INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2017-2020

TD 0335

STUDY GROUP 17

English only

Original: English

Question(s):	2/17	Geneva, 22-30 March 2017

TD

Source:	Editors
Title:	Template for new work item X.sdnsec-3 on “Security guideline of Service Function Chain based on software defined network”
Purpose:	Proposal

Contact:	Shu Guo China Mobile P.R.China	Tel: +86 15801696688-33251 Fax: E-mail: guoshu@chinamobile.com
Contact:	Qi Yuan CATR P.R.China	Tel: Fax: E-mail: yuanqi@caict.ac.cn
Contact:	Junjie Xia China Unicom China	Tel: Fax: E-mail: xiajj2@chinaunicom.cn
Contact:	Zhiyuan Hu Alcatel-Lucent Shanghai Bell P.R.China	Tel: Fax: E-mail: zhiyuan.hu@alcatel-sbell.com.cn
Contact:	Feng Zhang China Mobile P.R.China	Tel: +86-15801696688-33022 Fax: E-mail: zhangfeng@chinamobile.com
Contact:	JungSoo Park Electronic and Telecommunications Research Institute Republic of Korea	Tel: +82-42-860-6514 Fax: E-mail: pjs@etri.re.kr

Keywords: SDN; Service Function Chain

Abstract: This recommendation analyses the security threats encountered in the Service Function Chain based on software defined network, and provides the security guideline for SDN-based Service Function chain architecture.

C0060 was reviewed and accepted by joint meeting with Q2/17 and Q6/17. In addition, the comments and suggestions raised in this meeting were also accepted. The major modifications are listed below:

1) Liaisons with other study groups or with other standards bodies: IETF,ONF,ETSI.
2) The delegate from ETRI (Republic of Korea) support this new work item.

After discussion, the meeting agreed to this new work item.

Much more contributions are welcome.

Background:

Service Function Chain enables the administrators to distribute network policies more efficiently and conveniently, while Software-Defined Networking (SDN) helps to adjust traffic dynamically according to the changing requirements. These two technologies can be combined to give the network higher flexibility and stronger capability of serving on demand. IETF published RFC7665" Service Function Chain (SFC) Architecture"[1]; ETSI defines a use case on VNF Forwarding Graph[5]; ONF has finished a study on such SDN-based Service Function Chain and published "L4-L7 Service Function Chaining Solution Architecture"[2]. And industries have been developing similar solutions and products as well. However, it is realized that such SDN-based Service Function Chain also introduces new security challenges into the network, not only the legacy SDN threats, but also some new threats along with Security Function Chain, and there is an urgent need for a security guideline.

Because of using the SDN architecture, the common SDN threats will show up in the Service Function Chain based on SDN according to [ITU-T X.1038] and [ITU-T Y.3300], such as more severe DoS/DDoS attack caused by centralized SDN controller, and attacks on Application-Control interface, etc.

More security issues will also arise because of the deployment of the Service Function Chain. New network elements are introduced, like Service Function Chain Forwarder, and new information will be transferred among the network elements, like Service Function Chain. Threats against these entities should be mitigated.

Objectives:

This recommendation is to set up a new work item to analyze the security threats of the SDN-based Service Function Chain and gives security guideline on how to mitigate these threats. This work item contains the security architecture for SDN-based Service Function Chain, the threat analyse of network elements and corresponding interfaces, the analysis of problems of policy management, and countermeasures of this problems.

This security guideline can help the reader to understand the security risks encountered when using SDN-based Service Function Chain and further help to develop and implement secure Service Function Chain architecture.

Gap Analysis

Currently, IETF SFC has published and is developing the following standards and drafts:

(1) ITU-T X.1231 Technical strategies for countering spam, this recommendation aims to define general technical strategies for countering spam, and it is not specific to advertising spam. It mainly defines technical strategies, not detailed technical architecture, technical flows, etc. Also, the technical strategies specified in X.1231 are quite suitable for traditional spams, e.g. email spam, SMS spam, but some of the strategies are not quite applicable for internet services, e.g. equipment strategies and network strategies, also some technical methods are missing, e.g. automatic training, big data analytics, advanced algorithms.

