International Telecommunication Union

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

International
Telecommunication
Union

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/.

Table of Contents

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, misusing SDN network resources or reconfiguring the whole SDN network. Malicious applications or untrusted applications from the third party could masquerade as legal SDN applications to access application resources.

7.1.2 Security requirements

R-01 It is required to provide a functionality in the SDN application layer to authenticate the SDN controller.

R-02 It is required to provide a functionality in the SDN application layer to authenticate the user.

R-03 It is required to provide a functionality in the SDN application layer to authenticate the administrator.

R-04 It is required to provide a functionality in the SDN application layer to authorize the user to access system information (e.g., SLA, users' data, service logic, etc.).

R-05 It is required to provide a functionality in the SDN application layer to authorize the administrator to access system information.

R-06 It is required to provide a functionality in the SDN application layer to provide confidentiality protection for system information stored in the application platform.

R-07 It is required to provide a functionality in the SDN application layer to support key/certificate management.

R-08 It is required to provide a functionality in the SDN application layer to support log and audit.

R-09 It is recommended to provide a functionality in the SDN application layer to support defending against application vulnerabilities.

7.1.3 Security requirements mapping to security threats

As for the SDN application layer, security requirements deriving from the corresponding security threats are shown in Table 1.

Table 1 – SDN application layer: security requirements mapping to security threats

Security threats	Security requirements
Spoofing	R-01, R-02, R-03, R-04, R-05
Repudiation	R-01, R-02, R-03, R-07, R-08
Information disclosure	R-02, R-04, R-06
Application security vulnerability	R-09

7.2 SDN control layer

Securing the SDN controller is the top priority, since a compromise of the SDN controller will lead to the disaster of the entire network.

7.2.1 Security threats

Major security threats to the SDN control layer are described as follows:

– **Flow rules confliction**: An example of flow rules confliction is described in use case 1 of Annex A. It explains how malicious flows could bypass security detection, which conflicts with the preconfigured security policy and will adversely affect the SDN controller.

– **Fake flow rule insertion**: An attacker may hijack a SDN application and send some fraudulent flow rules to eavesdrop data. An example is elaborated in use case 2 of Annex A.

– **Spoofing**: An attacker may impersonate an administrator or a SDN application to remove or modify sensitive data (e.g., configuration data, user data) from the SDN controller or to obtain network topology information and routing information or even to have complete control of the SDN controller. By spoofing the address of a SDN controller, an attacker can take the control of the entire network by creating a fake SDN controller. Moreover, an attacker may create a fake SDN switch to perform network reconnaissance by observing how the controller responds to different packets which are generated by the fake SDN switch.

- **DoS attacks**: When a SDN switch encounters traffic for which it has no flow rule, it consults the SDN controller for a decision and a flow rule for future traffic of the same type. Therefore, it is possible for an attacker to create spoofed traffic to make DoS attacks on the SDN controller to cause it to fail. A spoofed SDN switch also could create DoS attacks on the SDN controller with unmanageable traffic to bog it down.
- **Delay in blocking/mitigating attacks**: Generally network policies are converted into flow entries to be sent to SDN switches in batches periodically in order to improve system performance. Currently, the SDN controller does not support blocking/mitigating attacks in real time and the SDN controller does not automatically identify which security policies have to be operated without any delay. Therefore, security attacks will last longer and will be more severe.
- **Repudiation**: An administrator or a SDN application, inserting malicious flow rules into the flow table to make inside attacks, may claim that he/she did not insert such malicious flow rules into the flow table.
- **Information disclosure**: It is possible for attackers to get sensitive system information (e.g., configuration data, user credentials) for a future attack.
- **Vulnerabilities in the operating system**: SDN controllers run on some form of operating systems (OS). If the SDN controller runs on a general purpose operating system, then the vulnerabilities of that OS become vulnerabilities for the SDN controller. An attacker may exploit vulnerabilities of the operating system such as default passwords, back-door accounts, open doors (e.g., open ports, services, and protocols), and even no security settings configured to destruct or alternate components of the OS or the complete OS, which will impact the SDN controller seriously.
- **Vulnerabilities in software**: SDN controllers operate as a software platform. Vulnerabilities of general software become vulnerabilities for the SDN controller. A software vulnerability is a flaw, defect in software construction, weakness or even an error, which could be exploited by attackers to alter the normal behaviour of the SDN network or to reconfigure the whole network to make further attacks.
- **Hardware failure**: Hardware failure, nothing new with information and communications technology (ICT), is a security threat representing the generic failure of hardware in SDN network elements (including controller and switch). Hardware failures will compromise network security or bring down the SDN network.

7.2.2 Security requirements

R-10 It is required to provide a functionality in the SDN control layer to authenticate administrators.

R-11 It is required to provide a functionality in the SDN control layer to authorize administrators to manage the SDN controller.

R-12 It is required to provide a functionality in the SDN control layer to authenticate the SDN application.

R-13 It is required to provide a functionality in the SDN control layer to authorize the SDN application to manage network policies in the SDN controller (e.g., to insert/update/delete flow rules in the flow table).

R-14 It is required to provide a functionality in the SDN control layer to authenticate the SDN switch.

R-15 It is required to provide a functionality in the SDN control layer to support preventing flow rules confliction in order to avoid mandatory network policies from being bypassed.

R-16 It is required to provide a functionality in the SDN control layer to support anti-DoS protection.

R-17 It is required to provide a functionality in the SDN control layer to support log and audit.

R-18 It is required to provide a functionality in the SDN control layer to perform integrity protection for configuration data stored in the SDN controller.

R-19 It is required to provide a functionality in the SDN controller layer to perform key/certificate management.

R-20 It is recommended to provide a functionality in the SDN control layer to automatically block or mitigate security attacks in real time.

R-21 It is recommended to provide a functionality in the SDN control layer to support packet scan detection.

R-22 It is recommended to provide a functionality in the SDN control layer to perform confidentiality protection for configuration data stored in the SDN controller.

