Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 12, 2015

K. Smith
Vodafone Group

June 10, 2015

Network management of encrypted traffic
draft-smith-encrypted-traffic-management-02

Abstract

Encrypted Internet traffic may pose traffic management challenges to network operators. This document recommends approaches to help manage encrypted traffic, without breaching user privacy or security.

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 December 12, 2015.

Table of Contents

1. Introduction

Networks utilise various management techniques to ensure efficient throughput, congestion management, anti-SPAM and security measures. Historically these functions have utilised visibility of the Internet application layer.

This visibility is rapidly diminishing - encrypted Internet traffic is expected to continue its upward trend, driven by increased privacy

awareness, uptake by popular services, and advocacy from the [IAB], [RFC7258] and W3C [TAG] .

[IAB], [RFC7258] and [mm-effect-encrypt] recognise that network management functions are impacted by encryption, and that solutions

are needed to persist them - as long as they do not threaten privacy. These solutions would ensure the benefits of encryption do not degrade network efficiency.

This document lists such solutions, and points to evolving IETF work addressing the problem.

1.1. Document structure

This document describes the network management functions that are likely to be hindered by traffic encryption.

It then describes the technical details of existing options to fully or partially persist these functions under encryption. 'Encryption' in this document typically refers to HTTP over TLS [RFC2818]; other forms of encryption are noted where applicable.

Finally, a summary is provided of ongoing IETF work which is investigating how middleboxes along the network path can improve encrypted traffic delivery - again without breaching user privacy or security.

The legal, political and commercial aspects of network management are recgnised but not covered in this technical document.

1.2. Security protocols

The following IETF protocols are considered in this document: TLS [RFC5246] , IPsec [RFC4301] and the ongoing transport layer security work of [TCPINC].

2. Network management functions

Editor's note: Part or all of this section may be removed where there is duplication with any updated version of [mm-effect-encrypt]

2.1. Queuing

Traffic flowing through a network may be queued for delivery. This is important at an access network where network conditions can change rapidly - such as a cellular radio access network. To account for congestion, the network will categorise content requests according to the latency and bandwidth required to deliver that content type. These combinations run from high-latency, low bandwidth (Email), medium latency, medium bandwidth (Web pages), low latency high bandwidth (video streaming), and many others including voice calls, texts, WebRTC and VoIP. A well-managed network will triage between

these content types and deliver from each queue in bursts, to ensure no user experiences a disrupted service.

2.2. Server load balancing

Where network load balancers have been configured to route according to application-layer semantics, an encrypted payload is effectively invisible.This has resulted in practices of intercepting TLS in front of load balancers to regain that visibility, but at a cost to security and privacy.

2.3. Intrusion detection

Networks will monitor traffic stream behaviours to identify likely Denial of Service attacks. Tools exist at each network layer to detect and mitigate these, including application layer detection.

2.4. Policy enforcement

Approved access to a network is a prerequisite to requests for Internet traffic - hence network access, including any authentication and authorisation, is not impacted by traffic encryption.

Cellular networks often sell tariffs that allow free-data access to certain sites, known as 'zero rating'. A session to visit such a site incurs no additional cost or data usage to the user. Such 'zero rating

Note: this section deliberately does not go into detail on the

ramifications of encryption as regards government regulation. These regulations include 'Lawful Intercept', adherence to Codes of Practice on content filtering, application of court order filters. However it is clear that these functions are impacted by encryption, typically by allowing a less granular means of implementation. The enforcement of any Net Neutrality regulations is unlikely to be affected by content being encrypted.

2.5. SPAM and malware filtering

This has typically required Deep Packet Inspection to filter various keywords, fraudulent headers and virus attachments.

3. Flow information visible to a network

3.1. IP 5-tuple

This indicates source and destination IP addresses/ports and the transport protocol. This information is available during TLS, TCP-layer encryption (except ports), and IP-layer encryption (IPSec); although it may be obscured in Tunnel mode IPSec.

This allows network management at a coarse IP-source level, which makes it of limited value where the origin server supports a blend of service types.

Obscured from network by: IPSec Tunnel Mode

3.2. TLS Server Name Indication

When initiating the TLS handshake, the Client may provide an extension field (server_name) which indicates the server to which it is attempting a secure connection. TLS SNI was standardized in 2003 to enable servers to present the "correct TLS certificate" to clients in a deployment of multiple virtual servers hosted by the same server infrastructure and IP-address. Although this is an optional extension, it is today supported by all modern browsers, web servers

and developer libraries. Notable exceptions are Android 2.2 and Internet Explorer 6 on Windows XP. It should be noted that HTTP/2 introduces the Alt-SVC method for upgrading the connection from HTTP/1 to either unencrypted or encrypted HTTP/2. If the initial HTTP/1 request is unencrypted, the destination alternate service name can be identified before the communication is potentially upgraded to encrypted HTTP/2 transport. HTTP/2 implementations MUST support the Server Name Indication (SNI) extension.

