Secure Communication Of NEtwork PROperties

IETF 120, Vancouver, July 2024

NOTE WELL

This is a reminder of IETF policies.

- By participating in the IETF, you agree to follow IETF processes and policies.
- If you are aware that any IETF contribution is covered by patents or patent applications that are owned or controlled by you or your sponsor, you must disclose that fact, or not participate in the discussion.
- As a participant in or attendee to any IETF activity you acknowledge that written, audio, video, and photographic records of meetings may be made public.
- Personal information that you provide to IETF will be handled in accordance with the IETF Privacy Statement.
- As a participant or attendee, you agree to work respectfully with other participants; please contact the ombudsteam if you have questions or concerns about this.

Definitive information on these policies:

- Internet Standards Process
- Working Group processes
- Anti-Harassment Procedures
- Code of Conduct
- Copyright
- Patents, Participation
- Privacy Policy

For advice, please talk to WG chairs or ADs.

Agenda

Introduction	Chairs	10m
Status at IETF 119 and since	Chairs	5m
Recap of Problem Statement	Marcus Ihlar	10m
Review of Open Issues	Matt Joras	20m
Proposed Charter	Chairs	15m
Charter discussion	Everyone	45m
BoF Questions	Chairs	15m

Status

First BoF at IETF 119

Discussion on the list on key points

- Several open questions have entire drafts answering them
- Refreshed charter

Drafts

draft-joras-sconepro-video-opt-requirements-00

draft-joras-sconepro-quic-protocol-00

draft-eddy-sconepro-api-03

draft-tan-sconepro-netneutrality-00

draft-tomar-sconepro-ecn-01

draft-tomar-sconepro-privacy-02

draft-brw-sconepro-rate-policy-discovery-02

draft-rwbr-sconepro-flow-metadata-02

Open Questions From IETF 119

+ How would the network element be discovered and authenticated?
+ How would the signal be propagated? How would it be protected?
+ What are the privacy properties of the signal? If making the signal available to applications is the goal, does that have unwanted properties?
+ Could this be used to violate or undermine things like network neutrality protections for network users?
+ How does this work in multipath contexts?
+ Can the signal be designed so that there is no incentive to fake it, like with ECN?

– https://mailarchive.ietf.org/arch/msg/sadcdn/tssCglEiQ3_307J88QZ3iq31A5k/

Goal For This Session

1. Is there a problem to be solved?
2. Do we understand that problem enough to engineer a solution?
3. Are enough people interested enough to do the work?

Charter

Charter: The Wordy Bit (1/3)

Video traffic is 70% of the overall traffic volume on the Internet and is expected to grow to 80% by 2028. Across developed and emerging markets video traffic forms 50-80% of traffic volume on mobile networks. New formats like short form videos have seen tremendous growth in recent years. These growth trends are likely to increase with new populations coming online on mobile-first markets.

Charter: The Wordy Bit (2/3)

Local access network conditions may constrain the maximum throughput for a given client, or be so volatile as to rapidly change the maximum throughput throughout the course of a session. In addition, despite capacity augmentation work such as deployment of new generations or new bands of spectrum, capacity augmentation efforts are not keeping pace with growth in demand. These network operators have found it faster and less expensive to invest in shaping (also called throttling) of video traffic on a per-flow basis, which negatively affects video stream quality. This is done for both network management and business motivations. Network operators cannot explicitly measure the degradation to end user quality of experience (QoE) caused by traffic shaping, making this approach open loop.

Charter: The Wordy Bit (3/3)

Video traffic usually employs adaptive bitrate (ABR) schemes to dynamically adjust the video quality (and thus the data rate) in response to changing network conditions. Ideally, when a network operator performs traffic shaping, the ABR scheme should adapt the video quality in use to reflect the data rate allowed by shaping, and converge on a bitrate allowed by the shaper. In practice this convergence is extremely difficult to achieve while maintaining a good user experience. Application providers are even designing algorithms to detect the presence of such traffic shapers and estimate the targeted shaping rate, however, these algorithms are likely to be both inaccurate and complex. Instead, it would be beneficial, for both the application provider and network operator, to signal network attributes to the application to self-adapt its video traffic to conform to the specified characteristics. The application provider has the ability to measure end user QoE and therefore can self-adapt with QoE feedback.

