

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.1038

(10/2016)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Information and network security – Network security

Security requirements and reference architecture for software-defined networking

Recommendation ITU-T X.1038

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	
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	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	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
PKI related Recommendations	X.1340–X.1349
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.1038

Security requirements and reference architecture for software-defined networking

Summary

Recommendation ITU-T X.1038 supports security protection and provides security requirements and a reference architecture for software-defined networking (SDN). This Recommendation identifies new security threats as well as traditional network security threats to SDN, defines security requirements, provides possible security countermeasures against new security threats, and designs a security reference architecture for SDN.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1038	2016-10-14	17	11.1002/1000/13058

Keywords

SDN security, security reference architecture, security requirement, security threat.

* 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 2017

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	2
3.1	Terms defined elsewhere	2
3.2	Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	3
5	Conventions	3
6	Overview.....	4
7	Security threats and requirements.....	4
7.1	SDN application layer	4
7.2	SDN control layer.....	5
7.3	SDN resource layer.....	8
7.4	Application-control interface.....	9
7.5	Resource-control interface.....	10
8	Security reference architecture for SDN.....	11
8.1	SDN application layer	11
8.2	SDN control layer.....	13
8.3	SDN resource layer.....	16
8.4	Multi-layer security management.....	17
Annex A	– Use cases of new security threats to SDN	19
A.1	Use case 1: Bypassing a predefined mandatory policy	19
A.2	Use case 2: Data eavesdropping attacks by inserting fraudulent flow entries	20
Annex B	– Fine-grained naming scheme for flow entry.....	22
B.1	Fine-grained naming scheme for flow entry	22
	Bibliography.....	23

Introduction

Generally, security threats to SDN are common to other targets and to traditional networking, but the profile of the threats (including their likelihood and impact and hence their overall risk level) changes with the new SDN architecture. With a centralized SDN controller, the impact of a denial-of-service (DoS)/distributed denial-of-service (DDoS) attack can be higher than that directed against a single router. Some new functional entities (e.g., SDN controller), protocols (e.g., ONF OpenFlow) and interfaces (e.g., application-control interface, resource-control interface) according to the framework of SDN [ITU-T Y.3300] will pose new security threats. All these security threats must be understood and addressed.

This Recommendation describes use cases to detail new security threats when introducing SDN. This Recommendation identifies security threats for the SDN application layer, SDN control layer, SDN resource layer, application-control interface, and resource-control interface according to the framework of SDN [ITU-T Y.3300]. This Recommendation also defines security requirements from above security threats analysis and studies possible security countermeasures against new security threats. With this information, a security reference architecture for SDN is designed based on the identified security threats, and security requirements and security countermeasures are specified. This security reference architecture can guide the developer to design a SDN security functional architecture and implement security functions when developing an SDN controller.

Recommendation ITU-T X.1038

Security requirements and reference architecture for software-defined networking

1 Scope

This Recommendation is to support security protection and to provide security requirements and a reference architecture for software-defined networking (SDN). This Recommendation:

- describes use cases to detail new security threats when introducing SDN;
- identifies major security threats to SDN;
- defines security requirements;
- provides possible security countermeasures against new security threats;
- designs a security reference architecture for SDN.

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 Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*.
- [IETF RFC 4210] IETF RFC 4210 (2005), *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*.
- [IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.
- [IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.
- [IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*.
- [IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.
- [IETF RFC 4314] IETF RFC 4314 (2005), *IMAP4 Access Control List (ACL) Extension*.
- [IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.
- [IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.
- [NIST 3DES] National Institute of Standards and Technology (2012), *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher* (Revision 1), NIST Special Publication 800-67, January.

- [NIST AES] National Institute of Standards and Technology (2001), *Specification for the Advanced Encryption Standard (AES)* FIPS 197. November 26.
- [NIST DSS] NIST FIPS PUB 186-4 (2013), *Digital Signature Standard*, National Institute of Standards and Technology, U.S. Department of Commerce, July.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 access control [ITU-T X.800]: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.1.2 authentication [b-ISO/IEC 18014-2]: Provision of assurance in the identity of an entity.

3.1.3 authorization [b-ITU-T X.1251]: The authorization service is designed to make decisions regarding the user's access rights and enforce authorization decisions according to the user's privileges. Authorization is an optional service; it is only provided when access to resources needs to be controlled based on the user's rights.

3.1.4 confidentiality [ITU-T X.800]: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

3.1.5 data integrity [ITU-T X.800]: The property that data has not been altered or destroyed in an unauthorized manner.

3.1.6 firewall [b-ISO/IEC 27033-1]: Type of security barrier placed between network environments – consisting of a dedicated device or a composite of several components and techniques – through which all traffic from one network environment traverses to another, and vice versa, and only authorized traffic, as defined by the local security policy, is allowed to pass.

