Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 4, 2021

S. Peng
Z. Li
Huawei Technologies
D. Voyer
Bell Canada
C. Li
China Telecom
P. Liu
China Mobile
C. Cao
China Unicom

October 1, 2020

APN Security and Privacy Considerations
draft-peng-apn-security-privacy-consideration-00

Abstract

APN (Application-aware Networking) architecture aims to convey Application-aware Information including application/user/flow identifiers and SLA/service requirements along with the data packets into the network and make the network aware of applications and their requirements in order to provide corresponding application-aware network services and guarantee their SLA requirements.

There have been challenges of the privacy and security issues that could potentially be introduced by conveying the application-aware information into the network. This document describes the security and privacy considerations of APN in various possible scenarios wherein APN will be deployed.

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 RFC 2119 [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 https://datatracker.ietf.org/drafts/current/.

Copyright Notice

Table of Contents

1. Introduction

Application-aware Networking (APN) is introduced in [I-D.li-apn-framework] and [I-D.li-apn-problem-statement-usecases]. APN conveys Application-aware Information (App-Info) such as application/user/flow identifiers and SLA/service requirements along with data packets into network [I-D.li-6man-app-aware-ipv6-network] and make the network aware of applications and their requirements in order to provide corresponding network services and guarantee their SLA requirements. The ever-emerging network services such as network slicing and iOAM can be further enhanced with the application awareness in the network enabled by APN.

Since with APN the Application-aware Information (App-Info) such as application/user/flow identifiers and SLA/service requirements are conveyed along with the data packets into network, APN has been challenged that it may potentially impose privacy and security issues.

This document describes the privacy and security considerations of APN.

2. Terminologies

AI: Artificial Intelligence

APN: Application-aware Networking

BNG: Broadband Network Gateway

CPE: Customer Premise Equipment

DPI: Deep Packet Inspection

OS: Operating System

RG: Residential Gateway

UPF: User Plane Function

5GC: 5G Core

3. Adding Points of Application-aware Information

3.1. APN Framework

The APN framework is introduced in [I-D.li-apn-framework], as shown in the Figure 1.

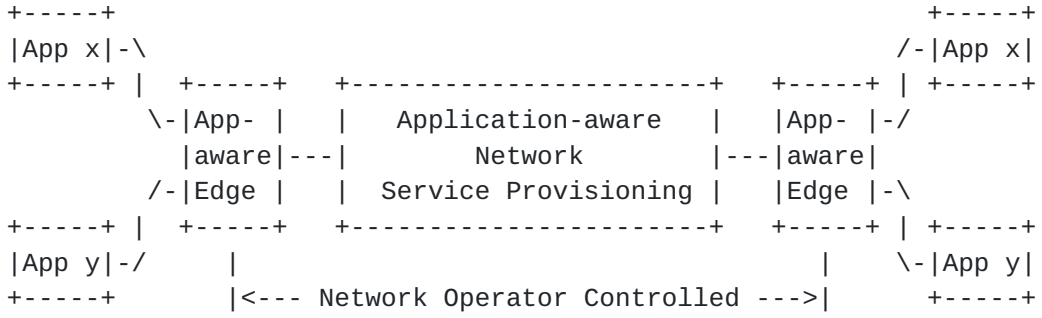

Figure 1. APN6 Framework

With APN, the application-aware information is added to the data packets (e.g. in the IPv6 extensions headers [I-D.li-6man-app-aware-ipv6-network]) and delivered to the network, wherein, according to the carried app-info, the application-aware network services such as application-aware network slicing are provisioned.

The app-info can be added either directly by the application (e.g. App x in the Figure 1) or at the network edge devices (i.e. App-aware Edge in the Figure 1).

3.2. App-info added by the application

The app-info can be added directly by the application, which is called as the host-side solution. With the host-side solution, after the app-info is obtained by the corresponding application, it will be added to the data packets during its encapsulation process going through the protocol stack in the OS.

The host-side solution may require an update of the underlying operating system in order to allow the application element to pass the app-info to the socket service when building the packet header.

3.3. App-info added by the Network Edge Device

The app-info can be added by the network edge device, which is called as the network-side solution. With the network-side solution, the app-info is added according to the configured policy at the network edge device, which is under the control of the network operator.

4. Privacy Considerations

In this section the privacy aspects of APN are evaluated according to the most common scenarios where APN could be deployed.