R-23 It is recommended to provide a functionality in the SDN control layer to perform confidentiality and/or integrity protection for user data stored in the SDN controller.

R-24 It is recommended to provide a functionality in the SDN control layer to support hardening the operating system.

R-25 It is recommended to provide a functionality in the SDN control layer to support software vulnerability detection and prevention.

R-26 It is recommended to provide a functionality in the SDN control layer to support hardware management to discover hardware failure automatically and recover from such a failure as soon as possible.

7.2.3 Security requirements mapping to security threats

As for the SDN control layer, security requirements deriving from the corresponding security threats are shown in Table 2.

Table 2 – SDN control layer: security requirements mapping to security threats

Security threats	Security requirements
Flow rules confliction	R-15
Fake flow rule insertion	R-12, R-13, R-19, R-35
Spoofing	R-10, R-11, R-12, R-13, R-14, R-19
DoS attacks	R-14, R-16, R-19
Delay in blocking/mitigating attacks	R-20, R-21, R-33
Repudiation	R-10, R-11, R-12, R-13, R-17, R-19
Information disclosure	R-10, R-11, R-18, R-19, R-22, R-23
Vulnerabilities in operating system	R-24
Vulnerabilities in software	R-25
Hardware Failure	R-26

7.3 SDN resource layer

7.3.1 Security threats

Major security threats to the SDN resource layer are described as follows:

– **Spoofing**: An attacker may impersonate an administrator or a SDN controller to remove or modify sensitive data (e.g., configuration data, flow table) from the SDN switch or to obtain sensitive information such as flow entries in the flow table.

– **Eavesdropping**: An attacker may eavesdrop on flows between SDN switches to see what flows are in use, what traffic is being permitted across the network and what data contents are being transported.

– **Information disclosure**: It is possible for attackers to get sensitive system information (e.g., flow table, configuration data) for a future attack.

– **Flow table overflow**: Typical SDN switches have rather limited flow table capacities. The flow table capacity bottleneck leads to potential flow table overflow. Therefore, it is possible for the attacker to overwrite legitimate flow rules as flow entries of the flow table, or to make DoS and flooding attacks, or even to do inference attack [b-arXiv 2015].

– **Repudiation**: An administrator or a SDN controller may make incorrect configuration and later claim that he/she did not do such attacks.

7.3.2 Security requirements

R-27 It is required to provide a functionality in the SDN resource layer to authenticate administrators.

R-28 It is required to provide a functionality in the SDN resource layer to authorize administrators to manage SDN switches.

R-29 It is required to provide a functionality in the SDN resource layer to authenticate the SDN controller.

R-30 It is required to provide a functionality in the SDN resource layer to support log and audit.

R-31 It is required to provide a functionality in the SDN resource layer to perform integrity protection for configuration data stored in the SDN switch.

R-32 It is required to provide a functionality in the SDN resource layer to perform key/certificate management.

R-33 It is required to provide a functionality in the SDN resource layer to support packet scan detection, which is derived from the requirements R-20 and R-21 in clause 7.2.2, in order to automatically block or mitigate security attacks in real time. .

R-34 It is recommended to provide a functionality in the SDN resource layer to perform confidentiality protection for configuration data stored in the SDN switch.

R-35 It is recommended to provide a functionality in the SDN resource layer to perform confidentiality and/or integrity protection for data transportation between SDN switches.

R-36 It is recommended to provide a functionality in the SDN resource layer to prevent flow table overflow.

7.3.3 Security requirements mapping to security threats

As for the SDN resource layer, security requirements deriving from the corresponding security threats are shown in Table 3.

Table 3 – SDN resource layer: security requirements mapping to security threats

Security threats	Security requirements
Spoofing	R-27, R-28, R-29, R-32
Eavesdropping	R-35
Information disclosure	R-31, R-32, R-34
Flow table overflow	R-36
Repudiation	R-27, R-28, R-29, R-30, R-31, R-32

7.4 Application-control interface

7.4.1 Security threats

Major security threats to the application-control interface are described below:

– **Eavesdropping**: An attacker can use information gathered through eavesdropping of messages to deduce network policies and to use them to elevate the attack.

– **Tampering and intercepting**: An attacker may intercept and tamper the messages between a SDN controller and an application. If successful, the attacker could potentially subvert the SDN controller and inject his/her own network policies which would have the authority of the SDN application and thus would direct network traffic to be transported in the way as he/she wants.

7.4.2 Security requirements

R-01 It is required to provide a functionality in the SDN application layer to authenticate the SDN controller.

R-07 It is required to provide a functionality in the SDN application layer to perform key/certificate management.

R-12 It is required to provide a functionality in the SDN control layer to authenticate the SDN application.

R-19 It is required to provide a functionality in the SDN controller layer to perform key/certificate management.

R-37 It is required to provide a functionality in the SDN control layer to perform confidentiality protection for data transportation over the application-control interface.

R-38 It is required to provide a functionality in the SDN control layer to perform integrity protection for data transportation over the application-control interface.

R-39 It is required to provide a functionality in the SDN application layer to perform confidentiality protection for data transportation over the application-control interface.

R-40 It is required to provide a functionality in the SDN application layer to perform integrity protection for data transportation over the application-control interface.

R-41 It is recommended to support TLS [IETF RFC 5246] or HTTPS [b-IETF RFC 2818] for data transportation between the SDN application and the SDN controller over the application-control interface.

7.4.3 Security requirements mapping to security threats

As for the SDN application-control interface, security requirements deriving from the corresponding security threats are shown in Table 4.

**Table 4 – SDN application-control interface:
security requirements mapping to security threats**

Security threats	Security requirements
Eavesdropping	R-01, R-12, R-07, R-19, R-37, R-39, R-41
Tampering and intercepting	R-01, R-12, R-07, R-19, R-38, R-40, R-41

7.5 Resource-control interface

7.5.1 Security threats

Major threats to the resource-control interface are described as follows:

– **Eavesdropping**: An attacker can use information gathered through eavesdropping of control messages to map out the network routing policies and to use this to elevate the attack.

