Internet Engineering Task Force
Internet-Draft
Intended status: Informational
Expires: April 27, 2015

M. Qi
X. Zhuang
China Mobile

October 24, 2014

Integrated Security with Access Network Use Case
draft-qi-i2nsf-access-network-usecase-00

Abstract

In traditional telecommunication system, operators usually provide general and limited security protection service for users during access (e.g. AKA in 3G/4G network). Now, with the development of network virtualization technology, the physical network device is became a network function software which is running on virtual machine and the network functions can be flexible and elastic. So operators can provide more flexible security function to users through network function. In order to provide more flexible security function, an interface between operator's network and user should be needed. The interface will be used to request/negotiate/allocate/ operate (Virtual) Network Security Functions from operator's network. This draft describes use cases for using the interface in operator's network environment.

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 April 27, 2015.

Table of Contents

1. Introduction

In traditional telecommunication system, operators will provide security protection function for users when they request to access the network, such as authentication, encryption and integrity protection function, etc. However, considering efficiency and costs of the network deployment, operators usually provide general and limited security protection service for users during access(e.g. AKA in 3G/4G network).Now, with the development of network virtualization technology, security function virtualization can help operators to provide flexible and reliable security protection service for users access.

2. Conventions used in this document

The section clarifies the intended meaning of specific terms used within this document.

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 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying [RFC2119] significance.

3. Interface about sending security configuration information from network to UE

In the traditional telecommunication network, when a user requests to access network, operators will provide security service during access procedure to ensure that users can securely connect to the telecommunications network. This security solution is not provided by the access equipment such as CPE, but by the operator's core network equipment (e.g. MME). As operators provide such security solutions by using physical network equipment, which would cause limitation for security service, operators should provide the same security function to all users, such as unified authentication mechanism (usually pre-shared key based authentication), same encryption capabilities and so on.

But under virtualized environment, the physical network device is as network function software which is running on virtual machine and the network functions can be flexible and elastic. So operators can provide more flexible security function to users through virtualized network function.

For example, it can provide different authentication function for different users. Authentication mechanism can be provided based on pre-shared key or based on certificate. What is more, it can also provide flexible encryption function. Operators can provide encryption by usingnot only encryption algorithms, but also keys with different lengths.

An concrete example is, Internet of Things(IoT)business. When a simple IoT services such as street lighting controlling need connect to the network, it only needs to implement simple network authentication with users, so it can choose one-way pre-shared key based access authentication through the interface like GSM authentication. While for another IoT business, such as home remote monitoring, it needs to utilize mutual authentication with pre-shared key between network and users. As a result UMTS access authentication would be chosen and applied through the interface. For some other kind of more sensitive IoT business, such as automatic selling machine, it would need certificate based authentication. As a result, operators need to inform the UE of the configuration information, and help UE to make a decision.

So an interface to sending such configuration is needed. The list of allowed security functions and prohibited security functions should be both passed in the interface.

4. Interface about optional security function negotiation between Network and UE

Under current network access environment, when users want to access to the network, operators can only provide necessarily basic security functions, which avoids impact to all of users by using advanced security functions designed for a specific user. However, in a virtualized network, operators can customize more flexible security functions for users.

For example, if a user does not want to receive spam, operator can provide countermeasures like key words filtering function to such user; if a user want to keep communication data with high security, operator can provide enhanced services based on IDS / IPS. And if users want to have no security requirement to speed up, there is no need for operator to provide any security functions.

In this case, an interface is needed for operators. It can inform the UE about what optional security functions they could provide.

5. UE proposed security request to the network

Before the virtualization of the network, UE can only be provided the fixed security services provided by operators when access to the network, which is mentioned as above. In a virtualized environment, operators has ability to provide more service. Therefore, UEs get new chance to send security services request based on its specific requirement to operators. And operators can fulfill users requirement by increasing, updating the corresponding network security functions.

In this case, a new interface is needed. It can be used by users to inform specific network element, like operator-specific gateway. Operators can convert the user's functional requirements into the corresponding security functions settings, then provide security access services in accordance with the required security function.

There are some kinds of fulfillment of such interface. For example, users don't want to receive abnormal traffic, like advertisement, worms, IP detecting flows, etc. Operators can provide IP address filtering capabilities according to the IP address defined requirements which have been negotiated with users. Alternatively, according to a list of pre-defined options, users can send the functions and configuration requirements in a specific format to the

operator's gateway, and operator provide services directly according to enabling security functions from related requirements. A concrete example is, a user hoping to filter traffic in tcp 21 port sent "tcp 21 port block on firewall " command directly to the operator gateway, then operator send the same command directly to the virtual firewall corresponding to users ,after testing the legality of the message.

6. The Benefits

It will bring benefits by defining such interface. Operator could send specific security configurations and optional security service list to user equipments. UE could send security policy/function request to operators. Through such interface, operator could provide more flexible and tailored security functions for specific user, which would lead more efficient and secure protection to each end user.

7. IANA Considerations

TBD

8. Informative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Authors' Addresses

Minpeng Qi
China Mobile
32 Xuanwumenxi Ave,Xicheng District
Beijing 100053
China

Email: qiminpeng@chinamobile.com

Xiaojun Zhuang
China Mobile
32 Xuanwumenxi Ave, Xicheng District
Beijing 100053
China

Email: zhuangxiaojun@chinamobile.com