligent Heuristic Method

By collection and convergence of the information of packet interval, packet size, port number, protocol type etc, the intelligent heuristic algorithm can guess correctly some the types of the content of the packet transmission as mentioned in previous chapter of IMS/SIP session type communication.

This method can be implemented in the mostly widely deployed Apache and or nginx HTTP Server package without destroying any current protocols. This method requires the OTT to deploy the modified Apache/nginx HTTP Server and an intelligent heuristic algorithm running in the cellular network to identify the dynamically changed content type of the encrypted HTTPS connection.

5.2. Legacy Protocol Extension

Regarding to the low-level dependence services, existing protocols could be extended in order to carry flow type, for example, enhancing TLS header.

A new TCP option to identify the encrypted content type has certain feasibility, but it may have problems when passing through some existing middleboxes.

For DSCP method, it requires OTTs to set the right DSCP field of outer IP packet corresponding to different content types in the encrypted TLS connection. But the DSCP value may be modified by the routers from the OTT to the cellular network.

5.3. New Substrate Protocol

New substrate protocols over existing transport layers, such as UDP, TCP, are considered to carry flow information in order to make middle-level dependence service effective.

Developing UDP-based substrate protocols to enable transport evolution is a hot topic in IETF recently. The QUIC protocol from Google falls into this space; however, QUIC is not aiming to solve the encrypted traffic management. One major issue with UDP-based substrate is middleboxes may block UDP or limit rate. SPUD-like [I-D.hildebrand-spud-prototype] UDP-based substrate could be a potential method to allow traffic management while using transport protocols. How middleboxes trust the information exposed by the endpoints should be considered.

However today's Internet is full of middleboxes that may interfere with the information sent in IP packets and TCP segments. "Is it still possible to extend TCP?" [ExtendTCP] shows the limitation imposed on TCP extensions by middleboxes behaviors, such as TCP options removed or updated, the source and destination port numbers translated by NATs. Though we can still extend TCP to support middle-level dependence services, extensions are very constrained as it needs to take into account middleboxes behaviors.

6. Conclusion

In this draft the importance of QoS in the cellular network service is discussed and the basic QoS management concept in the EPS system is described. Regarding to the low/middle-level dependence services, the challenges for potential traffic management methods for encrypted traffic are analyzed. Furthermore, possible IETF standardization work (i.e. legacy protocol extensions and new substrates) is explored in order to solve the conflict between user privacy and traffic management.

7. Acknowledgement

The editors would like to thank Ted Hardie and Dan Druta for their useful comments.

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

[RFC7624] Barnes, R., Schneier, B., Jennings, C., Hardie, T., Trammell, B., Huitema, C., and D. Borkmann, "Confidentiality in the Face of Pervasive Surveillance: A Threat Model and Problem Statement", RFC 7624, DOI 10.17487/RFC7624, August 2015, <http://www.rfc-editor.org/info/rfc7624>.

8.2. Informative References

[ExtendTCP] Honda, M., Nishida, Y., Raiciu, C., Greenhalgh, A., Handley, M., and H. Tokuda, "Is it Still Possible to Extend TCP", IMC'11 Page(s): 2-4, November 2011.

[I-D.flinck-mobile-throughput-guidance] Jain, A., Terzis, A., Flinck, H., Sprecher, N., Swaminathan, S., and K. Smith, "Mobile Throughput Guidance Inband Signaling Protocol", draft-flinck-mobile-throughput-guidance-03 (work in progress), September 2015.

[I-D.hildebrand-spud-prototype]
Hildebrand, J. and B. Trammell, "Substrate Protocol for User Datagrams (SPUD) Prototype", draft-hildebrand-spud-prototype-03 (work in progress), March 2015.

[I-D.mm-wg-effect-encrypt]
Moriarty, K. and A. Morton, "Effect of Ubiquitous Encryption", draft-mm-wg-effect-encrypt-02 (work in progress), July 2015.

[PCC] "3GPP TS 23.203, "Policy and charging control architecture"", 2015.

[XMPP] ""XMPP switches on mandatory encryption" (http://lwn.net/Articles/599647/)", May 2014.

Authors' Addresses

Jianjie You
Huawei
101 Software Avenue, Yuhuatai District
Nanjing, 210012
China

Email: youjianjie@huawei.com

Chunshan Xiong
Huawei
No.3, Xin-Xi Rd., Haidian District
Beijing, 100085
China

Email: sam.xiongchunshan@huawei.com