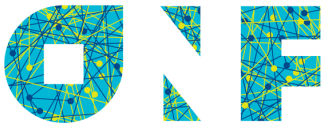

OPEN NETWORKING
FOUNDATION

Security Foundation Requirements for SDN Controllers

Version 1.0
July 2016

TR-529

ONF Document Type: Technical Recommendations
ONF Document Name: Security Foundation Requirements for SDN Controllers

Disclaimer

Open Networking Foundation
2275 E. Bayshore Road, Suite 103, Palo Alto, CA 94303
www.opennetworking.org

Table of Contents

List of Figures

1 Introduction

This document proposes a set of fundamental security requirements for SDN controllers. The SDN controller is specified in Issue 1 of the Open Networking Foundation's "SDN architecture" document [1]. The security requirements are derived from a threat analysis of the SDN controller. Microsoft's STRIDE model [2] has been used for the threat analysis, which is detailed in Section 6 of ONF's "Threat analysis for SDN architecture" [3]. Since one threat may require the proper implementation of multiple security requirements and different threats may be handled by a single security requirement, some security requirements will be merged in Chapter 4.2. All of the requirements are categorized as either general or specific in Chapter 4.3.

Note that the SDN controller is responsible for satisfaction of these requirements. However, it is neither specified nor constrained that the functionality to achieve that goal is contained exclusively within the SDN controller. In a specific instance, the requirement may be satisfied by subcontracting to an external service, e.g., an external authentication/authorization server.

The appendix to this document identifies the compliance of several publicly available SDN controllers with the security requirements in order to highlight the level of adoption of the identified security controls. Based on the evolution of security in SDN, this document—including the appendix—will be extended and/or updated to reflect additional requirements or compliance information, as required.

1.1 Common Terms, Abbreviations, and Definitions

This specification uses the terminology and acronyms defined in [1].

For the purposes of this document, the following abbreviations will be applied:

SDN	Software-defined networking
OSS	Operation support system
A-CPI	Application–control plane interface
D-CPI	Data–control plane interface
VM	Virtual machine
NE	Network entity
TLS	Transport layer security
GUI	Graphical user interface
DoS	Denial of service
API	Application programming interface

2 Critical Assets

The following diagram illustrates the SDN controller logic details as defined in [1].

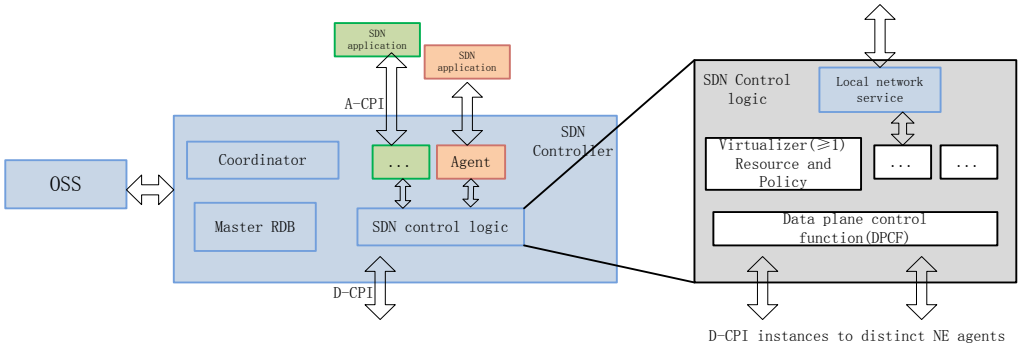

Figure 2.1: SDN Controller Logic

SDN controllers or SDN systems can be damaged or destroyed when critical assets are attacked. The critical assets of SDN controllers to be protected are:

- User account data and credentials (e.g., passwords, certificates)
- Configuration and management data (e.g., customer-specific resources and policies from OSS; the SDN controller's IP address, ports, and protocol version; etc.)
- Log data
- The operating system (OS)
- Software, including SDN controller software and application software
- The hardware (e.g., mainframe, board, power supply unit) used to run the SDN controller software, applications, etc.
- Resources (e.g., CPU processing capacity, memory processing capability, and storage processing capability)
- The interfaces of SDN controllers (e.g., A-CPI, D-CPI), including remote access interface between the SDN controller and OSS system.