– **Tampering and intercepting**: An attacker may intercept and tamper messages between the SDN controller and switches. If successful, the attacker could potentially subvert the SDN controller and inject his/her own control messages which would have the authority of the SDN controller and thus would allow complete control of SDN switches within its scope.

7.5.2 Security requirements

R-14 It is required to provide a functionality in the SDN control layer to authenticate the SDN switch.

R-19 It is required to provide a functionality in the SDN controller layer to perform key/certificate management.

R-29 It is required to provide a functionality in the SDN resource layer to authenticate the SDN controller.

R-32 It is required to provide a functionality in the SDN resource layer to perform key/certificate management.

R-42 It is required to provide a functionality in the SDN control layer to perform confidentiality protection for data transportation over the resource-control interface.

R-43 It is required to provide a functionality in the SDN control layer to perform integrity protection for data transportation over the resource-control interface.

R-44 It is required to provide a functionality in the SDN resource layer to perform confidentiality protection for data transportation over the resource-control interface.

R-45 It is required to provide a functionality in SDN resource layer to perform integrity protection for data transportation over the resource-control interface.

R-46 It is recommended to support TLS [IETF RFC 5246] or IPsec ([IETF RFC 4301], [IETF RFC 4303], [IETF RFC 4835]) for data transportation between the SDN controller and SDN switches over the resource-control interface.

7.5.3 Security requirements mapping to security threats

As for the SDN resource-control interface, security requirements deriving from the corresponding security threats are shown in Table 5.

Table 5 – SDN Resource-Control interface: security requirements mapping to security threats

Security Threats	Security Requirements
Eavesdropping	R-14, R-19, R-29, R-32, R-42, R-44, R-46
Tampering and intercepting	R-14, R-19, R-29, R-32, R-43, R-45, R-46

8 Security reference architecture for SDN

This clause specifies a security reference architecture to guide the developers to design a SDN security functional architecture and implement security functions when developing the SDN controller.

The security reference architecture described in this Recommendation (see Figure 8-1) is based on the high-level architecture of SDN provided in [ITU-T Y.3300].

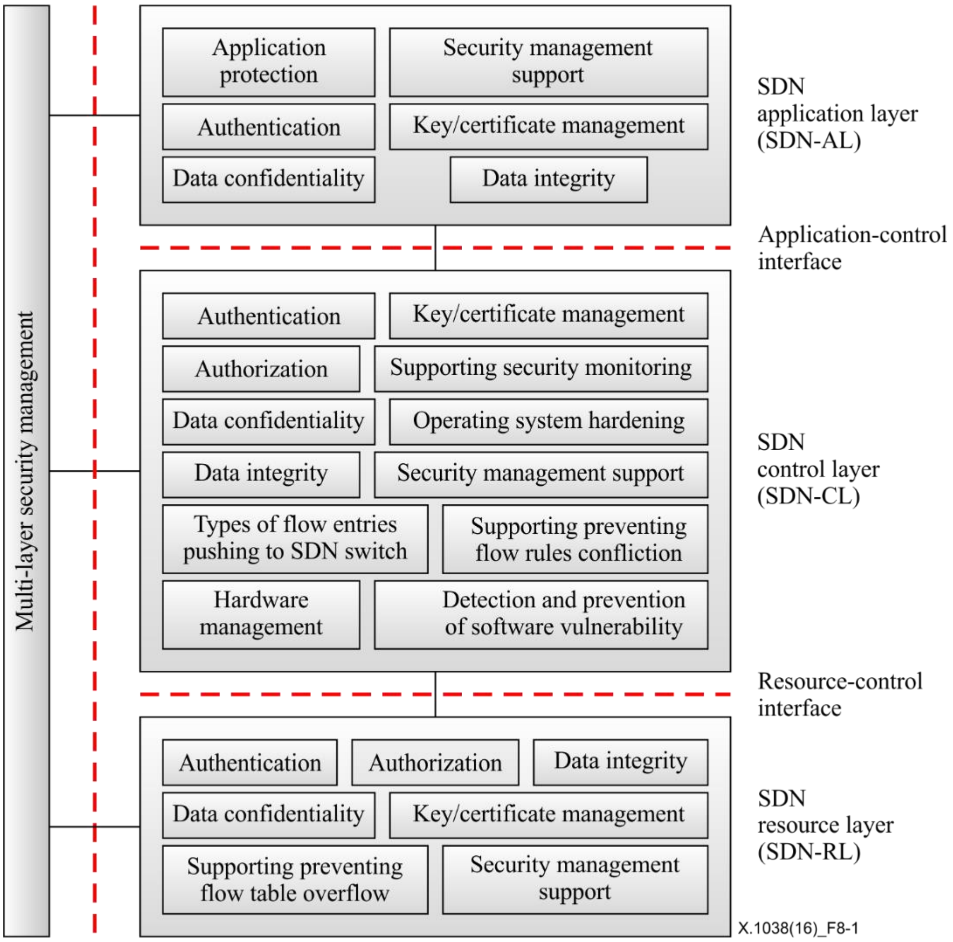
Multi-layer security management
Application protection
Security management support
Authentication
Key/certificate management
Data confidentiality
Data integrity
SDN application layer (SDN-AL)
Application-control interface
Authentication
Key/certificate management
Authorization
Supporting security monitoring
Data confidentiality
Operating system hardening
Data integrity
Security management support
Types of flow entries pushing to SDN switch
Supporting preventing flow rules confliction
Hardware management
Detection and prevention of software vulnerability
SDN control layer (SDN-CL)
Resource-control interface
Authentication
Authorization
Data integrity
Data confidentiality
Key/certificate management
Supporting preventing flow table overflow
Security management support
SDN resource layer (SDN-RL)
X.1038(16)_F8-1

Figure 8-1 – Security reference architecture for SDN

8.1 SDN application layer

Table 6 provides security mechanisms to meet corresponding security requirements on the SDN application layer.

