

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1046

(12/2020)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Network security

**Framework of software-defined security in
software-defined networks/network functions
virtualization networks**

Recommendation ITU-T X.1046

ITU-T

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
QUANTUM COMMUNICATION	
Terminologies	X.1700–X.1701
Quantum random number generator	X.1702–X.1709
Framework of QKDN security	X.1710–X.1711
Security design for QKDN	X.1712–X.1719
Security techniques for QKDN	X.1720–X.1729
DATA SECURITY	
Big Data Security	X.1750–X.1759
5G SECURITY	X.1800–X.1819

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

Recommendation ITU-T X.1046

Framework of software-defined security in software-defined networks/network functions virtualization networks

Summary

Recommendation ITU-T X.1046 specifies a framework of software-defined security in software-defined networks (SDNs) and the network functions virtualization (NFV) networks. This framework utilizes key advantages of SDN/NFV technologies such as on-demand capacity scale-in/scale-out, dynamic and intelligent security policy control regarding real-time network status, separated deployment of control layer and data forwarding layer, full view of traffic for monitoring and unified security policy setting.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1046	2020-12-14	17	11.1002/1000/14442

Keywords

SDN/NFV security, security controller, software-defined security.

* 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/11.1002/1000/114442>.

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/software copyrights, 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 appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2021

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.....	1
4	Abbreviations and acronyms	3
5	Conventions	4
6	Overview	5
7	Security challenges for SDN/NFV network	5
8	Requirements for software-defined security in SDN/NFV networks.....	6
9	Reference framework of software-defined security	6
	9.1 Reference framework	6
	9.2 Components.....	8
	9.3 Interfaces	11
	9.4 Lifecycle management of virtualized security function instance	12
10	Reference implementation of software-defined security	15
	10.1 Software-defined security deployment in NFV environment	15
	10.2 Software-defined security deployment in SD-WAN.....	16
	Bibliography.....	18

Introduction

In recent years traditional telecommunication networks have shown their disadvantages such as long construction cycles, high costs and poor flexibility. These constraints are most evident in the slowdown on the development and deployment of emerging services.

The introduction of software-defined networks (SDNs) and network functions virtualization (NFV) technologies fundamentally changes the way networks are built and operated, mainly by taking advantage of general-purpose hardware, virtualization software and programmable services. With SDN and NFV, network operation and maintenance costs are reduced, resource utilization is improved, network flexibility is increased, and time-to-market of new services is considerably decreased.

SDN and NFV are considered as innovation technologies for telecommunications network evolution. However, these technologies bring new security challenges for telecommunications networks. Traditional security concepts based on static, passive, separate and manual operations of security defence systems do not work well in the SDN/NFV network environment. New security concepts based on dynamic, proactive, centralized and intelligent security management capabilities are needed.

This Recommendation provides a framework of software-defined security in SDN/NFV networks. This framework utilizes key advantages of SDN/NFV technologies such as on-demand capacity scale-in/scale-out, dynamic and intelligent security policy control regarding real-time network status, separated deployment of control layer and data forwarding layer, full view of traffic for monitoring and unified security policy setting. This framework is a layered framework, it provides security orchestration, centralized and automated security policy management, and intelligent security analysis and response.

Recommendation ITU-T X.1046

Framework of software-defined security in software-defined networks/network functions virtualization networks

1 Scope

This Recommendation specifies a framework of software-defined security in software-defined networks (SDNs) and the network functions virtualization (NFV) networks. This Recommendation provides the following:

- analysis of the main security challenges including technical and operational aspects in telecom operators' SDN/NFV based networks;
- summarization of security requirements to address these challenges in SDN/NFV networks;
- introduction of the concept of 'software-defined security' based on identified requirements;
- definition of a framework for 'software-defined security' with functionality requirements for each component; and
- guidelines on implementation of software-defined security.

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.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*.
- [ITU-R M.1224-1] Recommendation ITU-R M.1224-1 (2012), *Vocabulary of terms for International Mobile Telecommunications (IMT)*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 security policy [ITU-R M.1224-1]: A set of rules which define and constrain the types of security-relevant activities of entities and parties.

3.1.2 policy conflict [b-ITU-T X.1036]: It defines the actions of two rules contradicting each other. The entity implementing the policy will not be able to determine which action to perform. To prevent this situation, the implementers of policy systems must provide conflict detection and avoidance or resolution mechanisms.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 distribution of security policy: A capability to distribute security policies to security functions.

3.2.2 flow collection function: A function for collecting network traffic so as to identify security threats. Commonly used technologies are those such as IP flow information export (IPFIX) [b-IETF RFC 3917] and sFlow [b-IETF RFC 3176].

3.2.3 forwarding policy: A set of rules which are distributed to switches by a SDN controller to indicate the way switches should forward network traffic.

3.2.4 lifecycle management of virtualized security function instance: A set of functions required to manage the instantiation, maintenance and termination of a virtualized security function.

3.2.5 network topology: Configuration of links connecting cross-connect physical devices (e.g., physical network device, physical security device) and virtualized functions such as virtualized network function (VNF) and virtualized security function (VSF).

3.2.6 optimization of security policy: Capabilities and operations to detect the activated security policies, redundant policies, usage frequencies, etc. and implement optimizations such as deleting non-activated security policies, merging or deleting redundant policies, etc.

3.2.7 security configuration parameter: A set of parameters which describe the features of the security function, such as maximum bandwidth, maximum number of connections, etc. supported by the security function, protected object and security actions of the security function.

3.2.8 security device: A physical device that provides security functions (e.g., firewalls, IDs, security gateways, and security management servers).

3.2.9 security information and event management system: A security and audit system that supports threat detection, compliance and security incident management through the analysis of security events.

NOTE – The security information and event management system collects, manages and analyses log events, and then produces operational advice or operates according to the results of the analysis.

3.2.10 security function vendor: A creator of a security function that provides physical/hardware security devices or software which executes security actions.

3.2.11 security function: Capabilities implemented in a physical/hardware device or by a software which executes security actions [b-UNISAFE] (e.g., detecting security malicious URLs, dropping a traffic, detecting DoS/DDoS attacks, scanning and removing viruses, traffic limit, access control based on source IP or destination IP, etc.) according to security policies.

3.2.12 security policy conflict: A contradiction when two security policies deal with the same flow, for example, one security policy is to drop a flow and another is to forward the flow.

3.2.13 service resource: A set of network devices in the telecom operator's network, which work together to deliver services to the telecom operator's customers.

3.2.14 security situation: Security information which is collected through continuous monitoring activities on a network in order to detect anomalies and potential security threats.

3.2.15 security situation awareness: Capability to provide information about the security situation.

3.2.16 SDN controller: A dedicated network element which provides a means to program, orchestrate, control and manage the network resources through software (i.e., SDN applications).

NOTE – Definition adapted from [ITU-T Y.3300].

3.2.17 software-defined security: Technologies enabling security capabilities such as decoupling of the security control plane with the enforcement plane of physical security devices, centralization of a decoupled security control plane, and opening of a programmable interface can achieve