3 Threats

This document does not describe the threats to SDN controllers. For an extensive discussion of that topic, see Chapter 6 of ONF's "Threat analysis for SDN architecture" [3].

4 Security Requirements

4.1 Template for Security Requirement Descriptions

Security requirement descriptions should be clear, concise, and unambiguous. Each description should include:

- *Requirement name*: A unique name assigned to each security requirement. The name indicates the topics covered by the requirement.
- *Requirement description:* A detailed description for the security requirements identified by ONF Security WG to reduce/counteract the risks outlined by the threat analysis.
- *Threat references:* A list of the related security threats.

4.2 Security Requirements Derived from Threats

The following security requirements are derived from the threat analysis of the SDN controller [3]. There may be some overlap, so convergence and categorization of all derived security requirements will be shown in Section 5.3.

4.2.1 Authentication on Interfaces of SDN Controllers

- *Requirement name*: Authentication on interfaces of SDN controllers
- *Requirement description:* Identity of all entities (e.g., switch, application, and SDN controller) that access to the SDN controller via the interfaces must be authenticated by the SDN controller. Certificate and shared keys are common methods for identity verification.
- *Threat references:* 6.1 in [3]

4.2.2 IP Check

- *Requirement name*: IP check
- *Requirement description:* The SDN controller should have capability to check the trust of source IP addresses. The SDN controller should limit the IP address list or range for:
    - Remote login access
    - Northbound access
    - Southbound equipment
    - Neighboring controllers
    - *Threat references:* 6.1 in [3]

4.2.3 User Authentication

- *Requirement name*: User authentication
- *Requirement description:* A user must use a unique identity and one or more related authentication attributes to be authenticated by the SDN controller, when the user uses system functions in the SDN controller. The authentication attributes shall be strong to prevent attacks. For example, using strong passwords as an authentication attribute can increase the workload required to perform a brute force or dictionary attack. The following password policy shall be used:
    - The minimum length of a password must be 8 characters.

- Character categories in a password include uppercase, lowercase, numeric, and special characters. At least 3 categories must be included in each password.
- A password cannot contain a user name or the reverse of a user name.
- The maximum number of times a character can be repeated in one password is configurable.
- A password must be encrypted and must not be displayed or saved in plaintext.
- The SDN controller must support password changes. Password change must be enforced after initial login or expiry. The original password and the authentication are required during a password change attempt.
- The minimum password change interval is configurable.

- *Threat references:* 6.1, 6.3 in [3]

4.2.4 Account Management

- *Requirement name*: Account management
- *Requirement description:*
  - In the SDN controller, all predefined or default accounts must be deleted or disabled. This can prevent attackers using these predefined or default accounts to log into the SDN controller.
  - Accounts must be unique, and the minimum length of an account name is configurable.
  - Accounts that are not in the validity period are locked.
  - If an operator account has not been used for a long time, it will be locked automatically.
  - Accounts that are locked by the system administrator can be unlocked only manually by the system administrator.
  - Account locking policy:
    - The period during which an account is locked because of consecutive login failures is configurable.
    - The maximum number of consecutive login failures allowed is configurable.
    - A locked account is automatically unlocked after the locking duration expires.
    - The management account and service account are independent of each other.
    - The man-machine interface account and machine-machine interface account are independent of each other.
- *Threat references:* 6.1 in [3]

4.2.5 Hardware Consistency

- *Requirement name*: Hardware consistency
- *Requirement description:* Hardware integrity and consistency must be guaranteed as controllers and switches are remotely deployed. A fake hardware device can introduce severe security risks.
- *Threat ref*erences: 6.1 in [3]