4.1. Network Operator Self-Operating Application

Nowadays, more and more network operators start operating their own applications. In this scenario, the network operators control and manage both, their own networks and their own applications. Typically, the steering of application traffic is triggered at the packet source (within the operator domain) and ends at the egress point of the operator's network which implies that the APN scheme is confined within the operator's domain.

When the APN information is inserted, used and removed in/from the data packet inside the operator's domain, no additional security and privacy issues are introduced other than the usual ones when carrying metadata within a controlled domain (e.g. SFC).

4.2. Application Providers Self-Operating Network

Similarly, more and more application providers start building and operating their own networks. In this way, the application providers control and manage both their own networks and their own applications.

This scenario is actually the same as the previous one, which is, the APN scheme is confined within a controlled domain owned by the application provider. In this way, no additional security and privacy issues are introduced other than the usual ones when carrying metadata within a controlled domain (e.g. SFC).

4.3. Network Operator's Limited Controlled Domain

In this case, the App-Info is only used within the network operator's controlled limited domain. A limited domain is intended as a portion of the operator infrastructure where APN is deployed. When the application packet reaches the boundary of the limited domain, the app-info is added to the packet, used in order to steer the packet within the limited domain and then removed when the packet leaves the limited domain.

No matter what kind of app info is tagged from outside, within the APN network domain, the App-Info is added at the ingress node and removed from the egress node. In the APN network domain, the App-Info only serves for the application-aware network service

provisioning, and there is no harm for the outside of the APN network domain.

This case is a sub-case of the previous one where the operator controls the whole infrastructure and applies APN only on a limited part of it. Similarly, the privacy aspects related to APN are no different from the existing mechanisms already used in order to tag and forward data packets.

4.4. Network Operator Controlled Edge Devices

In this case, it is assumed that the App-Info is added by the network edge device [I-D.li-apn-framework] based on a matching policy, which is configured by the network operator. The matching policy can be directly based on the port being used (e.g., QinQ) or derived through other mechanisms (e.g., AI (Artificial Intelligence)) and not through mechanisms like DPI (Deep Packet Inspection) which may incur privacy issues in some cases. Although, in this way, the level of granularity may not be as good.

No additional privacy issues are introduced than any other policy based solution where the packet is inspected, tagged and steered according to a preconfigured policy.

4.5. Encrypted App-Info carried in the data packets

Here, the App-info is added directly by the applications and it is encrypted. In this case, while the packets carrying the App-Info are being delivered along the path, the privacy-related information that may be exposed by the original plain App-Info won't be leaked since it is already encrypted. The nodes along the path won't be able to infringe the privacy of the application's user.

The traffic steering at the network headend/ingress can be simply based on the encrypted App-info if it is what the network operator installed in its forwarding table. If the traffic steering needs to be based on the decrypted App-info, a key should be shared between the encryption source node and the decryption destination node, which is based on a trustworthy agreement.

4.6. Explicit App-Info carried in the data packets

If the App-info is added directly by the applications but it is not encrypted, the privacy-related information of the application's user might be exposed along the path.

There might be privacy issues introduced by the APN in this scenario. Mechanisms on the proper encoding of the App-Info would be required.

APN is based on the trust relationship between the users, the network operators and the application providers. If the users want to enjoy the application-aware network services, such as game acceleration provided by the network operator, they will need to sign the trustworthy agreement with the network operator. If it is the network operator or application provider that owns both the network and application as in 4.1 and 4.2, it makes the trust relationship more easily to be set up, that is, if the users sign the agreement with them the relationship is established.

5. Security Considerations

In this section the security aspects of APN are evaluated in the following scenarios.

5.1. Inter-DC Scenario

In order to reduce the IT investment, most enterprises have moved some of their applications and data into the Cloud. For the large-scale enterprises, generally their applications and data are distributed across multiple clouds. The communication in between clouds and datacenters represents most of the inter-DC traffic. Since the servers generating the traffic often belong to certain enterprise, the source and the destination of the traffic and the path used are known. There is no need for doing the access control even when APN is deployed in this scenario.

To be more general, the Inter-DC traffic is usually originated and destined within the domain, and steered according to inter-DC policies. The presence (or not) of APN information in data packets does not interfere with the inter-DC traffic scheme and does not require any additional security measure.

