**SA WG2 Meeting #S2-162 S2-240xxxx**

**15 – 19 April, 2024, Changsha, China (revision of S2-240xxxx)**

**Source: Futurewei**

**Title: KI#2: Principles for Evaluation**

**Document for: Approval**

**Agenda Item: 19.3**

**Work Item / Release: FS\_XRM\_Ph2 /Rel-19**

***Abstract of the contribution:****This contribution proposes considerations for evaluating KI#2.*

# 1 Discussion

E2E encrypted packets have resulted in the need for different approaches to network collaboration using path signals (as well as for network monitoring). With unencrypted packets, networks used Deep Packet Inspection (DPI) to identify an “implicit signal” derived from the contents of a packet. When packet contents are encrypted, this method is no longer viable and one of many approaches with encrypted packets is to use side channels that carry an “explicit signal” (this approach is common to all KI#2 solutions considered).

However, the use of side channels to address the needs for cooperative exchange (and network monitoring) is still being researched and few underlying standards exist. Many aspects need more investigation, and they include the scalability of solutions, collaboration between multiple parties on-path, and the amount/nature (technical, legal, regulatory and ownership) of data shared. IETF (responsible for N6 protocols) is in the process of working out the underlying protocols that different stakeholders (operators, application providers and end-users) are willing to accept for metadata between parties.

Some principles:

Discussion: Unencrypted communications used “implicit signals” to handle QoS and network monitoring. However, with encrypted communications, there are recommendations to use “explicit signals” in RFC 8558 and RFC 9419. They apply to metadata signalling and to allow a user to opt-in (and UE feedback for server pacing). KI#2 was designed to address the metadata aspects, but these gaps remain open.

1. **For encrypted communications and metadata, protocols, and mechanisms that different stakeholders (user, network operator, application provider) can accept explicitly should be considered.**

Discussion: Applications from a provider are used across mobile networks, Wi-Fi, or fixed networks and all these networks use QoS and traffic shaping to manage network performance. It would be beneficial to have one set of metadata that applications send to different networks to shape traffic. Each network may adapt it to its own needs (e.g., classification by UPF in 3GPP networks ). However, KI#2 has considered metadata applicable to 3GPP networks only.

1. **Applications may serve different networks including mobile, Wi-Fi or fixed networks. Metadata to assist with QoS (in N6/IP network) should be possible to use across different access networks.**

Discussion: Some signals like timestamp, sequence numbers are sent in with only integrity protection in various media protocols as they do not reveal additional information about the user or content, and other fields that are sensitive are encrypted (e.g., SRTP, RTP cryptex). QUIC however encrypts all headers except the connection identifier and a few flags. However, encryption does not prevent traffic analysis. Metadata should not allow additional information leakage through traffic analysis.

1. **Protection of sensitive information and detection of modification (integrity protection) of any information on path is necessary. Traffic analysis of the metadata should reveal no additional information.**

Discussion: Levels of trust, agreements and regulatory aspects differ between various network and application providers. The N6 side channel for metadata should provide commonly usable information. Rich information can be provided via AF – NEF/PCF between application provider/network based on trust and agreements.

RFC 6973 (7.1) outlines various aspects to consider including identifiers, information on users/devices, observation, fingerprinting, correlation with information obtained outside of protocol. This also relates to point (1) where it is not clear what information stakeholders like the application providers are willing to expose to trusted entities on path.

1. **Metadata should be minimized to avoid leakage on path and reduce the amount of information revealed to trusted parties on path.**

Discussion: Application layer devices incur relatively high costs in processing application logic and caching compared to the cost of proxying/encryption. However, for network devices (even complex ones like UPF) minimizing processing latency is essential. In fact, the aim of the side channel metadata is to assist and improve QoS handling. Current encryption methods impose acceptable costs for link encryption (NR, MACsec) and application transport but it is neither lightweight nor designed for small packets[[1]](#footnote-2).

