February 2017

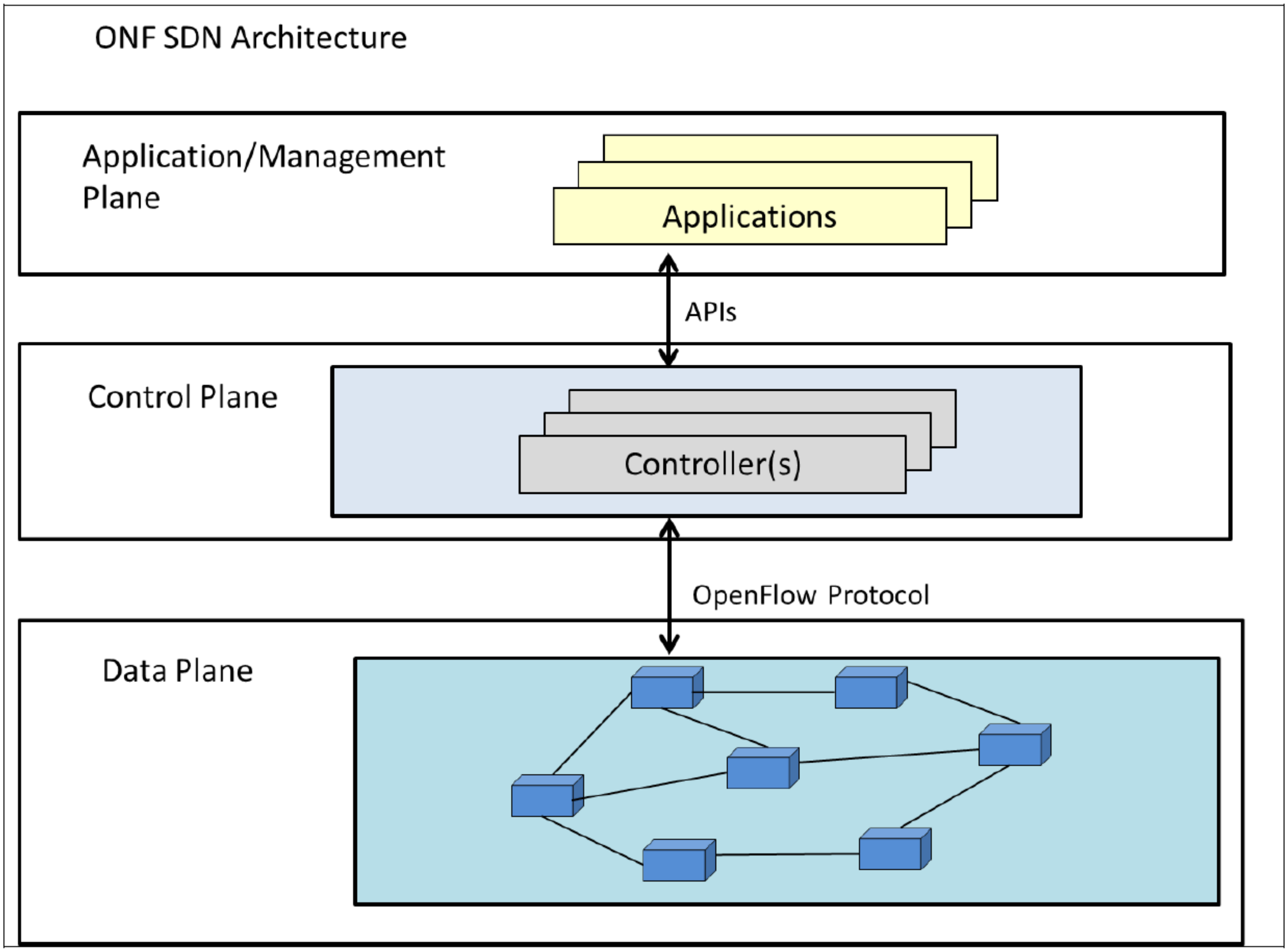
Overview of Software Defined Networking (SDN) Risks

Software Defined Networking (SDN) is an emerging technology, defined by the Open Networking Foundation (ONF) as “the physical separation of the network control plane from the forwarding plane, and where the control plane controls several devices.” While SDN offers new capabilities, it also introduces new risks. This document provides technical background, an overview of risks, and guidance for decision makers regarding SDN. For some networks, it may be impossible to mitigate critical risks due to architectural or implementation challenges.