Charter: Goal

The Secure Communication of Network Properties (SCONEPRO) Working Group's primary objective is to specify a 'maximum achievable throughput' property for QUIC-based streaming video and an on-path protocol for securely communicating this property from a network device to a client endpoint.

Charter: Solution Characteristics (1/3)

The properties of this mechanism are as follows:

1. Flow associativity. The network communicates applicable properties as they relate to specific QUIC connections. This ensures that applications can authorize and apply actions on a per-QUIC connection basis.
2. Single communication channel for both client initiation and network properties. The communication channel is initiated by a client device, just as the end to end application flows are also typically initiated by a client. The same communication channel is used to provide network properties to the client.
3. Network properties sent from the network. The network provides the properties to the client. The client might communicate with the network, but won't be providing network properties.

Charter: Solution Characteristics (2/3)

4. On-path establishment. That is, no off-path element is needed to establish the communication channel between the entity communicating the properties and the client.
5. Optionality. The communication channel is strictly optional for the functioning of application flows. A client's application flow must function even if the client does not establish the channel.
6. Properties are not directives. A client is not mandated to act on properties received from the network, and the network is not mandated to act in conformance with the properties.

Charter: Solution Characteristics (3/3)

7. Resilient to NAT rebinding, QUIC connection migration, and Multipath QUIC operation. The mechanism will allow the communication channel to be resilient to NAT rebinding, as long as the client is still served by the same logical Communication Service Provider (CSP). Additionally, the mechanism must work with flows that utilize QUIC connection migration or Multipath QUIC, and be able to distinguish network properties from two or more paths.
8. Scalability. The mechanism must be scalable and implementable by Internet infrastructure as it exists today~~, for example mobile network packet cores~~.
9. Security. The mechanism will have the ability to invoke security mechanisms that provide confidentiality, integrity, and authenticity of the communication. The working group will consider the value and implications of different confidentiality modes of the communication.

Charter: Out of Scope

The following topics are out of scope for SCONEPRO:

1. Support for streaming video flows carried in other transports and substrates than QUIC.
2. Support for other media types that would require awareness of additional network attributes beyond the attributes applicable to ABR video.
3. Support for general purpose network attributes. If additional network attributes are identified, the working group will request recharter to add them to SCONEPRO.
4. Support for congestion signaling from the network. SCONEPRO should not be treated as mechanism to replace congestion control or rate adaptation.

Charter: Principles

The working group will consider RFC 9419 as a source of principles in the development of this mechanism, and will consider relevant lessons from past IETF work in Path Aware Networking from RFC 9049.

Charter: Coordination

The working group will coordinate with other groups, both inside and outside the IETF, as work progresses. Some of these groups might be

- WEBTRANS (in the IETF, which coordinates with W3C, responsible for browser specifications and APIs)
- MOQ (producing a specification for streaming media over QUIC)
- AVTCORE (producing an RTP-over-QUIC specification for real-time media)
- MOPS (responsible for discussion of video technology's requirements of networking standards, as well as proposals for new uses of IP technology in video)
- QUIC or HTTPbis, (if the working group identifies requirements for protocols used by SCONEPRO)
- TSVWG and CCWG (if these working groups work on mechanisms that could be used in response to changes in SCONEPRO path properties)

Charter: Deliverables

The proposed deliverables for SCONEPRO are as follows:

- Develop a standard track "SCONEPRO protocol" to securely communicate network information to clients.
- Develop an Informational SCONEPRO Protocol Applicability and Manageability specification.

Goal For This Session

1. Is there a problem to be solved?
2. Do we understand that problem enough to engineer a solution?
3. Are enough people interested enough to do the work?