SCONE
Internet-Draft
Intended status: Informational
Expires: 8 November 2025

A. Tomar
W. Eddy
A. Tiwari
M. Joras
Meta

7 May 2025

SCONE Privacy Properties and Incentives for Abuse
draft-tomar-scone-privacy-01

Abstract

This document discusses privacy properties of the SCONE metadata or network-to-host signals. This covers questions that were raised during the IETF 119 BoF and subsequent discussions. It is not intended to be published as a separate RFC but might be incorporated as a part of the security considerations or other content within eventual SCONE RFCs together with other documents covering security considerations. Other documents will address additional aspects of the security considerations for SCONE metadata.

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 https://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 8 November 2025.

Copyright Notice

Table of Contents

1. Introduction

The general problem statement for Standard Communication with Network Elements (SCONE) is described in the video optimization requirements document [I-D.joras-scone-video-optimization-requirements], including the shaping or throttling that Communication Service Providers (CSPs) perform [ABR-Video-Shaping].

There were questions rasied at the IETF 119 BoF on SCONEPRO (that led to SCONE) regarding privacy considerations, include:

1. What are the privacy properties of the SCONE signal? If making the signal available to applications is the goal, does that have unwanted properties?

2. Can the signal be designed so that there is no incentive to fake it, similar to ECN?

This document provides additional context necessary, and then directly addresses these questions.

2. Conventions and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

3. SCONE Context

SCONE is focusing on streaming video optimization use-cases through network-assisted application-level self-adaptation of media/video bit rate. SCONE addresses the following high-level problem statement:

1. Currently Communication Service Provider (CSP) networks (mainly cellular and satellite networks) perform bit-rate throttling (either shaping or policing) of streaming video flows. The motivation behind throttling may vary across CSPs. For example, the motivation can be:

   * To support different data rates based on the subscribers' data plans;

   * To reduce egress towards radio base-stations in downlink direction;

   * To limit the overall capacity/bandwidth required and to manage capex requirements (e.g. need for more RF spectrum and deployment of more radio base-stations), etc.

2. To perform throttling, CSP networks need to detect streaming video flows, which uses deep packet inspection and trial decryption of QUIC initial packets in order to decode and read the Server Name Indication (SNI) field present in initial ClientHello messages. This requires significant compute resources. Throttling (shaping or policing) also requires nontrivial compute and memory resources. For details refer to [ABR-Video-Shaping].

3. Throttling in the CSP network has a significant negative impact on streaming video application quality of experience (QoE), and it also degrades mobile User Equipment (UE) battery performance.

4. An equivalent reduction in network traffic can be achieved more intelligently via self-adaptation by Content Application Providers (CAPs), because CAPs can actually measure QoE parameters and can tune their self adaptation strategy much more effectively than the QoE-blind approach taken by CSP's network

throttlers. Hence, this approach of self-adaptation by CAPs is much superior in terms of end user QoE compared to CSP-led network throttling.

5. CSPs currently use intentional (artificial) network throttling as a way to create service differentiation between users on different payment plans and to enforce fair usage plans.

6. CAPs do not and should not have access to subscriber payment plan information.

7. There is a need for a solution to the above multi-objective optimization problem which achieves both: (a) superior user QoE, and (b) differentiated data limitation consistent with subscriber plans.

8. One potential solution to this problem is self-adaptation of video sessions by CAPs. Since the subscriber plan information must live within the CSP network domain, the CSP network can abstract out the different traffic profiles suited to different subscriber plans and provide the abstracted information to application-clients running on the UEs for CAP self-adaptation implementations.

For details, refer to the proof of concept trial [I-D.ihlar-scone-masque-mediabitrate] and YouTube plan aware streaming [YouTube].

The SCONE network rate-limiting information (metadata) and the means of conveying the information is to be defined by the IETF.

4. Privacy Properties

This document section describes the privacy properties of the SCONE signal and considerations with regard to making the signal available to applications.

It is required that the SCONE signal shall not carry information that includes either:

* Any Personal Identifiable Information (PII) that can be used to identify the subscriber such as International Mobile Subscriber Identity (IMSI). IMSI is a unique 15-digit number that identifies every user uniquely within a mobile network.

* Network' s policy associated with a subscriber - the CSP Network stores subscriber policies in network elements such as HSS (Home Subscriber Server)/UDM(Unified Data Management)/PCRF(Policy and Charging Rules function) to support various subscriber specific features in the network.

To help describe the SCONE approach to meet these privacy requirements, as well as to ensure the signal does not have unwanted properties, the next subsections provide an example and then general approach.

4.1. Mobile Network Example

Using a mobile network as a reference, the diagram in Figure 1 explains how CSP networks implement throttling to support different data rates based on the subscribers' data plans.