(1) RFC7665 Service Function Chain (SFC) Architecture, this draft is an overview of a service chaining architecture that clearly defines the roles of the various and the scope of a service function chaining encapsulation

(2) RFC 7498 Problem Statement for Service Function Chaining, this draft outlines the problems encountered with existing service deployment models, like topological dependencies, configuration complexity, etc.

(3) draft-mglt-sfc-security-environment-req-02(individual draft),this draft describes SFC environment Security requirements, protocol independed, nothing about SDN.

(4) draft-ietf-sfc-nsh-10 (ietf draft),this draft shows NSH, which is the SFC encapsulation referenced in RFC7665.

(5) draft-ietf-sfc-control-plane-08 (ietf draft), this draft describes requirements for conveying information between Service Function Chaining (SFC) control elements and SFC data plane functional elements.

(6) draft-ietf-sfc-dc-use-cases-05 (ietf draft), this draft describes use cases within a data center environment and provides SFC requirements for data center centric use cases.

In ONF, L4-L7 WG has published a standard TS-027 “L4-L7 Service Function Chaining Solution Architecture”, which gives how to implement SFC in SDN network to improve the inefficiencies faced by the traditional network and no security context.

In ETSI, the standard ETSI GS NFV 001 defines a use case on VNF Forwarding Graph, which is very similar to SFC. However, VNFFG only involves VNF.

In summary, the recommendations above are related to SFC, However,

1、IETF concentrates on architecture, protocol, deployment models and security environments of SFC, but not SDN-based SFC,

2、ETSI describes NFV use case, only involving VNFs into VNFFG, and not SDN related.

3、ONF shows how to implement SFC in SDN network, but no security considerations.

Annex A.1 justification for proposed draft new Recommendation ITU-T X.xxxx
Annex A.2 Draft Recommendation ITU-T X.sdnsec-3

Annex A.1

A.1 justification for proposed draft new Recommendation ITU-T X.sdnsec-3

Question:	2/17	**Proposed new ITU-T Recommendation**	**22-30 March 2017**	
Reference and title:	ITU-T X.sdnsec-3"Security guideline of Service Function Chain based on software defined network"			
Base text:	Annex A.2		**Timing:**	03-2019
Editor(s):	Feng Zhang, Chinamobile, zhangfeng@chinamobile.com Min Zuo, China Mobile, zuomin@chinamobile.com Junjie Xia, China Unicom, xiajj2@chinaunicom.cn Zhiyuan HU, Alcatel-Lucent Shanghai Bell		**Approval process:**	AAP

	zhiyuan.hu@alcatel-sbell.com.cn JungSoo Park, ETRI, pjs@etri.re.kr		
Scope (defines the intent or object of the Recommendation and the aspects covered, thereby indicating the limits of its applicability): This recommendation analyzes the security threats encountered in the Service Function Chain based on software defined network, and provides the security guideline for SDN-based Service Function chain architecture. This work item contains the security architecture for SDN-based Service Function Chain, the threat analyse of network elements and corresponding interfaces, the analysis of problems of policy management, and countermeasures of this problems.			
Summary (provides a brief overview of the purpose and contents of the Recommendation, thus permitting readers to judge its usefulness for their work): This recommendation is to analyze the security threats of the SDN-based Service Function Chain and gives security guideline on how to mitigate these threats. This security guideline can help the reader to understand the security risks encountered when using SDN-based Service Function Chain and further help to develop and implement secure Service Function Chain architecture.			
Relations to ITU-T Recommendations or to other standards (approved or under development): ITU-T Y.3300, ITU-T X.1038, ONF TS-027, IETF RFC 7665, ETSI GS NFV 001			
Liaisons with other study groups or with other standards bodies: IETF SFC, ONF L4-L7 WG			
Supporting members that are committing to contributing actively to the work item: <Member States, Sector Members, Associates, Academia> China Mobile, CATR, China Unicom, Alcatel-Lucent Shanghai Bell, ZTE, BUPT,ETRI			

Field Code Changed

Annex A.2

A.2 Draft Recommendation ITU-T X.sdnsec-3

Security guideline of Service Function Chain based on software defined network

Summary

This recommendation is to analyze the security threats of the SDN-based Service Function Chain and gives security guideline on how to mitigate these threats. This security guideline can help the reader to understand the security risks encountered when using SDN-based Service Function Chain and further help to develop and implement secure Service Function Chain architecture.

