

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1043

(03/2019)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Network security

Security framework and requirements for service function chaining based on software- defined networking

Recommendation ITU-T X.1043

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES (1)	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols (1)	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES (2)	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1319
Smart grid security	X.1330–X.1339
Certified mail	X.1340–X.1349
Internet of things (IoT) security	X.1360–X.1369
Intelligent transportation system (ITS) security	X.1370–X.1389
Distributed ledger technology security	X.1400–X.1429
Distributed ledger technology security	X.1430–X.1449
Security protocols (2)	X.1450–X.1459
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1043

Security framework and requirements for service function chaining based on software-defined networking

Summary

Recommendation ITU-T X.1043 analyses security threats to and specifies security requirements for service function chaining based on software-defined networking (SDN). The corresponding security countermeasures are also given. Recommendation ITU-T X.1043 also aims to help understanding of security risks encountered when using SDN-based service function chaining and implementation of secured SDN-based service function chains.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1043	2019-03-16	17	11.1002/1000/13872

Keywords

SDN, service function chain, SFC, software-defined networking.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2019

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	3
5	Conventions	3
6	Overview.....	4
7	General security framework of software-defined networking-based service function chaining	6
8	Threat analysis and requirements of critical network elements.....	7
	8.1 Critical network elements.....	7
	8.2 Security threats and requirements	7
9	Threat analysis and requirements of interfaces	12
	9.1 Interfaces	12
	9.2 Security threats and requirements	12
10	Security considerations of policy management	12
11	Countermeasures.....	12
	11.1 Countermeasures for critical network elements	13
	11.2 Countermeasures for interface security	14
	11.3 Countermeasures for secure policy management	14
	Annex A – Classification table and service function path forwarding table	15
	A.1 Classification table	15
	A.2 Service function path forwarding table	17
	Appendix I – Service function chain architecture specified by other standards development organizations	18
	Bibliography.....	20

Introduction

Service function chaining enables administrators to distribute network policies more efficiently and conveniently, while software-defined networking (SDN) helps to adjust traffic dynamically according to changing requirements. These two technologies can be combined to give a network higher flexibility and stronger capability to support on-demand services.

However, it is clear that SDN-based service function chaining also introduces new security challenges to the network, not only legacy threats associated with SDN, but also new threats associated with the service function chain (SFC).

Use of SDN architecture means that common networking threats will show up in SDN-based service function chaining, e.g., more severe denial of service/distributed denial of service (DoS/DDoS) attacks caused by a centralized SDN controller and attacks on the application-control interface.

More security issues arise because of the deployment of service function chaining. New network elements are introduced, like an SFC forwarder, and new information is transferred among network elements, like SFC classification rules and service function path (SFP) forwarding rules. Threats against these entities should be mitigated. Thus there is an urgent need for the security guidelines in this Recommendation.

Recommendation ITU-T X.1043

Security framework and requirements for service function chaining based on software-defined networking

1 Scope

This Recommendation analyses security threats encountered in service function chaining based on software-defined networking (SDN) and specifies security guidelines for SDN-based service function chaining architectures. This Recommendation:

- describes a general security architecture for SDN-based service function chaining;
- analyses security threats to and requirements of network elements and corresponding interfaces in the SDN-based service function chaining architecture;
- describes and analyses policy management problems in SDN-based service function chaining;
- suggests countermeasure solutions to meet these requirements.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T X.800] Recommendation ITU-T X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.
- [ITU-T X.1038] Recommendation ITU-T X.1038 (2016), *Security requirements and reference architecture for software-defined networking*.
- [ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 classification [b-IETF RFC 7665]: Locally instantiated matching of traffic flows against policy for subsequent application of the required set of network service functions. The policy may be customer/network/ service specific.

3.1.2 classifier [b-IETF RFC 7665]: An element that performs classification.

3.1.3 metadata [b-IETF RFC 7665]: Provides the ability to exchange context information between classifiers and SFs, and among SFs.

3.1.4 service function (SF) [b-IETF RFC 7665]: A function that is responsible for specific treatment of received packets. A service function can act at various layers of a protocol stack (e.g., at the network layer or other OSI layers). As a logical component, a service function can be realized as a virtual element or be embedded in a physical network element. One or more service functions can

be embedded in the same network element. Multiple occurrences of the service function can exist in the same administrative domain.