Limitation: This information is only visible if the client is populating the Server Name Indication extension. This need not be done, but may be done as per TLS standard. Therefore, even if existing network filters look out for seeing a Server Name Indication extension, they may not find one. The per-domain nature of SNI may not reveal the specific service or media type being accessed, especially where the domain is of a provider offering a range of email, video, Web pages etc. For example, certain blog or social network feeds may be deemed 'adult content', but the Server Name Indication will only indicate the server domain rather than a URL path to be blocked.

Obscured from network by: not providing the SNI, IPSec

3.3. Application Layer Protocol Negotiation (ALPN)

ALPN is a TLS extension which may be used to indicate the application protocol within the TLS session. This is likely to be of more value to the network where it indicates a protocol dedicated to a particular traffic type (such as video streaming) rather than a multi-use protocol. ALPN is used as part of HTTP/2 'h2', but will not indicate the traffic types which may make up streams within an HTTP/2 multiplex.

4. Inferred flow information

4.1. Heuristics

Heuristics can be used to map given input data to particular

conclusions via some heuristic reasoning. Examples of input data to this reasoning include IP destination address, TCP destination port, server name from SNI, typical traffic pattern (e.g. occurrence of IP packets and TCP segments over time). The accuracy of heuristics depends on whether the observed traffic originates from a source delivering a single service, or a blend of services. In many scenarios, this makes it possible to directly classify the traffic related to a specific server/service even when the traffic is fully encrypted.

If the server/service is co-located on an infrastructure with other services that shares the same IP-address, the encrypted traffic cannot be directly classified. However, commercial traffic classifiers today typically apply heuristic methods, using traffic pattern matching algorithms to be able to identify the traffic. As an example, classifier products are able to identify popular VoIP services using heuristic methods although the traffic is encrypted and mostly peer-to-peer.

5. Providing hints to and from the network

The following protocols aim to support a secure and privacy-aware dialogue between client, server and a network middlebox. These hints can allow information item exchange between the endpoints and the network, to assist queuing mechanisms and traffic pacing that accounts for network congestion and variable connection strength. These relate to the cooperative path to endpoint signalling as discussed at the IAB SEMI workshop [SEMI], with the network following a more clearly-defined role in encrypted traffic delivery.

5.1. DiffServ Code Points (DSCP)

Data packets are flagged with a traffic class (class of service). Network operators may honour a DiffServ classification entering their network, or may choose to override it (since it is potentially open to abuse by a service provider that classifies all its content as high priority). The purpose is to help manage traffic and congestion in the network.

Limitations: This requires the content provider to flag data packets. This is extra work for the provider, and it has potential for abuse if a content provider simply flags all packets with high priorities. The network would need to know which flags to trust and which to override. The use of DiffServ within the operator network is beneficial where the operator determines the class of service itself; but where content is encrypted then heuristics would be needed to predict the traffic type entering the network. HTTP/2 allows several streams to be multiplexed over a single TCP connection. This means that if a provider decides to send Web pages, videos, chat etc. as individual streams over the same connection, then DiffServ would be useless as it would apply to the TCP/IP connection as a whole. However it may be more efficient for such Web providers to serve each content type from separate, dedicated servers - this will become clearer as HTTP/2 deployments are tuned for optimal delivery.

5.2. Explicit Congestion Notification

Explicit Congestion Notification (ECN) routers can exchange congestion notification headers to ECN compliant endpoints. This is in preference to inferring congestion from dropped packets (e.g. in TCP). The purpose is to help manage traffic and congestion in the network.

This solution is required to be implemented at network and service provider. The service provider will utilise the ECN to reduce throughput until it is notified that congestion has eased.

Limitation: As with DiffServ, operators may not trust an external entity to mark packets in a fair/consistent manner.

5.3. Multi Protocol Label Switching

Description: on entering an MPLS-compliant network, IP packets are flagged with a 'Forward Equivalence Class' (FEC). This allows the network to make packet-forwarding decisions according to their latency requirements. MPLS routers within the network parse and act upon the FEC value. The FEC is set according to the source IP address and port. The purpose is to help managing traffic and

congestion in the network. This requires deployment of an MPLS

'backbone' with label-aware switches/ routers.

