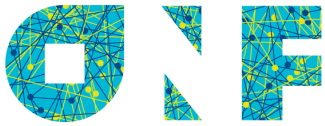

OPEN NETWORKING
FOUNDATION

Charter of Security Project

Date: 2014/11/25

Authors:

Dacheng Zhang, Huawei, zhangdacheng@huawei.com
Sriram Natarajan , Deutsche Telekom, sriram.natarajan@telekom.com
Aubrey Merchant-Dest, Blue Coat, aubrey.merchant@bluecoat.com
Sandra Scott-Hayward, Queen's University Belfast, s.scott-hayward@qub.ac.uk

1. Introduction and Business Case

Security Project (Sec Project) will take the responsibility of leading the SDN security work in order to ensure the standards proposed by ONF fulfill expected security capabilities. Specifically, the project will explore potential security issues in SDN networks and ONF proposals, review the documents/solutions of other projects, and propose specifications for securing proposed ONF solutions if necessary.

Establishing a Security Project will enable ONF to lead the SDN security considerations and support existing efforts in other industry groups and standards organizations (e.g. ETSI, ITU-T, IETF, and IRTF) that highlight the importance of security in SDN and NFV. If necessary, Sec Project will also analyze the gaps that may occur during the integration of these organization's security solutions into ONF-based SDN networks.

2. Program of Work

The work of the project can be classified into three categories (see Figure 1), *Fundamental Research*, *Hardening SDN*, and *Improvement of Security Services*.

- *Fundamental Research* includes any work which benefits the understanding of security issues with SDN technologies. The tasks that the project currently plan to engage in include:
  - *Security Principles and Requirements* which aims to provide the criteria to assess the design of ONF proposals and specifications with respect to security.
  - Threat Analysis which aims to explore the potential threats/vulnerabilities associated with the ONF-based SDN solutions in different deployment models and real world use cases.
- *Hardening SDN* is concerned with the provisioning of security mechanisms (e.g. credential management, secure audit) to protect the SDN protocols or devices against various types of attacks, and the analysis of the possibilities of using SDN technologies to improve network security. It will also include the efforts towards the definition of global recommendations for secure SDN in line with standard information security domains [5].
- *Improvement of Security Services* involves helping other ONF projects review their deliveries and fix identified security breaches.

In the work plan for the first year, these three categories are designated by work packages, as follows:

WP1: ***Fundamental Research***

- Publish the security principles document and the security requirements document for ONF Protocols.
- Perform threat analysis based on the SDN architecture specified in [4].

WP2: ***Hardening SDN***

- Design a credential management mechanism for ONF-based SDN networks.

WP3: ***Improvement of Security Services***

- Help FA Project specify extensions for securing TTP/NDM.
- Perform vulnerability assessment on Openflow and OF-Config (and other ONF proposals if necessary).
- Provide assistance to other projects when they meet security related issues during their work.

3. Deliverables and Timetable

The timetable for delivering the work plan outlined in Section 4 is provided in Table 1. Although the work packages will be carried out in parallel, the completion of initial drafts and deliverable documents are staggered to support review and discussion by the full membership of the project, i.e. the project can focus on one draft/deliverable at one time.

Activity	Duration
Project setup–appointment of Editor/Chair/Vice-chair Election of WP Leaders	2014/11/01
WP1: Finish the Security Principles and Requirements Document WP 1: Start the writing of threat analysis document WP 2: Start the design of credential management mechanism WP 3: Start the vulnerability analysis of ONF protocols WP 3: Start the design of a signature mechanism for NDM	2015/01/01
WP 3: Finish the initial draft of signature mechanism and collect feedbacks from FA Project	2015/02/01
WP 2: Finish the document of credential management mechanism	2015/03/01
WP 1: Finish the initial draft of threat analysis and collect feedback	2015/05/01
WP 3: Finish the design of a signature mechanism for NDM	2015/06/01
WP 3: Finish the vulnerability analysis for ONF protocols	2015/08/01
WP 1: Finish the threat analysis document	2015/09/01
WP1-3: Progress and Deliverables Review Recommendations on next steps (e.g. global recommendations for secure SDN, Secured enhanced SDN architecture)	2015/10/01

Table 1: Sec Project Year 1 Timetable

4. Considerations

Security is often considered to be an add-on and, as such, a non-essential and time-consuming part of the design process. It will be an objective of the project to simplify the process of security specifically in interactions with other projects.

5. Relationship of Proposed Project to Existing Efforts within and outside of ONF

An important role of the proposed project is to act as the “background” or the “security consultant group” to support the security related work in all the other projects. In addition, many tasks (e.g. the work in ***Security Principles and Requirements*** and ***Threat Analysis***) that the project will be engaged in are not covered in the charters of any other projects. Therefore, it is reasonable to form a new security Project rather than a sub-project under another existing project.

When designing security solutions for ONF-based SDN, a key strategy is to make use of proven security mechanisms whenever possible; new protocols and algorithms are

created as a last resort when stated requirements cannot be met. However, when an SDN security solution is developed by implementing the protocols or algorithms proposed by other standard organizations (e.g. TLS by IETF), or before directly migrating a security mechanism that was designed for traditional networks in SDN, there are several important issues (e.g. the incompatibility, complexity) to be evaluated. As a result, it is reasonable to invite the security experts of other standard organizations (e.g. IETF, IRTF, ITU-T, IEEE) to participate in the review of the security solution (when they have already been published), since those experts have better and deeper understanding of their protocols and solutions. Therefore, Sec Project can provide a platform for security experts in ONF to collaborate with other standardization bodies in a more productive and well organized manner.

6. ONF Member Company Anticipated Participants

Currently, there are more than 10 regular contributors:

Alcatel-Lucent, Blue Coat Systems, Broadcom, Brocade, China Mobile Technology (USA) Inc., Cisco, Deutsche Telekom Inc., Ericsson, Freescale, Goldman Sachs, GuardiCore, Huawei Technologies, IBM Corporation, Infoblox, Luxoft, NetScout Systems, NTT, ONF Research Associates, Telefonica, Verizon, ZTE Corporation, Inc.

7. Reference Materials

[1] ONF Security Principles,
http://login.opennetworking.org/bin/c5i?mid=4&rid=5&gid=0&k1=423&tid=1402650023.

[2] ONF Security Requirements for SDN Protocols,
http://login.opennetworking.org/bin/c5i?mid=4&rid=5&gid=0&k1=558&tid=1402649875.

[3] Openflow Negotiable Datapath Models,
http://login.opennetworking.org/bin/c5i?mid=4&rid=5&gid=0&k1=679&tid=1403084717.

[4] SDN Architecture,
http://login.opennetworking.org/bin/c5i?mid=4&rid=5&gid=0&k1=257&tid=1403084812.

[5] The 10 Security Domains,
http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_050430.hcsp?dDocName=bok1_050430.