3.1.5 service function chain (SFC) [b-IETF RFC 7665]: A service function chain defines an ordered set of abstract service functions and ordering constraints that must be applied to packets and/or frames and/or flows selected as a result of classification.

3.1.6 service function forwarder (SFF) [b-IETF RFC 7665]: A service function forwarder is responsible for forwarding traffic to one or more connected service functions according to information carried in the SFC encapsulation, as well as handling traffic coming back from the SF. Additionally, an SFF is responsible for delivering traffic to a classifier when needed and supported, transporting traffic to another SFF (in the same or different type of overlay), and terminating the service function path (SFP).

3.1.7 service function path (SFP) [b-IETF RFC 7665]: The service function path is a constrained specification of where packets assigned to a certain service function path must go. While it may be so constrained as to identify the exact locations, it can also be less specific. The SFP provides a level of indirection between the fully abstract notion of service chain as a sequence of abstract service functions to be delivered, and the fully specified notion of exactly which SFF/SFs the packet will visit when it actually traverses the network. By allowing the control components to specify this level of indirection, the operator may control the degree of SFF/SF selection authority that is delegated to the network.

3.1.8 SFC-enabled domain [b-IETF RFC 7665]: A network or region of a network that implements SFC. An SFC-enabled domain is limited to a single network administrative domain.

3.1.9 SFC encapsulation [b-IETF RFC 7665]: The SFC encapsulation provides, at a minimum, SFP identification, and is used by the SFC-aware functions, such as the SFF and SFC-aware SFs. The SFC encapsulation is not used for network packet forwarding. In addition to SFP identification, the SFC encapsulation carries metadata including data-plane context information.

3.1.10 SFC proxy [b-IETF RFC 7665]: Removes and inserts SFC encapsulation on behalf of an SFC-unaware service function. SFC proxies are logical elements.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 service function chain classification rule: A rule generated and maintained by a service function chain (SFC) controller and classifier, respectively. It reflects the policies for binding an incoming flow to a given SFC and service function path (SFP). An SFC classification rule can be translated into an SFC flow rule by the software-defined networking (SDN) controller and formed into an entry in an SFC classification table, like an SDN flow entry in an SDN flow table.

3.2.2 service function chain controller: A function in a software-defined networking (SDN) controller that instructs the functional elements on the service function chain (SFC) resource layer to process packets within an SFC-enabled domain. After receiving the SFC requirements from the applications (apps), the SFC controller translates the requirements into the SFC classification rules and service function path (SFP) forwarding rules and sends them to the classifiers and the service function forwarders (SFFs), respectively, via the SDN controller.

3.2.3 service function chain flow rule: A flow rule on the classifiers and the service function forwarders (SFFs) that are translated by the software-defined networking (SDN) controller from the service function chain (SFC) classification rule and the service function path (SFP) forwarding rule.

3.2.4 service function path forwarding rule: A rule generated and maintained by a service function chain (SFC) controller and a service function forwarder (SFF), respectively. It reflects the policies for forwarding an incoming flow to a given service function (SF). A service function path (SFP) forwarding rule can be translated into an SFC flow rule by the software-defined networking

(SDN) controller and formed into an entry in an SFP) forwarding rule table like an SDN flow entry in an SDN flow table.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL	Access Control List
AES	Advanced Encryption Standard
app	application
DDoS	Distributed Denial of Service
DoS	Denial of Service
HMAC	Hash-based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
LSP	Label-Switched Path
MPLS	Multi-Protocol Label Switching
NBI	Northbound Interface
NSH	Network Service Header
OSI	Open Systems Interconnection
PSK	Pre-Shared Key
RBAC	Role-Based Access Control
SDN	Software-Defined Networking
SF	Service Function
SFC	Service Function Chain
SFF	Service Function Forwarder
SFP	Service Function Path
SI	Service Index
SPI	Service Path Identifier
TLS	Transport Layer Security
TTL	Time To Live
VNF	Virtualized Network Function

5 Conventions

In this Recommendation:

The keywords "**is required to**" indicate a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "**is recommended**" indicate a requirement that is recommended but which is not absolutely required. Thus, this requirement need not be present to claim conformance.

The keywords "**is prohibited from**" indicate a requirement that must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.