1. **Encrypted side channel with metadata in a small packet can introduce significant overhead and delays. Mitigation of these costs should be considered.**

Discussion: Getting agreement with multiple parties and interests will be time consuming. There are at least three metadata side channel directions already proposed with drafts for server – network metadata, network – user, and user – network. In each case, there is a desire to have limited and common mechanisms for both metadata and the side channel (transport of metadata).

1. **Related to several points above, the process to standardize the metadata in the IETF (which is responsible for N6 protocols) and challenges related to the limited time to standardize for Release 19 should be considered a key factor.**

 A preliminary analysis indicates that solutions in KI#2 are not general and have several gaps :

* MoQ (sol 9, 10) protocols apply only in scenarios where the application provider and network provider have the same, high levels of trust and regulation. This may be possible for applications that DASH and HLS target.
* The UDP Options mechanism is nearly standardized but its use in sol 11, 27 needs to address metadata minimization to be used without encryption (e.g., like an extended DSCP) and would need security analysis.
* The UDP Options mechanism in Sol 12 uses obfuscation and can be used for RTP and QUIC (and for KI#4), but a full security analysis and minimization of metadata will take time. This may be a viable mid/long-term approach for two party metadata exchange.
* UDP connect proxying in sol 24, 26 are protected on-path but data minimization is not considered. Sol 26 in forwarding mode is intended for QUIC media transports and sol 24 with proxying incurs higher cost of proxying and re-encryption. It is also not clear what data application providers will be willing to expose as encrypted data. These may be a viable mid/long-term approach for two party metadata exchange.
* Preconfigured GTP based approach in sol 25 may not be acceptable for application servers. Application server network stack are usually heavily optimized and have frameworks for only commonly used protocols in that space.

The solutions do not fully address the principle of data minimization, security and various other aspects outlined in 7.X below. Mixing solutions like sol 24/26 with sol#12 can possibly yield a solution that addresses side channel efficiency and security, but it would require extensions to QUIC aware proxying to carry metadata and would still be limited to QUIC protocols like RoQ (i.e., no RTP/cryptex support). UDP options in #11 and #12 have longer term potential but is also not ready for Rel 19. The question of metadata (i.e., what kind of information is acceptable for an application provider) and what is practical to standardize in the IETF remains open.

The considerations in 7.X below identify some aspects by which to evaluate KI#2.

 **\* \* \* \* 1st Change (all new text) \* \* \* \***

# 7 Overall Evaluation

Editor's note: This clause provides evaluations of different solutions.

## 7.X Key Issue 2 Considerations

Solutions proposed for KI#2 use side channels that are separate from the e2e media transport to transport metadata. However, the use of side channels to address the needs for cooperative exchange is still being researched and few standards exist. Many aspects that need more investigation include the scalability of solutions, collaboration between one or more parties on-path, and the amount and nature of data shared (also see RFC 9419 – Considerations on Application – Network Collaboration Using Path Signals).

Some principles:

1. For encrypted communications and metadata, protocols, and mechanisms that different stakeholders (user, network operator, application provider) can accept explicitly should be considered.
2. Applications may serve different networks including mobile, Wi-Fi or fixed networks. Metadata to assist with QoS (in N6/IP network) should be possible to use across different access networks.
3. Protection of sensitive information and detection of modification (integrity protection) of any information on path is necessary. Traffic analysis of the metadata should reveal no additional information.
4. Metadata should be minimized to avoid leakage on path and reduce the amount of information revealed to trusted parties on path.
5. Encrypted side channel with metadata in a small packet can introduce significant overhead and delays. Mitigation of these costs should be considered.
6. Related to several points above, the process to standardize the metadata in the IETF (which is responsible for N6 protocols) and challenges related to the limited time to standardize for Release 19 should be considered a key factor.

**\* \* \* \* End of Changes \* \* \* \***

1. Encryption using AES is efficient for bulk encryption (e.g., packets of entire interface with IPSec) or lower layers. TCP/TLS encrypts large chunks (16 KB/11+ packets at a time) for optimizing latency and throughput. As packet (chunk) sizes go down, the cost incurred for encryption/decryption does not reduce significantly (i.e., implication for small packets of 50 – 100 B of metadata in a side channel). [↑](#footnote-ref-2)