4.2.6 Hypervisor Security

- *Requirement name*: Hypervisor security
- *Requirement description:* Resource separation for controllers and applications running on virtual machines (VMs) is implemented based on separation between VMs. Once the Hypervisor is attacked, the VM separation mechanism becomes ineffective. An integrity protection mechanism based on trusted computing architecture is required to protect the Hypervisor from being attacked.
- Threat references: 6.1, 6.4, and 6.6 in [3]

4.2.7 Software Package Integrity

- *Requirement name*: Software package integrity
- *Requirement description:* SDN controllers must support integrity verification of software (e.g., SDN controller software, application software) and update packages in the installation/upgrade stage. The validation methods can be a digital signature, a strong MAC (Message Authentication Code) algorithm, etc. Tampered software must not be executed or installed if an integrity check fails.
- *Threat references:* 6.2 in [3]

4.2.8 Protecting the Integrity of Data in Transit

- *Requirement name*: Protecting the integrity of data in transit
- *Requirement description:* The integrity of the communication packets between the SDN controller and any entity (e.g., an NE, an application, or an OSS) should be protected with standard network protocols (e.g., TLS). SDN controllers must support these network protocols. For example, the OpenFlow port on a controller should only accept Transport Layer Security (TLS) communications when OpenFlow is used between the SDN controller and a switch.
- *Threat references:* 6.2 in [3]

4.2.9 Protecting Reference Data from Unauthorized Modification

- *Requirement name*: Protecting reference data from unauthorized modification
- *Requirement description:* Any reference data modification (e.g., configuration and backup flow table modification) in the SDN controller must be authorized. An appropriate access control can be used for related applications, switches, other SDN controllers, and users.

- *Threat references:* 6.2 in [3]

4.2.10 Log Function

- *Requirement name*: Log function
- *Requirement description:* SDN controllers must support a log function to record the operations on it. These operations include the login and logout of administrators, any reference data modifications, etc. The parameters captured in logs shall include at least user name, start time, stop time, performed action, and result. The controller should also log which NBI functions are called by whom, when, what was the result, etc.
- *Threat references:* 6.3 in [3]

4.2.11 Log Files Access Protection

- *Requirement name*: Log files protection
- *Requirement description:* Access to the log file must be controlled (file access rights) and only privileged users should have access to the log files.
- *Threat references:* 6.3 in [3]

4.2.12 Log Modification Protection

- *Requirement name*: Log modification protection
- *Requirement description:* Any modifications of a log file must be authorized and these modifications must also be logged.
- *Threat references:* 6.3 in [3]

4.2.13 Authorization for Access to Sensitive Data

- *Requirement name*: Authorization for access to sensitive data
- *Requirement description:* Unless legally authorized by the SDN controller, any applications, switches, other controllers, and users cannot access the sensitive data on the controller.
- *Threat references:* 6.4 in [3]

4.2.14 Protecting the Confidentiality of Data in Transit

- *Requirement name*: Protecting the confidentiality of data in transit
- *Requirement description:* The confidentiality of the communication packets between the SDN controller and any entity (e.g., an NE, an application, or an OSS) should be protected with standard network protocols (e.g., TLS). The SDN controller must support these network protocols. For example, the OpenFlow port on the controller should only accept Transport Layer Security (TLS) communications when OpenFlow is used between the SDN controller and a switch.
- *Threat references:* 6.4 in [3]

4.2.15 Hiding Password and Key Display

- *Requirement name*: Hiding password and key display
- *Requirement description:* Passwords, digital certificate private keys, encryption keys, etc. in the SDN controller must not be displayed on the screen in plain text.
- *Threat references:* 6.4 in [3]

4.2.16 Application Isolation

- *Requirement name*: Application isolation
- *Requirement description:* The SDN controller should strictly isolate the data between different applications. Without authorization, one application should not be able to access or modify the state of other applications, or to change resource limit settings of other applications, or to unsubscribe services of other applications from the SDN controller.
- *Threat references:* 6.4 in [3]