5.2. Enterprise Scenario

The enterprise traffic often accesses from CPE (Customer Premise Equipment) towards the Internet or Clouds along the paid leased lines through the controlled BNG (Broadband Network Gateway) interfaces, which means that the enterprise traffic is going to be validated and authorized by the BNG, as shown in Figure 2.

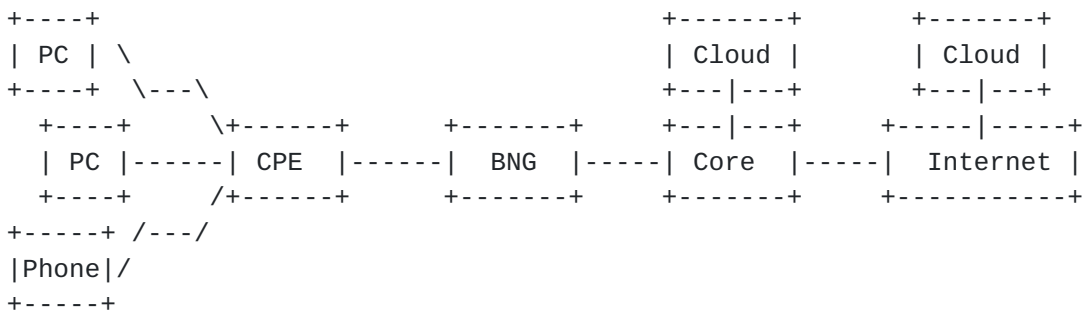

Figure 2. Enterprise Scenario

Therefore, there will be no additional security issue introduced by APN in the Enterprise scenario.

5.3. Broadband Scenarios

APN may only introduce security issues when the users access the operators' networks from an untrusted domain. However, as shown in Figure 3, the user traffic from the home broadband will be checked and authorized by the BNG, while as shown in Figure 4, the user traffic from the mobile broadband will be authorized by the 5GC function.

In the home broadband scenario, generally a home broadband user is authorized using the MAC address of the RG (Residential Gateway), the VLAN/QinQ, and the input port on the BNG. Whether the home broadband user has bought a value-added service like game acceleration will be checked further. With APN, the value-added service can be indicated by the App-Info carried in the packets, and it will be checked against the one that the operator has configured in the BNG. If the carried App-Info matches the corresponding policy entry for the user, the validation is passed and the access control is released, so the user can start enjoying the acceleration service for its application.

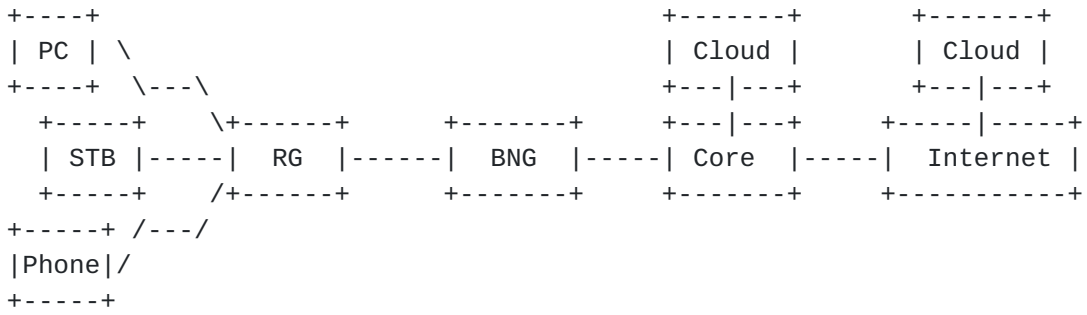

Figure 3. Home Broadband Scenario

In the mobile broadband scenario, a UE is authorized by the 5GC function, and the traffic steering and QoS policy are enforced by the UPF (User Plane Function) node. Whether the user has bought a value-added service like game acceleration will be checked against the configured policies. With APN, the value-added service can be indicated by the App-Info carried in the packets, and it will be checked against the one that the operator has configured in the UPF node. If the carried App-Info matches the corresponding policy entry, the validation is passed and the access control is released, so the user can start enjoying the acceleration service for its application.