Table 6 – SDN application layer: security mechanisms to meet security requirements

Security requirements	Security mechanisms
R01/R02/R03 – to authenticate the SDN controller/ the user/the administrator	authentication
R04/R05 – to authorize the user/administrator to access system information	authorization
R06/R39 – to provide confidentiality protection for system information stored in application platform/to perform confidentiality protection for data transportation over the Application-Control interface	data confidentiality
R07 – to support key/certificate management	key/certificate management

Table 6 – SDN application layer: security mechanisms to meet security requirements

Security requirements	Security mechanisms
R08 – to support log and audit	security management
R09 – support defending against application vulnerabilities	application protection
R40 – to perform integrity protection for data transportation over the application-control interface	data integrity

According to Figure 8-1 and Table 6, security logical functions for the SDN application layer are described as follows:

- Authentication

  The SDN application shall authenticate the SDN controller to make sure that the SDN controller is authentic, but not a fake one.

  There are some available authentication mechanisms including, but are not limited to, pre-shared key (PSK) based authentication [IETF RFC 4279] [IETF RFC 4306], and certificate based authentication [IETF RFC 4306] [IETF RFC 5246].

- Data confidentiality

  Network policies (including security policies and quality-of-service (QoS) policies) shall be encrypted before being transported from the SDN applications to the SDN controller over the application-control interface in order to avoid eavesdropping attacks.

  Some available cryptographic algorithms used for data encryption include, but are not limited to, advanced encryption standard (AES) [AES], Blowfish [b-BLOWFISH], and triple data encryption algorithm (3DES) [b-NIST 3DES].

- Data integrity

  Data integrity protection shall be provided for network policies (including security policies and QoS policies) while being transported from SDN applications to the SDN controller over the application-control interface in order to avoid tampering attacks.

  There are some available data integrity mechanisms including, but are not limited to, message authentication code (MAC) [b-IETF RFC 2104], keyed-hash message authentication code (HMAC) [b-IETF RFC 2104], and digital signature [DSS].

- Key/certificate management

  Key/certificate management shall refer to key management defined in [ITU-T X.800] and certificate management protocol defined in [IETF RFC 4210].

- Application protection

  Attack detection tools (e.g., intrusion detection systems, application firewalls) should be applied in the SDN application layer to protect applications at runtime. Attack detection tools use approaches based on either anomaly detection or signatures [b-PRDC2009]. Anomaly-detection-based tools are based on a baseline for network behaviour to detect any behaviour that fall outside the predefined or accepted model of behaviour. Signature-based tools look for patterns of a predefined set of rules or signatures indicating an attack. Anomaly-detection-based tools perform better for simpler applications, while signature-based tools are better for more complex applications.

  Before installing an application, real-time verification shall be provided that the application certification is current and valid in order to make sure that this application is from trusted third party.

- Security management support

  Security management support shall be provided to the support for the function multi-layer security management which is described in clause 8.4.

8.2 SDN control layer

Table 7 provides security mechanisms to meet corresponding security requirements for the SDN control layer.

Table 7 – SDN control layer: security mechanisms to meet security requirements

Security requirements	Security mechanisms
R10/R12/R14 – to authenticate administrators/SDN application/SDN switch	authentication
R11/R13 – to authorize administrators/SDN application to manage the SDN controller	authorization
R15 – to support prevent flow rules confliction	preventing flow rules confliction
R16 – to support anti-DoS protection	authentication, security management
R17 – to support log and audit	security management
R18/R23/R38/R43 – to perform integrity protection for configuration data stored in the SDN controller/ to perform integrity protection for user data stored in the SDN controller/ to perform integrity protection for data transportation over the application-control interface/ to perform integrity protection for data transportation over the resource-control interface	data integrity
R19 – to perform key/certificate management	key/certificate management
R20 – to block or mitigate security attacks in real time and automatically	types of flow entries being pushed to SDN switches
R21 – to support packet scan detection	supporting security monitoring
R22/R23/R37/R42 – to perform confidentiality protection for configuration data stored in the SDN controller/to perform confidentiality protection for user data stored in the SDN controller/ to perform confidentiality protection for data transportation over the application-control interface/to perform confidentiality protection for data transportation over the resource-Control interface	data confidentiality
R24 – to support hardening operating system	operating system hardening
R25 – to support software vulnerability detection and prevention	detection and prevention of software vulnerability
R26 – to support hardware management to discover hardware failure automatically and recover from such a failure as soon as possible	hardware management

According to Figure 8-1 and Table 7, security logical functions for the SDN control layer are described as follows:

- Authentication

  The SDN controller shall authenticate the SDN application to make sure that the SDN application is authentic, but not a fake one.

  The SDN controller shall authenticate the SDN switch to make sure that the SDN switch is authentic, but not a fake one.

The SDN controller shall authenticate administrators to make sure that these administrators are authentic.

There are some available authentication mechanisms including, but are not limited to, username/password based authentication, PSK (pre-shared key) based authentication [IETF RFC 4279] [IETF RFC 4306], and certificate based authentication [IETF RFC 4306] [IETF RFC 5246].

- Authorization

  SDN applications and administrators access to the SDN controller shall comply with access control policies.

  Some available access control mechanisms include, but are not limited to, whitelist/blacklist [b-IETF RFC 5782] [b-IETF RFC 5851], access control list (ACL) [IETF RFC 4314] [b-IETF RFC 4949], role based access control (RBAC) [b-INCITS RBAC].

- Data confidentiality

  Network policies (including security policies and QoS policies) from the SDN application layer shall be decrypted by the SDN controller before being interpreted as flow rules.

  Flow rules/entries shall be encrypted before being transported from the SDN controller to SDN switches over the resource-control interface in order to avoid eavesdropping attacks.

  Flow rule inquiries from the SDN switches shall be decrypted by the SDN controller before the SDN controller looks for corresponding flow rules.