4.2.17 Traffic Separation

- *Requirement name*: Traffic separation
- *Requirement description:* The SDN controller should support physical or logical separation of OSS traffic and control plane traffic.
- *Threat references:* 6.4 in [3]

4.2.18 Access Control on the GUI

- *Requirement name*: Access control on the GUI
- *Requirement description:* There must be authentication and authorization for any user who accesses the GUI.
- *Threat references:* 6.4 in [3]

4.2.19 VM Security

- *Requirement name*: VM security
- *Requirement description:* VMs need to take measures such as cgroup technology to restrict, collect statistics for, or separate resources of process groups (CPU, memory, and disk input/output) to prevent system resource abuse.
- *Threat references:* 6.4 in [3]

4.2.20 Closing Unnecessary Ports/Services

- *Requirement name*: Closing unnecessary ports/service
- *Requirement description:* The SDN controller should close any unnecessary ports/services and only open necessary ports/services.
- *Threat references:* 6.4, 6.5 in [3]

4.2.21 Physical Host Security

- *Requirement name*: Physical host security
- *Requirement description:* Specific security measures (e.g., redundant deployment, resource planning, etc.) must be taken to minimize overload risks brought by insufficient resources for physical hosts, such as the server of the controller.
- *Threat references:* 6.5 in [3]

4.2.22 Restriction for Forwarding Packets from Switches

- *Requirement name*: Restriction for forwarding packets from switches
- *Requirement description:* The SDN controller should restrict packet-in messages that include mismatched packets from switches to prevent DoS attacks due to a large number of packets forwarded from switches.
- *Threat references:* 6.5 in [3]

4.2.23 Authorization for Flow Table Creation

- *Requirement name*: Authorization for flow table creation
- *Requirement description:* The SDN controller should check the authorization of an application when the application requests the controller to create a flow table.
- *Threat references:* 6.5 in [3]

4.2.24 Anti-DoS from Computing Capacity Exhaustion

- *Requirement name*: Anti-DoS from computing capacity exhaustion
- *Requirement description:* The SDN controller should support monitoring of the computing capacity consumption and turn on the anti-DoS mechanisms when the consumption reaches the threshold.
- *Threat references:* 6.5 in [3]

4.2.25 Anti-DoS from Northbound/Southbound Interfaces

- *Requirement name*: Anti-DoS from northbound/southbound interfaces
- *Requirement description:* The SDN controller should support anti-DoS from northbound/southbound interfaces. The SDN controller should support monitoring of access traffic from the northbound/southbound interfaces and turn on the anti-DoS mechanisms when the access traffic reaches the threshold.
- *Threat references:* 6.5 in [3]

4.2.26 Anti-DoS from Excessive Resource Consumption

- *Requirement name*: Anti-DoS from excessive resource consumption

- *Requirement description:* The SDN controller should limit the maximum boundary of resource (e.g., CPU, memory) consumption by the application. The maximum boundary should be set according to the authorization of the application.
- *Threat references:* 6.5 in [3]

4.2.27 Privileged Control of Applications

- *Requirement name*: Privileged control of applications
- *Requirement description:* The SDN controller should allocate privileges for each application (i.e., the controller shall authorize each application) and verify the privileges of applications when they access the controller.
- *Threat references:* 6.6 in [3]

4.2.28 Policy Conflict Resolution

- *Requirement name*: Policy conflict resolution
- *Requirement description:* The SDN controller should support the detection of policy conflicts and give an appropriate resolution. The SDN controller may set different priorities for different types of applications to ensure that the policy from non-security applications cannot bypass the policy from administrators or security applications.
- *Threat references:* 6.6 in [3]

4.2.29 Authorization for Using System Functionalities

- *Requirement name*: Authorization for using system functionalities
- *Requirement description:* The SDN controller must support authorization for using system functionalities such as the access console interface, debug interface, APIs and SSH, FTP service, etc.
- *Threat references:* 6.6 in [3]