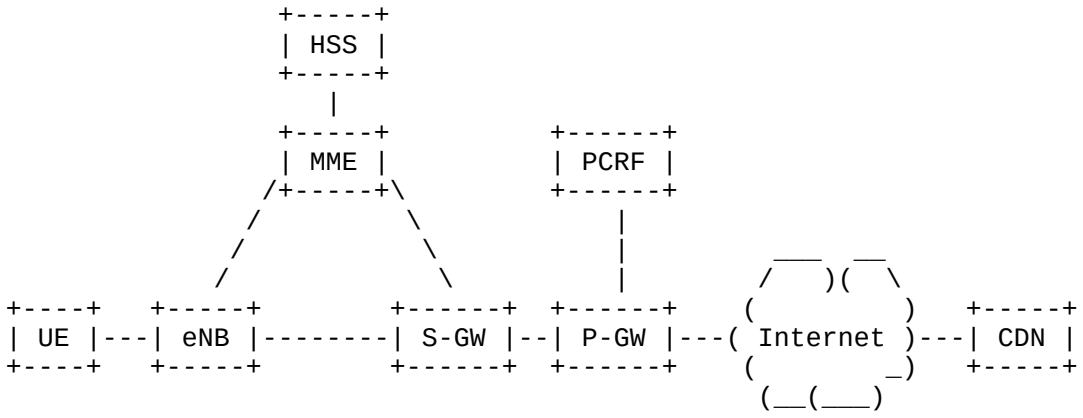

Figure 1: Mobile Network Data Flow

In order to perform throttling to enable different data-rates based on the subscribers' data plans, the CSP network need to support following high-level functionalities:

1. Detect the streaming video flows.

2. Identify the bearer associated with the flow.

    * Bearer is a logical pipe between UE (Mobile phone) and P-GW (PDN Gateway) to carry packets belonging to one or more IP flows. IP flows (aka service data flows -SDFs) may belong to one or more services. All the service data flows within a bearer gets the same level of QoS.

3. Identify the subscriber who is using this service/flow by using mapping between bearer and subscriber ID (IMSI).

4. Extract the network's policy associated with a subscriber.

5. Activate throttling to limit the flow's bit-rate according to subscribers' data plans.

This is performed in the network element which is on the data path and has access to the subscriber policies through standard interface with PCRF (Policy Charging and Rule function). In a 4G network this network-element is P-GW (PDN Gateway) and in a 5G network this network-element is UPF (User Plane Function). Note - UPF is not shown in above diagram as above diagram is for 4G mobile network. UPF is equivalent to P-GW in the 5G mobile network.

4.2. SCONE's Approach

To meet the privacy requirements as well as to ensure that signal does not have unwanted properties, SCONE proposes following approach:

1. Use an on-path interface between the user's application end-point and network element to exchange the SCONE signal. This should be the same on-path interface that has already been established between application end-point and network element to carry the video flow whose bit-rate needs to be regulated. Due to the usage of an on-path interface there is no need to exchange additional subscriber specific information (that could have been otherwise used to identify the subscriber) between CSP network and application end-point to establish association between the flow and scone signaling.

2. Network elements to be involved in SCONE signaling should be on data-path and should have access to the subscriber policies. This network element should calculate the target bit-rate for the specific flow based on subscribers' data plan, network configuration & capacity and CSP network policy and share only the just enough information (for e.g. video/media bit-rate etc. Exact metadata and data-types to be defined during the solution definition phase of SCONE) with application end-point via SCONE signaling. This would ensure that SCONE signal does not carry the network's policy associated with a subscriber and it does not carry unwanted network information/properties.

Note - Information such as video/media bit-rate, that is required to be shared by a network device with client application end-point using SCONE signal can already be learnt by application end-point currently, through various mechanisms (the effect of on-path

throttlers is clearly visible by observing application traffic by third party tools like PCAP). So as part of SCONE scope we are not proposing, network to share any information with application endpoints which can not be known without SCONE, rather objective is that such information be made explicit.

5. Incentives for Abuse

In early discussion, at the IETF 119 BoF session, it was pointed out that possible incentives for abuse need to be considered, and that a good example existing network-to-host signalling case is Explicit Congestion Notification (ECN), for which the impact of both lying/ cheating hosts and network devices has been analyzed, and for which there are no strong incentives for either hosts or network devices to unnecessarily forge or tamper with ECN codepoints.

Note, why ECN is not suitable as a method to meet SCONE requirements is a separate topic, discussed in another document [I-D.tomar-sconepro-ecn], while the discussion below is focused on considering ECN operation only as an inspiration for properties SCONE signaling should have.

ECN is an extension to the Internet Protocol. ECN allows end-to-end notification of network congestion without dropping packets. ECN is an optional feature that may be used between two ECN-enabled endpoints when the underlying network infrastructure also supports it. In general both classic ECN [RFC3168] and L4S ECN [RFC9330] [RFC9331] [RFC9332] are mechanisms to send end-to-end notification of network congestion. And it relies on following principles:

1. Sender to set the ECT code-points correctly for a particular flow.

2. Receiver to send the feedback back to the sender correctly based on CE value.

3. Network elements to set the CE bit correctly based on actual congestion conditions in the network.

4. ECN codepoints are not bleached or remarked within the network, other than to set the CE bit when appropriate.

The case of SCONE is similar in many ways to ECN:

* Any network device which can alter ECN bits can simply drop the packets. And packet drop may have more negative impact on application’ s performance compared to using ECN bits to indicate congestion in the network.