  Configuration data from the SDN management console shall be decrypted by the SDN controller before being updated into corresponding configuration component in the SDN controller.

  Some sensitive data (e.g., configuration data, user data) shall be encrypted and stored in the SDN controller to prevent data theft.

  Some available cryptographic algorithms used for data encryption include, but are not limited to, AES [AES], Blowfish [b-BLOWFISH], and 3DES [b-NIST 3DES].

- Data integrity

  Data integrity validation for network policies (including security policies and QoS policies) from SDN applications shall be operated by the SDN controller before being interpreted as flow rules.

  Data integrity protection shall be provided for flow rules/entries while being transported from the SDN controller to the SDN switches over the resource-control interface in order to avoid tampering attacks.

  Data integrity validation for flow rule inquiries from SDN switches shall be operated by the SDN controller before the SDN controller looks for corresponding flow rules.

  Data integrity validation for some configuration data from the SDN management console shall be operated by the SDN controller before being updated into corresponding configuration component in the SDN controller.

  Data integrity protection shall be provided for some sensitive data (e.g., configuration data, user data) while storing in the SDN controller to prevent them from tampering.

  There are some available data integrity mechanisms including, but are not limited to, MAC (Message authentication code) [b-IETF RFC 2104], HMAC [b-IETF RFC 2104], and digital signature [DSS].

- Key/certificate management

  Key/certificate management shall refer to key management defined in [ITU-T X.800] and certificate management protocol defined in [IETF RFC 4210].

- Types of flow entries being pushed to SDN switches

  There are two types of flow entries being pushed to SDN switches: real-time push and periodic push.

  Some flow rules/entries are used to block or mitigate security attacks which are detected by security applications (e.g., firewall, deep packet inspection (DPI), and intrusion detection and prevention (IDP)). Those flow entries have to be pushed to SDN switches in real time.

  Some flow rules/entries can be operated with some delay. Those flow entries shall be pushed to SDN switches in batches periodically in order to improve system performance.

  One suitable solution is to add a new attribute to a flow rule in order to indicate the flow entry to be pushed to SDN switches in real time or sometime later [b-ICIN2015 SDNSEC]. With that attribute, the SDN controller could distinguish the flow entries need to be pushed to SDN switches in real time from those flow entries need to be pushed to SDN switches periodically.

- Preventing flow rules confliction

  Currently, the SDN controller cannot distinguish the application generating the new flow entry from another application generating the old entry. So, it is possible for an application to create a new flow entry to replace the flow entry which reflects a mandatory policy predefined by a security administrator. One of the use cases is described in clause A.1. Therefore, the SDN controller should have the ability to judge if an application has the right to insert/update/delete the flow entry in the flow table in order to avoid flow rules conflicting.

  One of suitable solutions is to support fine-grained naming scheme for flow entry [b-ICIN2015 SDNSEC], which is described in clause B.1.

- Supporting security monitoring

  The module of supporting security monitoring is to enable administrators to monitor the entire SDN network, especially on security policies enforcement. For example, a security administrator wants to know the details regarding a security policy for a specified data flow and sends a request to the supporting security monitoring module. This module retrieves related information (e.g., flow entries, flow entries generators, security policies, etc.) from flow tables, then analyses the retrieved information, generates a report and displays the report to the security administrator.

- Operating system hardening

  The purpose of operating system hardening is to eliminate as many security risks as possible and to make an operating system more secure. It often requires numerous actions such as configuring system and network components properly, deleting unused files, removing all non-essential software programs, applying the latest patches, reformatting the hard disk and only installing the bare necessities that the server needs to function, disabling guest account, and renaming the administrator account.

- Detection and prevention of software vulnerability

  In order to understand and prevent vulnerabilities, software vulnerability detection should be performed first. There are two main categories of automated methods for software vulnerability detection: static detection (e.g., pattern matching and data flow analysis) which is performed without running the source code; and dynamic detection (e.g., fault injection, fuzzing testing) which is performed when the program is executed. Usually, a hybrid combination of both techniques is used.

  Two possible vulnerability prevention methods developed in the literature are software inspection (e.g., security goal indicator trees [b-HASE2008] and vulnerability inspection diagram [b-SHIELDS]) and security activity graph [b-ICSE2006],[b-ARES2008].

- Hardware management

  The hardware management system against hardware failures arisen from the SDN network shall be based on a management model constructed as a relational database to visually manage network elements and their correlative relationships [b-IFIP2015 IM]. With a hardware management system, a hardware failure can be detected timely and network elements affected can be specified. Therefore, the network administrator can work on recovery operations faster and earlier and enhance availability of the network.

- Security management support

  Security management support shall provide the support for the function multi-layer security management which is described in clause 8.4.

8.3 SDN resource layer

Table 8 provides security mechanisms to meet corresponding security requirements for the SDN application layer.

Table 8 – SDN resource layer: security mechanisms to meet security requirements

Security requirements	Security mechanisms
R27/29 – to authenticate administrators/SDN controller	authentication
R28 – to authorize administrators to manage SDN switches	authorization
R30 – to support log and audit	security management
R31/R35/R45 – to perform integrity protection for configuration data stored in the SDN switch/ to perform integrity protection for data transportation between SDN switches/ to perform integrity protection for data transportation over the resource-control interface	data integrity
R32 – to perform key/certificate management	key/certificate management
R34/R35/R44 – to perform confidentiality protection for configuration data stored in the SDN switch/ to perform confidentiality protection for data transportation between SDN switches/ to perform confidentiality protection for data transportation over the resource-control interface	data confidentiality
R36 – to prevent flow table overflow	preventing flow table overflow

According to Figure 8-1 and Table 8, security logical functions for the SDN resource layer are described as follows:

- Authentication

  The SDN switch shall authenticate the SDN controller to make sure that the SDN controller is authentic, but not a fake one.

  The SDN switch shall authenticate administrators to make sure that these administrators are authentic.