4.2.30 Interface Authorization for Third Parties

- *Requirement name*: Interface authorization for third parties
- *Requirement description:* The SDN controller must support authorization for third parties to use interfaces to test, maintain, debug, or monitor the application.
- *Threat references:* 6.6 in [3]

4.2.31 Security of the Hosting OS

- *Requirement name*: Security of the hosting OS
- *Requirement description:* The hosting OS of the SDN controller must be secured. An attacker may control the SDN controller software through vulnerabilities of the hosting OS. As the SDN controller software runs on a traditional server or virtualized machine, the

security requirements of the hosting OS are the same as the traditional OS. The traditional OS's hardening methods should therefore apply to the controller's hosting OS.

- *Threat references:* 6.6 in [3]

4.3 Categorized Security Requirements

4.3.1 General Security Requirements

The following are requirements that may not be directly related to the design and development of the controller itself but are important to its environment, operation, or management.

1) IP check (4.2.2)
2) User authentication (4.2.3)
3) Account management (4.2.4)
4) Hardware consistency (4.2.5)
5) Hypervisor security (4.2.6)
6) Software package integrity (4.2.7)
7) Protecting the integrity of data in transit (4.2.8)
8) Log function
    a) Log function (4.2.10)
    b) Log files access protection (4.2.11)
    c) Log modification protection (4.2.12)
9) Protecting the confidentiality of data in transit (4.2.14)
10) Hiding password and keys display (4.2.15)
11) Traffic separation (4.2.17)
12) Access control on GUI (4.2.18)
13) VM security (4.2.19)
14) Physical host security (4.2.21)
15) Anti-DoS function:
    a) Anti-DoS from computing capacity exhaustion (4.2.24)
    b) Closing unnecessary ports/services (4.2.20)
16) Authorization for using system functionalities (4.2.29)
17) Interface authorization for third parties (4.2.30)
18) Security of the hosting OS (4.2.31)

4.3.2 Specific Security Requirements

The following are the requirements that have a close relationship with the design and development of the controller itself. These are the core elements to distinguish the security of different controllers.

1) Authentication on interfaces of SDN controllers (4.2.1)
2) Protecting reference data from unauthorized modification (4.2.9)
3) Authorization for access to sensitive data (4.2.13)
4) Hiding password and key display (can be either general or specific, depending on the development) (4.2.15)
5) Application isolation (4.2.16)
6) Anti-DoS function
    a) Restriction for forwarding packets from switches (4.2.22)
    b) Authorization for flow table creation (4.2.23)
    c) Anti-DoS from northbound/southbound interfaces (4.2.25)
    d) Anti-DoS from excessive resource consumption (4.2.26)
7) Privileged control of applications (4.2.27)
8) Policy conflict resolution (4.2.28)

5 Conclusion

According to SDN architecture specifications, SDN controllers have logically centralized control, open programmable interfaces, abstracted network resources, and state features. These features make SDN controllers high-value targets for attackers [4], so controller security is very important. An entire network can be disabled if its SDN controllers are compromised. This document provides security foundation requirements for SDN controllers to ensure that they have basic security assurance. This document will be extended and/or updated to reflect additional requirements or compliance information, as required.

6 References

[1] ONF, “SDN architecture,” Issue 1, June, 2014, ONF TR-502, available at: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/TR_SDN_ARCH_1.0_06062014.pdf

[2] Microsoft STRIDE: http://www.microsoft.com/en-us/download/details.aspx?id=14719

[3] ONF, “Threat analysis for SDN architecture,” Issue 1, July 2016, ONF TR-530, available at https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/Threat_Analysis_for_the_SDN_Architecture.pdf

[4] ONF, "Principles and Practices for Securing Software-Defined Networks," Issue 1, January, 2015, ONF TR-511, available at: https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/Principles_and_Practices_for_Securing_Software-Defined_Networks_applied_to_OFv1.3.4_V1.0.pdf

[5] POX Python network controller: http://www.noxrepo.org/pox/about-pox/

[6] Shin, Seungwon, et al, "Rosemary: A Robust, Secure, and High-Performance Network Operating System," CCS'14, Arizona, USA.