Limitations: an up-to-date correspondence table between Websites and server IP address must be created. Then, the category(s) of traffic have to be consistently mapped to a set of MPLS labels ,which entails a significant effort to setup and maintain.

Note: MPLS can specify how OSI Layer 3 (IP layer) traffic can be routed over Layer 2 (Data Link); DiffServ only operates over Layer 3. DiffServ is potentially a less complex integration as it is applied at the network edge servers only.

5.4. Substrate Protocol for User Datagrams (SPUD)

SPUD [SPUD] allows network devices on the path between endpoints to participate explicitly in a 'tube' of grouped UDP packets. The network involvement is outside of the end-to-end context, to minimise any privacy or security breach. The initial prototype is based on UDP packets but will investigate the support of additional transport layers (such as TCP).

5.5. Mobile throughput Guidance

Mobile Throughput Guidance In-band Signalling [MTG] allows the network to inform the server endpoint as to what bandwidth the TCP connection can reasonably expect. This allows the server to adapt their throughput pacing based on dynamic network conditions, which can assist mechanisms such as Adaptive Bitrate Streaming and TCP congestion control.

5.6. Port Control Protocol Flowdata options

PCP Flowdata options [PCPFD] defines a mechanism for a host to signal flow characteristics to the network, and the network to signal its ability to accommodate that flow back to the host. This allows certain network flows can to receive service that is differentiated from other network flows, and may be used to establish flow priority before connection establishment. PCP Flowdata operates at IPv4 /IPv6 level.

5.7. IPv6 Flow label

IPv6 includes a flow label header field. [RFC6438] details how this may be used to identify flows for load balancing and multipath routing, which may be of particular use for application-layer encrypted traffic. The flow label field is part of the main header, which means it is not subject to the disadvantages of extension

headers (namely their risk of being dropped by intermediary routers). The flow label may also be exposed as part of the outer IP packet in an IP tunnel, thus providing network flow information without compromising the payload.

5.8. DISCUSS

Differentiated prIorities and Status Code-points Using Stun Signalling [DISCUSS] describes a mechanism for information exchange between an application and the network, viable only for UDP. As such it can be considered in the same bracket as SPUD

6. Acknowledgements

The editor would like to thank the GSMA Web Working Group for their contributions, in particular to the technical solutions and network management functions, as well as contributions via the SAAG mailing list (Panos Kampanakis, Brian Carpenter)

7. IANA Considerations

There are no IANA consideraions.

8. Security Considerations

The intention of this document is to consider how to persist network management of encrypted traffic, without breaching user privacy or end-to-end security. In particular this document does not recommend any approach that intercepts or modifies client-server Transport Layer Security.

9. References

9.1. Normative References

[RFC2818] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC6438] Carpenter, B. and S. Amante, "Using the IPv6 Flow Label for Equal Cost Multipath Routing and Link Aggregation in Tunnels", RFC 6438, 2011.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, May 2014.

9.2. Informative References

[DISCUSS] Cisco, "Differentiated prIorities and Status Code-points Using Stun Signalling", 2015, <https://tools.ietf.org/html/draft-martinsen-tram-discuss-02>.

[IAB] IAB, "IAB statement on Internet confidentiality", n.d., <https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/>.

[MTG] IETF, "Mobile Throughput Guidance Inband Signaling Protocol", n.d., <https://tools.ietf.org/html/draft-flinck-mobile-throughput-guidance-02>.

[PCPFD] Cisco, "PCP Flowdata option", 2013, <https://tools.ietf.org/html/draft-wing-pcp-flowdata-00>.

[SEMI] IAB, "IAB workshop, 'Stack Evolution in a Middlebox Internet'", n.d., <https://www.iab.org/activities/workshops/semi/>.

[SPUD] IETF, "Substrate Protocol for User Datagrams", n.d., <https://tools.ietf.org/html/draft-hildebrand-spud-prototype-03>.

[TAG] W3C, "Securing the Web", n.d., <https://w3ctag.github.io/web-https/>.

[TCPINC] IETF, "TCP Increased Security", n.d., <https://datatracker.ietf.org/wg/tcpinc/charter/>.

[mm-effect-encrypt] IETF, "Effect of Ubiquitous Encryption", n.d., <https://datatracker.ietf.org/doc/draft-mm-wg-effect-encrypt/>.

Author's Address

Kevin Smith
Vodafone Group

Email: kevin.smith@vodafone.com