  There are some available authentication mechanisms including, but are not limited to, username/password based authentication, PSK (pre-shared key) based authentication [IETF RFC 4279] [IETF RFC 4306], and certificate based authentication [IETF RFC 4306] [IETF RFC 5246].

- Authorization

  The SDN controller and administrators access to the SDN switch shall comply with access control policies.

Some available access control mechanisms include, but are not limited to, whitelist/blacklist [b-IETF RFC 5782] [b-IETF RFC 5851], access control list (ACL) [IETF RFC 4314] [b-IETF RFC 4949], role based access control (RBAC) [b-INCITS RBAC].

- Data confidentiality

  Flow rules/entries from the SDN controller shall be decrypted by SDN switches before being updated into flow table.

  Flow rule inquiries shall be encrypted before being transported from SDN switches to the SDN controller over resource-control interface in order to avoid eavesdropping attacks.

  Configuration data from the SDN management console shall be decrypted by SDN switches before being updated into corresponding configuration component in SDN switches.

  Some sensitive data (e.g., configuration data, user data) shall be encrypted and stored in SDN switches to prevent data theft.

  Some available cryptographic algorithms used for data encryption include, but are not limited to, AES [AES], Blowfish [b-BLOWFISH], and 3DES [b-NIST 3DES].

- Data integrity

  Data integrity validation for flow rules/entries from the SDN controller shall be operated by SDN switches before being updated into flow table.

  Data integrity protection shall be provided for flow rule inquires while being transported from SDN switches to the SDN controller over resource-control interface in order to avoid tampering attacks.

  Data integrity validation for configuration data from the SDN management console shall be operated by SDN switches before being updated into corresponding configuration component in SDN switches.

  Data integrity protection shall be provided for some sensitive data (e.g., configuration data, user data) while stored in SDN switches to prevent them from tampering.

  There are some available data integrity mechanisms including, but are not limited to, MAC (Message authentication code) [b-IETF RFC 2104], HMAC [b-IETF RFC 2104], and digital signature [DSS].

- Key/certificate management

  Key/certificate management shall refer to key management defined in [ITU-T X.800] and certificate management protocol defined in [IETF RFC 4210].

- Preventing flow table overflow

  Except for some general countermeasures of buffer overflow (e.g., pointer protection, executable space protection) for preventing flow table overflow, current SDN switches and flow table designs should be improved [b-arXiv 2015]. For flow table maintenance, the SDN switch itself can decide which flow entry to delete and then sync with the SDN controller.

- Security management support

  Security management support shall provide the support for the function multi-layer security management which is described in clause 8.4.

8.4 Multi-layer security management

The logical function multi-layer security management is to provide security configuration and management for the SDN application layer, control layer and resource layer, including:

- to control access to platform-specific resources according to security policies so that the platform cannot be sabotaged (intentionally or unintentionally);

- to monitor users logging on to a platform, refusing access to those who enter inappropriate access codes, making a platform-specific minimum configuration, enforcing security policies on operating system and application system;
- to use aggregate information and statistics for the purposes of monitoring attacks on the platform.

For the application-control interface, it is recommended that TLS [IETF RFC 5246] or HTTPS [b-IETF RFC 2818] protocols are implemented and deployed in the SDN application and the SDN controller to provide mutual authentication between the SDN application and the SDN controller, as well as to provide data confidentiality and data integrity for data transportation over the application-control interface.

For the resource-control interface, it is recommended that TLS [IETF RFC 5246] or IPSec protocols ([IETF RFC 4301], [IETF RFC 4303], [IETF RFC 4835]) are implemented and deployed in the SDN controller and SDN switches to provide mutual authentication between the SDN controller and SDN switches, as well as to provide data confidentiality and data integrity for data transportation over the resource-control interface.

Annex A

Use cases of new security threats to SDN

(This annex forms an integral part of this Recommendation.)

In this annex, the following use cases are illustrated to describe new security threats when introducing SDN.

A.1 Use case 1: Bypassing a predefined mandatory policy

SDN applications are programs that explicitly, directly, and programmatically communicate their network requirements and desired network behaviour (i.e., network policies) to the SDN controller via application-controller interfaces. The controller converts these network policies into flow entries and inserts them into the flow table. However, currently a flow entry in OpenFlow flow table does not distinguish the application generating the new flow entry from another application generating the old flow entry. So, it is possible that a new network policy generated by a general application can replace a non-bypass security policy predefined by the security administrator. In Figure A.1, the security administrator proactively configures a non-bypass security policy as follows: the packets must be sent to the firewall for packet scan detection if these packets are delivered from Host A (172.0.0.1) to Host B (172.0.0.2), as data transportation path_1 in green *(the path_1: Host A -> SDN_Switch_1 -> SDN_Switch_2 -> Firewall -> SDN_Switch_3 -> Host B)*. Sometime later, the application App_X needs the shortest path for data transportation with low delay and generates the policy as follows: the shortest transportation path will be selected if these packets are delivered from Host A (172.0.0.1) to Host B (172.0.0.2), as data transportation path_2 in brown *(the path_2: Host A -> SDN_Switch_1 -> SDN_Switch_3 -> Host B)*. According to the format of the flow entry in OpenFlow flow table, the controller will replace the former non-bypass security policy with the later shortest path policy. This subverts security administrator intention and the mandatory security policy will be bypassed. Thus, it is possible that malicious flows bypass security detection and will adversely affect the SDN controller.