Background

SDN was developed to meet the needs of cloud-based network architectures, which had to be dynamic and highly scalable. Features promised or provided by SDN solutions include programmability, automation, network control, centralized management, and cost savings.

The following diagram is an SDN architecture as defined by ONF:



ONF maintains the OpenFlow Protocol Specification which defines an interface between the control and data plane, also called the Southbound Interface [8]. ONF also chartered a Northbound Interface working group in 2013 to define and subsequently specify SDN interfaces between the control plane and management plane. However, OpenFlow as presently defined may not adequately scale for intended applications and it is not implemented by all vendors offering SDN solutions. In fact, industry is not on a clear trajectory toward any particular specification.

Some vendors address each plane of the SDN architecture individually while others provide an integrated solution to handle all three planes. These solutions also exhibit varying degrees of hardware independence. Gartner categorized three distinct approaches toward SDN based on the majority market share in the report "Use Software-Defined Networking to Transform Your Data Center Network Business", published 10 June 2015:

- Products with a basis in open source projects. This includes SDN Controllers (OpenDaylight, Open Network Operating System (ONOS)[1], Floodlight®[2]), SDN switches (Open vSwitch, OpenSwitch™[3],) and newly released SDN/NFV Orchestrator Platform (Open-O®[4]). Commercial versions of these products include offerings as for example from HP, BigSwitch, Quanta, Dell, Brocade, and Cumulus.
- VMware®'s Software Defined Data Center Solution using vSphere® and NSX®[5].
- Cisco®'s[6] Application Centric Infrastructure (ACI) product which provides programmability and centralized policy management.

Software Defined Network Risks

The abstraction provided by SDN does not automatically improve the security of a networking architecture. At a minimum, SDN shifts the risk paradigm when compared to traditional networking. The following table provides a high-level list of SDN-specific risks, discussion of those risks, and mitigation when available.

[1] Open Network Operating System® is a registered trademark of ONOS

[2] Floodlight® is a registered trademark of Big Switch Networks, Inc.

[3] OpenSwitch™ is a trademark of SAP

[4] Open-O® is a registered trademark of The Linux Foundation.

[5] VMWare®, vSphere® and VMWare NSX® are registered trademarks of VMWare, Inc.

[6] Cisco® is a registered trademark of Cisco Systems, Inc.