* Similarly any network device which can send SCONE signaling can throttle the application flow. Throttling may have a more negative impact on application's performance compared to using SCONE signaling to influence the incoming flow bit-rate from the sender. So like ECN, there should not be any incentive for the network device to fake the SCONE signal.

* Regarding faking CE bit (either setting or clearing it), there is no incentive either way, because both cases may have more negative impact on application's performance within the network faking the ECN signals

* Similarly, faking SCONE signaling (sending incorrect meta-data) there is no incentive because sending incorrect meta-data may have more negative impact on application's performance within the network faking the SCONE signals

6. Security Considerations

SCONE security considerations are discussed in the other documents covering specific network-to-host signaling methods and their implications. This document provides answers to questions regarding privacy of the SCONE signaling and metadata. There are no additional security considerations raised by this.

Other security considerations for SCONE signalling will be covered in separate Internet-Drafts (such as [I-D.thoji-scone-protocol]).

7. IANA Considerations

This document has no IANA actions.

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, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

8.2. Informative References

[ABR-Video-Shaping]
Ihlar, M., "ABR Video Shaping", 21 March 2024, <https://datatracker.ietf.org/meeting/119/materials/slides-119-sconepro-how-networks-shape-traffic-02>.

[I-D.ihlar-scone-masque-mediabitrate]
Ihlar, L. M. and M. Khlewind, "MASQUE extension for signaling throughput advice", Work in Progress, Internet-Draft, draft-ihlar-scone-masque-mediabitrate-02, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ihlar-scone-masque-mediabitrate-02>.

[I-D.joras-scone-video-optimization-requirements]
Joras, M., Tomar, A., Tiwari, A., and A. Frindell, "SCONE Video Optimization Requirements", Work in Progress, Internet-Draft, draft-joras-scone-video-optimization-requirements-00, 4 November 2024, <https://datatracker.ietf.org/doc/html/draft-joras-scone-video-optimization-requirements-00>.

[I-D.thoji-scone-protocol]
Thomson, M., Huitema, C., Oku, K., Joras, M., and L. M. Ihlar, "Standard Communication with Network Elements (SCONE) Protocol", Work in Progress, Internet-Draft, draft-thoji-scone-protocol-00, 6 May 2025, <https://datatracker.ietf.org/doc/html/draft-thoji-scone-protocol-00>.

[I-D.tomar-sconepro-ecn]
Tomar, A., Ihlar, L. M., Eddy, W., Swett, I., Tiwari, A., and M. Joras, "SCONEPRO Need for Defining A New On-Path Signaling Mechanism", Work in Progress, Internet-Draft, draft-tomar-sconepro-ecn-01, 23 May 2024, <https://datatracker.ietf.org/doc/html/draft-tomar-sconepro-ecn-01>.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, DOI 10.17487/RFC3168, September 2001, <https://www.rfc-editor.org/rfc/rfc3168>.

[RFC9330] Briscoe, B., Ed., De Schepper, K., Bagnulo, M., and G. White, "Low Latency, Low Loss, and Scalable Throughput (L4S) Internet Service: Architecture", RFC 9330, DOI 10.17487/RFC9330, January 2023, <https://www.rfc-editor.org/rfc/rfc9330>.

[RFC9331] De Schepper, K. and B. Briscoe, Ed., "The Explicit Congestion Notification (ECN) Protocol for Low Latency, Low Loss, and Scalable Throughput (L4S)", RFC 9331, DOI 10.17487/RFC9331, January 2023, <https://www.rfc-editor.org/rfc/rfc9331>.

[RFC9332] De Schepper, K., Briscoe, B., Ed., and G. White, "Dual-Queue Coupled Active Queue Management (AQM) for Low Latency, Low Loss, and Scalable Throughput (L4S)", RFC 9332, DOI 10.17487/RFC9332, January 2023, <https://www.rfc-editor.org/rfc/rfc9332>.

[YouTube] YouTube, "YouTube Plan Aware Streaming", 21 March 2024, <https://datatracker.ietf.org/meeting/119/materials/slides-119-sconepro-youtube-plan-aware-streaming-01>.

Acknowledgments

This document represents collaboration and inputs from others, including:

* Spencer Dawkins

* Alan Frindell

* Bryan Tan

Authors' Addresses

Anoop Tomar
Meta
Email: anooptomar@meta.com

Wesley Eddy
Meta
Email: wesleyeddy@meta.com

Abhishek Tiwari
Meta
Email: atiwari@meta.com

Matt Joras
Meta
Email: mjoras@meta.com