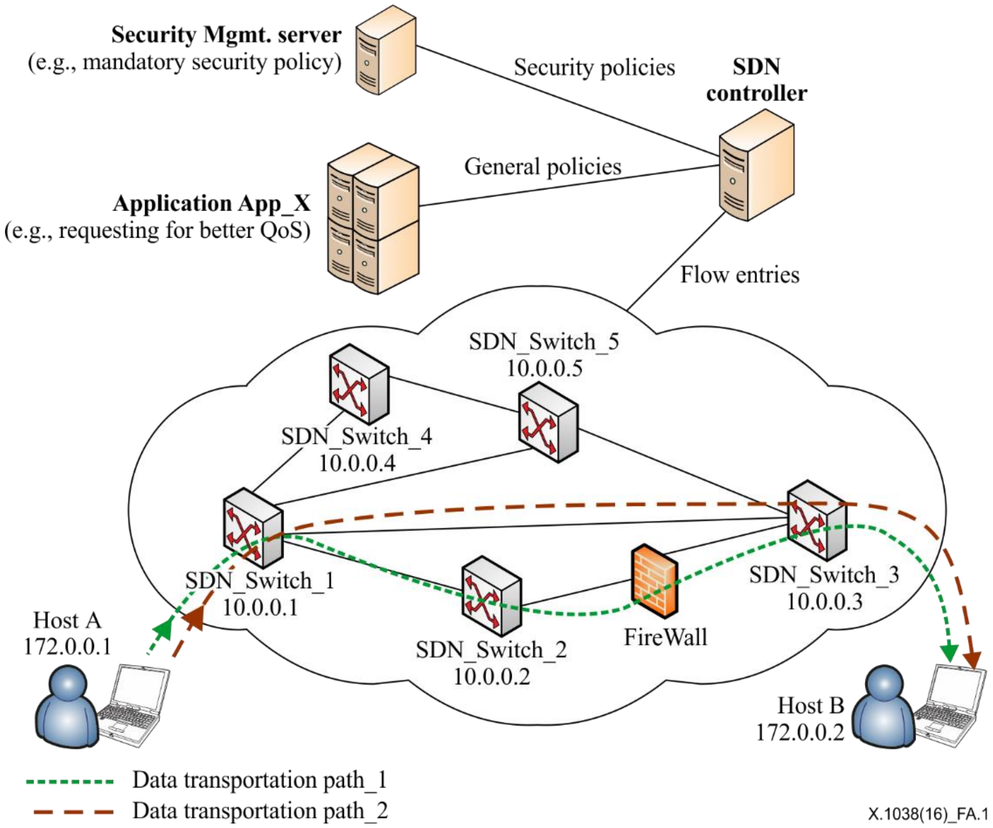

Figure A.1 – Bypassing a predefined mandatory policy

A.2 Use case 2: Data eavesdropping attacks by inserting fraudulent flow entries

An attacker may hijack a SDN application and insert fraudulent flow entries to make data eavesdropping attacks. In Figure A.2, the attacker hijacks the SDN application to generate the policy as follows: the packets are copied and forwarded to the attacker with IP address 192.0.0.10 if these packets are delivered from Host A (172.0.0.1) to Host B (172.0.0.2). This policy is converted into a flow entry then inserted into SDN_Switch_1 flow tables through the message *OFPT_Flow_MOD* from the controller. In this way, the attacker can easily intercept the packets from Host A to Host B.

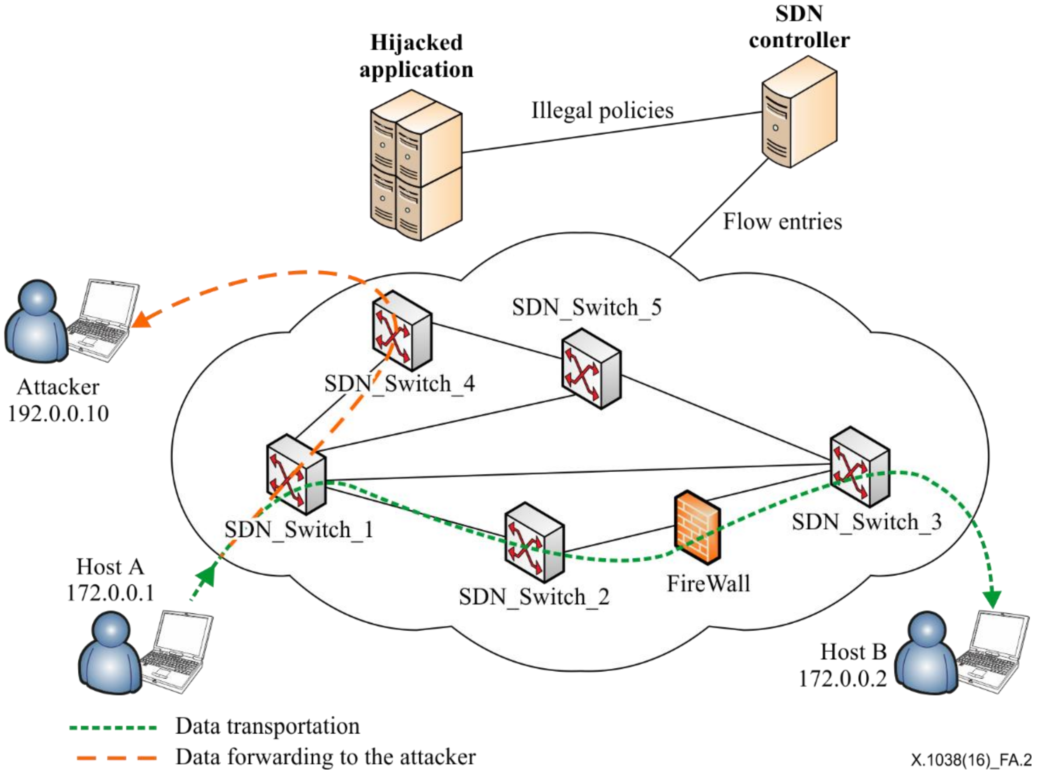

Figure A.2 – Data eavesdropping attacks by inserting fraudulent flow entries

Annex B

Fine-grained naming scheme for flow entry

(This annex forms an integral part of this Recommendation.)

In this annex, suitable security mechanisms are provided to meet new security requirements in order to prevent new security threats when introducing SDN.

B.1 Fine-grained naming scheme for flow entry

A fine-grained naming scheme for flow entry [b-ICIN2015 SDNSEC] stored in the SDN controller is proposed to avoid mandatory network policies from being bypassed.