3.1.7 intrusion detection system [b-ISO/IEC 27039]: Information systems used to identify that an intrusion has been attempted, is occurring, or has occurred.

3.1.8 key [ITU-T X.800]: A sequence of symbols that controls the operations of encipherment and decipherment.

3.1.9 key management [ITU-T X.800]: The generation, storage, distribution, deletion, archiving and application of keys in accordance with a security policy.

3.1.10 public-key certificate (PKC) [b-ITU-T X.509]: The public key of an entity, together with some other information, rendered unforgeable by digital signature with the private key of the certification authority (CA) that issued it.

3.1.11 software-defined networking [ITU-T Y.3300]: A set of techniques that enables to directly program, orchestrate, control and manage network resources, which facilitates the design, delivery and operation of network services in a dynamic and scalable manner.

3.1.12 threat [b-ISO/IEC 27000]: Potential cause of an unwanted incident, which may result in harm to a system or organization.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 network resources: Network devices that can perform packet forwarding in a network system. The network resources include network switch, router, gateway, WiFi access points, and similar devices.

3.2.2 certificate management: The creation, storage, distribution, suspension, revocation, archiving and application of certificates in accordance with a security policy.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

3DES	Triple Data Encryption Algorithm
ACL	Access Control List
AES	Advanced Encryption Standard
DDoS	Distributed Denial of Service
DoS	Denial of Service
DPI	Deep Packet Inspection
HMAC	keyed-Hash Message Authentication Code
ICT	Information and Communications Technology
IDP	Intrusion Detection and Prevention
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
MAC	Message Authentication Code
ONF	Open Networking Foundation
OS	Operating System
PSK	Pre-Shared Key
QoS	Quality of Service
RBAC	Role Based Access Control
SDN	Software-Defined Networking
SLA	Service Level Agreement
TLS	Transport Layer Security

5 Conventions

In this Recommendation:

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

The keywords "**can optionally**" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with the specification.

6 Overview

Software-defined networking (SDN) enables the administrators to configure network resources very quickly and to adjust network-wide traffic flow to meet changing needs dynamically. SDN controllers serve as a type of operating system for network. By separating the control plane from the network hardware and running the control plane instead as software, the controller facilitates automated network management, as well as integration and administration of applications and network services. However, there are some challenges for implementing a full-scale carrier SDN. One of the most important challenges is SDN security.

Generally, security threats to SDN are common to other targets and to traditional networking, but the profile of the threats (including their likelihood and impact and hence their overall risk level) changes with the new SDN architecture. With a centralized SDN controller, the impact of a DoS/DDoS attack can be higher than that directed against a single router. Some new functional entities (e.g., SDN controller), protocols (e.g., ONF OpenFlow) and interfaces (e.g., application-control interface, resource-control interface) according to the framework of SDN [ITU-T Y.3300] will pose new security threats. All these security threats must be understood and secured.

This Recommendation describes use cases to detail new security threats when introducing SDN. This Recommendation identifies security threats for the SDN application layer, SDN control layer, SDN resource layer, application-control interface, and resource-control interface according to the framework of SDN [ITU-T Y.3300]. This Recommendation also defines security requirements from above security threats analysis and studies possible security countermeasures against new security threats. With this information, a security reference architecture for SDN is designed based on above studies on security threats, security requirements and security countermeasures. This security reference architecture can guide the developer to design a SDN security functional architecture and implement security functions when developing an SDN controller.

7 Security threats and requirements

This clause identifies security threats for the SDN application layer, SDN control layer, resource layer, application-control interface and resource-control interface, and defines corresponding security requirements.

7.1 SDN application layer

SDN applications can be seen as the "SDN network brains", since they implement a majority of network functionalities which will be translated into flow rules to be installed in SDN resource layer and to dictate the behaviour of the forwarding devices. So, attacks on SDN applications if not stopped early enough, can impact the SDN control layer.

7.1.1 Security threats

Major security threats to SDN application layer are described as below:

- **Spoofing:** An attacker masquerades as a SDN controller to get the service level agreement (SLA) or users' data (e.g., user identification, credentials) or service logic and use it for the future attack.
- **Repudiation:** A user or an administrator, enforcing a malicious network policy (e.g., copying and forwarding specific traffic flows to a malicious server), may claim that he/she did not make such network policy enforcement.
- **Information disclosure:** It is possible for attackers to get user's credentials and then to masquerade as a legitimate user to inject forged flows into network through SDN application.
- **Application security vulnerabilities:** SDN applications vulnerabilities such as code flaws and insecure code could be exploited by the attacker to access resources (e.g., SLA, users' data, service logic) possessed by SDN applications to make further attacks, for example,