Keywords

SDN; Service Function Chain

Table of Contents

1 Scope .... 8~~6~~

2 References .... 8~~6~~

3 Definitions .... 8~~7~~

4 Abbreviations and acronyms .... 8~~7~~

5. Conventions .... 9~~7~~

6. Overview .... 9~~7~~

7.General Security Architecture of SDN-based Service Function Chain .... 9~~7~~

8. Threat analysis and requirements of critical network elements .... 9~~7~~

8.1 Critical network elements .... 9~~7~~

8.2 Security threats and requirements .... 9~~8~~

8.2.1 Security threats and requirements of SF .... 9~~8~~

8.2.2 Security threats and requirements of SFF .... 9~~8~~

8.2.3 Security threats and requirements of <xxx> .... 10~~8~~

9. Threat analysis and requirements of interfaces .... 10~~8~~

10. Security considerations of Policy management .... 10~~8~~

11. Countermeasures .... 10~~8~~

Introduction

Service Function Chain enables the administrators to distribute network policies more efficiently and conveniently, while Software-Defined Networking (SDN) helps to adjust traffic dynamically according to the changing requirements. These two technologies can be combined to give the network higher flexibility and stronger capability of serving on demand. However, it is realized that such SDN-based Service Function Chain also introduces new security challenges into the network, not only the legacy SDN threats, but also some new threats along with Security Function Chain, and there is an urgent need for a security guideline.

Because of using the SDN architecture, the common SDN threats will show up in the Service Function Chain based on SDN according to [ITU-T X.1038] and [ITU-T Y.3300], such as more severe DoS/DDoS attack caused by centralized SDN controller, and attacks on Application-Control interface, etc.

More security issues will also arise because of the deployment of the Service Function Chain. New network elements are introduced, like Service Function Chain Forwarder, and new information will be transferred among the network elements, like Service Function Chain. Threats against these entities should be mitigated.

Draft Recommendation ITU-T X.sdnsec-3

Security guideline of Service Function Chain based on software defined network

1 Scope

This recommendation analyzes the security threats encountered in the Service Function Chain based on software defined network, and provides the security guideline for SDN-based Service Function chain architecture. This recommendation covers as follows:

- Describe a general security architecture for SDN-based Service Function Chain;

- Analyze the security threats and requirements of network elements and corresponding interfaces in SDN-based service Function chain;

- Describe and analyze the problems of policy management in SDN-based service Function chain;

- Provide countermeasures of above mentioned problems;

2 References

[1] IETF RFC7665 Service Function Chain (SFC) Architecture, 2015 October

[2] ONF TS-027 L4-L7 Service Function Chain Solution Architecture, 2015 June14

[3] ITU-T X.1038

[4] ITU-T Y.3300

[5] ETSI GS NFV 001

< Others to be added>

3 Definitions

<Check in ITU-T Terms and definitions database under http://www.itu.int/sancho/index.htm if the term is not already defined in another recommendation. It could be more consistent to refer to such a definition rather than redefined it>

Service Function Chain (SFC): An ordered list of Service Function instances.

Service Function Chain Forwarder (SFF): Provides service layer forwarding. An SFF receives frames/packets carrying SFC header and forwards the frames/packets to the associated SF instances using information contained in the SFC header.

< Others to be added>

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

SFC	Service Function Chain

SFP	Service Function Chain Path
SF Proxy	Service Function Proxy
SFF	Service Function Chain Forwarder
DDoS	Distributed Denial of Service

< Others to be added>

5. Conventions

6. Overview

7.General Security Architecture of SDN-based Service Function Chain

A general security architecture of SDN-based Service Function Chain is given as below based on IETF SFC architecture and ONF L4-L7 Service Function Chain solution Architecture:

<TBD>

8. Threat analysis and requirements of critical network elements

8.1 Critical network elements

SF：<TBD>

SFF：<TBD>

SFC：<TBD>

SFP：<TBD>

SF Proxy：<TBD>

<TBD>

8.2 Security threats and requirements

<TBD>

8.2.1 Security threats and requirements of SF

<TBD>

8.2.2 Security threats and requirements of SFF

<TBD>

8.2.3 Security threats and requirements of <xxx>

<TBD>

9. Threat analysis and requirements of interfaces

<TBD>

10. Security considerations of Policy management

<TBD>

11. Countermeasures

<TBD>