Currently the components "match fields" and "priority" are taken together to identify a unique flow entry in the OpenFlow flow table. In this way, a flow entry in the flow table does not distinguish a SDN application generating the new flow entry from another SDN application generating the old flow entry. So, it is possible for a SDN application to create a new flow entry to replace the flow entry which reflects a mandatory policy predefined by a security administrator.

In order to design a fine-grained naming scheme for the flow entry, two new features will be added. One is the role of policy creator, the other is the level of the security privilege of the role.

The role of policy creator is used to define the role of the administrator/application that creates a given network policy. The role of creator may be a security administrator, a general administrator, a user, or a guest.

The security privilege level of the role is used to specify different security privilege levels for different roles of policy creators. Hierarchical levels from the highest to the lowest may be L5, L4, L3, L2, L1, and L0. The role with the relatively higher security privilege level is given more rights to access the SDN controller. For example, the policy created by the creator with relatively low security privilege level is replaced by the policy created by the creator with a higher level. In one illustrative embodiment, security privilege levels of roles can be set as follows: security administrator – L5 (highest); general administrator – L4; user – L2; and guest – L1. It is to be understood that, in this illustrative embodiment, there is no dedicated role for security privilege levels L3 and L0. However, the quantity and assignment of security privilege levels is open to the developer and can be instantiated based on the specific needs of the SDN network design. Overwriting policy by role level as above may not work for heterogeneous networks, since the definition of role level for those networks may be different.

With the above two new additional features to describe a flow entry defined in the SDN controller, the new flow entry can be inserted into the flow table correctly since the flow entry created by the security administrator with a high security privilege level cannot be replaced by the new flow entry created by a SDN application with a low security privilege level. In this way, mandatory network policies will not be overwritten and bypassed.

There is no impact on the resource-controller interface and flow tables of switches since these two features are stored in the controller to help the controller make decision when updating flow entries.

Bibliography

[b-ITU-T X.509] Recommendation ITU-T X.509 (2012) | ISO/IEC 9594-8:2014, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.

[b-ITU-T X.1251] Recommendation ITU-T X.1251 (2012), *A framework for user control of digital identity.*

[b-ISO/IEC 18014-2] ISO/IEC 18014-2:2009, *Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens.*

[b-ISO/IEC 27000] ISO/IEC 27000:2014, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*

[b-ISO/IEC 27039] ISO/IEC 27039:2015, *Information technology – Security techniques – Selection, deployment and operations of intrusion detection and prevention systems (IDPS).*

[b-ISO/IEC 27033-1] ISO/IEC 27033-1:2015, *Information technology – Security techniques – Network security – Part 1: Overview and concepts.*

[b-IETF RFC 2104] IETF RFC 2104 (1997), *HMAC: Keyed-Hashing for Message Authentication*. URL: www.ietf.org/rfc/rfc2104.txt

[b-IETF RFC 2818] IETF RFC 2818 (2000), *HTTP Over TLS*.

[b-IETF RFC 4949] IETF RFC 4949 (2007), *Internet Security Glossary, Version 2*.

[b-IETF RFC 5782] IETF RFC 5782 (2010), *DNS Blacklists and Whitelists*.

[b-IETF RFC 5851] IETF RFC 5851 (2010), *Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks*.

[b-ARES2008] Byers, D., Shahmehri, N. (2008), *A Cause-Based Approach to Preventing Software Vulnerabilities*. ARES, pp. 276-283, Third International Conference on Availability, Reliability and Security.

[b-arXiv 2015] Leng, J., Zhou, Y., Zhang, J., and Hu, C. (2015), *An Inference Attack Model for Flow Table Capacity and Usage: Exploiting the Vulnerability of Flow Table Overflow in Software-Defined Network,* arXiv:1504.03095.

[b-BLOWFISH] Schneier, B. (1994), *The Blowfish Encryption Algorithm*, Dr. Dobb's Journal, v. 19, n. 4, April.

[b-HASE2008] Peine, H., Jawurek, M., and Mandel, S. (2008), *Security Goal Indicator Trees: A Model of Software Features that Supports Efficient Security Inspection*. HASE, pp. 9-18, 11th IEEE High Assurance Systems Engineering Symposium.

[b-ICIN 2015 SDNSEC] Hu Z., Wang, M., Yan, X., Yin, Y. and Luo, Z. (2015), *A Comprehensive Security Architecture for SDN*, 18th International Conference on Intelligence in Next Generation Networks, IEEE, pp. 30-37.

[b-INCITS RBAC] INCITS 359-2012: *Information Technology – Role Based Access Control.*

[b-ICSE 2006] Ardi, S., Byers, D., and Shahmehri, N. (2006), *Towards a Structured Unified Process for Software Security*. In Proceedings of the ICSE 2006

	Workshop on Software Engineering for Secure Software (SESS06), Shanghai, China.
[b-IFIP 2015 IM]	Miyazawa, T., Furukawa, H., Torita, T., Sugawara, M., Kinugasa, M., Yashima, E., and Harai, H. (2015), *Management architecture against hardware failures in an optical packet and circuit integrated network*. Integrated Network Management (IM), IFIP IEEE 2015, pp. 665-671.
[b-ONF OpenFlow]	*OpenFlow Switch Specification Version 1.4.0*, Open Networking Foundation. URL: www.opennetworking.org/sdn-resources/technical-library
[b-PRDC2009]	Antunes, N. and Vieira, M. (2009), *Comparing the Effectiveness of Penetration Testing and Static Code Analysis on the Detection of SQL Injection Vulnerabilities in Web Services*, Proc. 15th IEEE Pacific Rim International Symposium on Dependable Computing (PRDC 09), IEEE CS, 2009, pp. 301-306.
[b-SHIELDS]	SHIELDS Project Consortium. D2.1 *Formalism Definitions and Representation Schemata*. SHIELDS Project Deliverable D2.1. www.cspforum.eu/D2.1_Formalism_Definitions_and_Representation_Schemata.pdf.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2017