[7] ONOS Drake 1.3.0 Release Notes: https://wiki.onosproject.org/display/ONOS/Release+Notes+-+Drake+1.3.0

[6] Sandra Scott-Hayward, "Design and deployment of secure, robust, and resilient SDN Controllers," 1st IEEE Conference on Network Softwarization (IEEE NetSoft), 2015.

[8] Khondoker, Rahamatullah, et al, "Feature-based comparison and selection of Software Defined Networking (SDN) controllers." 2014 World Congress on Computer Applications and Information Systems (WCCAIS), IEEE, 2014.

7 Contributors

Ivy Guo (China Mobile)

Makan Pourzandi (Ericsson),

Sandra Scott-Hayward (Queen's University Belfast),

Haibin Song (Huawei)

Clair Wangke (China Mobile)

Frank Xialiang (Huawei)

Dacheng Zhang （Alibaba）

Xiaojun Zhuang (China Mobile)

8 Appendix: Open Source Practice

This appendix summarizes the security requirements compliance of several publicly available SDN controllers, some of which are widely used. The purpose of this appendix is to highlight the level of adoption of the identified security controls at the time of publication of this document.

A checkmark indicates that the requirement is supported, an 'x' indicates that the requirement is unsupported, and a blank cell indicates that the requirement has not been tested.

No.	General Security Requirement	ONOS v1.4.0	OpenDaylight Lithium	POX [5]	Rosemary [6]	Ryu 3.1.3	Trema (0.3.19)
1	IP check						
2	User authentication	✓ [7]	✓ [8]			× [8]	
3	Account management						
4	Hardware consistency						
5	Hypervisor security						
6	Software package integrity						
7	Protecting the integrity of data in transit[1]	✓ [7]	D-CPI [8]	D-CPI [9]		D-CPI [8]	D-CPI [9]
8.a	Log function	✓ [8]	✓ [8]		✓ [6]	✓ [8]	
8.b	Log files access protection	✓ [8]	✓ [8]			✓ [8]	
8.c	Log modification protection						
9	Protecting the confidentiality of data in transit[1]	✓ [7]	D-CPI [8]	D-CPI [9]		D-CPI [8]	D-CPI [9]
10	Hiding password and keys display						
11	Traffic separation						
12	Access control on the GUI	✓ [7]	✓ (weak) [8]		N/A [6]	× [8]	N/A [9]
13	VM security						
14	Physical host security						
15.a	Anti-DoS from computing Capacity exhaustion				✓ [6]	× [8]	
15.b	Closing unnecessary ports/services						
16	Authorization for using system functionalities						

[1] With respect to TLS, a checkmark indicates that TLS is supported, not that it is implemented by default.

17	Interface authorization for third parties						
18	Security of the hosting OS						

No.	Specific Security Requirement	ONOS v1.4.0	OpenDaylight Lithium	POX [5]	Rosemary [6]	Ryu 3.1.3	Trema (0.3.19)
1	Authentication on interfaces of SDN controllers	✓ [7]	D-CPI [8]	D-CPI [9]		D-CPI [8]	D-CPI [9]
2	Protecting reference data from unauthorized modification						
3	Authorization for access to sensitive data		✓ [8]		✓ [6]	× [8]	
5	Application isolation				✓ [6]	× [8]	
6.a	Restriction for forwarding packets from switches						
6.b	Authorization for flow table creation						
6.c	Anti-DoS from northbound/southbound interfaces (A-CPI, D-CPI)						
6.d	Anti-DoS from excessive resource consumption				✓ [6]	× [8]	
7	Privileged control of applications	✓ [7]				× [8]	
8	Policy conflict resolution	✓ (Data-Store) [8]				× [8]	