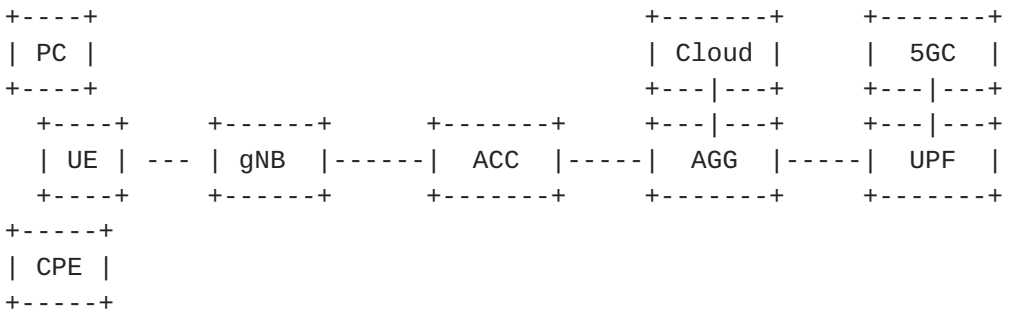

Figure 4. Mobile Broadband Scenario

6. Potential Security Issues and Mitigations

There are potentially four scenarios where APN might introducing security issues.

6.1. One application within one terminal

An application in one terminal (UE) may add arbitrary App-Info including its requirements on the network.

This issue can be tackled or resolved via the OS. If the App-Info is eventually sent out along with the data packets, it can still be blocked by the BNG or 5GC since it violates the already-signed agreements between the users and the network operators.

Note that this is not different from any service/SLA selection scheme where the application/user traffic may be marked but anyway checked at ingress for correctness of the marking.

6.2. Two different applications within one terminal

One application in the terminal (UE) may add the App-Info of another application in the same terminal. For example, the Email App attempts to forge the high-level SLA guarantee of the Live Video Streaming App.

This issue can be tackled or resolved via the OS. If the App-Info is eventually sent out along with the data packets, it can still be blocked by the BNG or 5GC since it violates the already-signed agreements between the users and the network operators.

6.3. The same applications in two terminals

An application in one terminal may forge the App-Info of the same App running in another terminal.

Once the App-Info is sent out along with the data packets, the existing network security mechanisms such as HMAC can be utilized to validate the source of the forged App-Info being sent out from.

6.4. App-info tampered along the way

The App-Info may be tampered along the way between the App-Info Encapsulator and the Network Boarder Node.

Once the App-Info is sent out along with the data packets, the existing network security mechanisms such as HMAC can be utilized to validate the tampered App-Info.

7. IANA Considerations

There are no IANA considerations in this document.

8. Contributors

Chongfeng Xie
China Telecom
China

Email: xiechf@chinatelecom.cn

Liang Geng
China Mobile
China

Email: gengliang@chinamobile.com

Shuai Zhang
China Unicom
China

Email: zhangs366@chinaunicom.cn

9. Normative References

[I-D.li-6man-app-aware-ipv6-network]
Li, Z., Peng, S., Li, C., Xie, C., Voyer, D., Li, X., Liu, P., Liu, C., and K. Ebisawa, "Application-aware IPv6 Networking (APN6) Encapsulation", draft-li-6man-app-aware-ipv6-network-02 (work in progress), July 2020.

[I-D.li-apn-framework]
Li, Z., Peng, S., Voyer, D., Li, C., Geng, L., Cao, C., Ebisawa, K., Previdi, S., and J. Guichard, "Application-aware Networking (APN) Framework", draft-li-apn-framework-01 (work in progress), September 2020.

[I-D.li-apn-problem-statement-usecases]
Li, Z., Peng, S., Voyer, D., Xie, C., Liu, P., Qin, Z., Ebisawa, K., Previdi, S., and J. Guichard, "Problem Statement and Use Cases of Application-aware Networking (APN)", draft-li-apn-problem-statement-usecases-01 (work in progress), September 2020.

[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/info/rfc2119>.

Authors' Addresses

Shuping Peng
Huawei Technologies
Beijing
China

Email: pengshuping@huawei.com

Zhenbin Li
Huawei Technologies
Beijing
China

Email: lizhenbin@huawei.com

Daniel Voyer
Bell Canada
Canada

Email: daniel.voyer@bell.ca

Cong Li
China Telecom
China

Email: licong@chinatelecom.cn

Peng Liu
China Mobile
China

Email: liupengyjy@chinamobile.com

Chang Cao
China Unicom
China

Email: caoc15@chinaunicom.cn