Risk	Discussion	Mitigation
Controller as Single Point of Compromise.	A single centralized controller in an SDN architecture presents a tempting target for adversaries. Compromise of the controller implies compromise of all of the network infrastructure under its control. Effectively, this implies compromise of the entire network.	In order to guard against compromise, security investment should focus on maintaining integrity of the controller. Considerations include: • Integrity of all the components of the controller. This includes using trusted network device hardware and software, operating system software and application software. • Auditing of controller activities, such as authentication events and tasking to switches.
Interception, Modification, or Disruption of Management and Controller Traffic.	Communication channels in common SDN implementations are not encrypted or authenticated. OpenFlow, for example, does not enforce the use of encryption between the control and data plane. Considerable variations exist in the security of Northbound interfaces, which may depend upon the particular application tasking the control plane. Rogue nodes or compromised hosts can take advantage of this in order to intercept, modify, or otherwise disrupt management and controller traffic. This includes collection of credentials or other sensitive data, reprogramming the network to hide malicious activity, and denial-of-service attacks.	Perform a complete survey of all communication channels between the three planes of the SDN implementation. Activate encryption and authentication wherever possible, and architect the network to address any unprotected communications. If the network cannot be architected to ensure protection of any unencrypted management and controller traffic, this this creates a critical risk.
High Complexity Leads to Compromise or Failure.	Many components make up an SDN deployment. The deployment inherits vulnerabilities from all underlying components, which can be substantial. Because there are not well-established standards for communication between SDN components, interoperability problems can arise. Compounding the complexity challenge, SDN is still rapidly evolving. Network administrators are more likely to have difficulty troubleshooting technology that is rapidly changing. They are also likely to encounter challenges in achieving a secure configuration for deployment.	Implement a regime for rapidly applying software updates to all components of the SDN deployment. Use commercially-supported components or solutions. This guidance applies equally to open source and closed source software, in accordance with DoD CIO guidance [15]. Using open source software without commercial support creates significant integration and deployment risks. Invest in training for network administrators to ensure they stay up-to-date on SDN technology, including security. Apply vendor-supported, vendor-specific configuration guidance whenever available. [i.e. 11].

Guidance

Risk decision makers for SDN systems must weigh several risks before deciding whether or how to adopt SDN. In addition to the risks and mitigations described in the previous section, these factors include the level of assurance in the products being procured.

Due to its rapid evolution, there is no standard for evaluating SDN product offerings today. However, some individual components within an SDN deployment can be evaluated against National Information Assurance Partnership (NIAP) Protection Profiles [1], which are required for all National Security Systems including DoD networks [2 and 3]. Protection Profiles which can be evaluated against include the Network Device Protection Profile, the General Purpose Operating System Protection Profile, and the Server Virtualization Protection Profile. The NIAP is also actively tracking the development of SDN technologies in order to determine when creation of a Protection Profile for this technology area is appropriate.

References

1. https://www.niap-ccevs.org/Profile/PP.cfm: most recent version of:
    - ***Guidance for When No PP Exists***, ***Protection Profile for General Purpose Operating Systems***, ***Protection Profile for Server Virtualization***,
    - ***Protection Profile for General Purpose Operating Systems***
    - ***Protection Profile for Server Virtualization.***
2. https://www.cnss.gov/CNSS/isuances/Policies.cfm: ***CNSSP 11, Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products***
3. nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800.53r4.pdf: ***NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations***.
4. https://www.sdxcentral.com: News coverage, leaders interviews product and technology announcements and content about SDN, NFV, Cloud, Containers, DevOps, Security, Virtual Edge and White Box.
5. https://wwwlinuxfoundation.org: Linux Foundation – SDN related OpenSource Projects such as:
    - https://www.opendaylight.org: OpenDaylight®[7]
    - http://docs.opendaylight.org/en/latest/getting-started-guide/security_considerations.html
    - https://www.openvswitch.org: OpenVSwitch
    - https://www.open-o.org: SDN/NFV Orchestrator Platform
6. http://onosproject/org: Open Networking Operating System (ONOS) – SDN OS that has scalability, high availability, high performance and abstractions to make it easy to create apps and services.
7. https://osrg.github.io/ryu/: RYU – a component-based software defined networking framework.
8. https://www.opennetworking.org: Open Networking Foundation (ONF).
    - ***OpenFlow Switch Specification, Version 1.0.0***, December 31, 2009.
    - ***OpenFlow Switch Specification, Version 1.3.3***, December 18, 2013.
    - ***OpenFlow Switch Specification, Version 1.4.0***, October 15, 2013.
    - https://www.opennetworking.org/openflow-conformance-certification.
9. http://www.gartner.com/technology/home.jsp: Information technology research and advisory company.

[7] OpenDayLight® is a registered trademark of Opendaylight Project, Inc.

10. https://www.vmware.com/products/nsx: VMware product information for NSX.
11. https://communities.vmware.com/docs/DOC-28142: ***NSX-v 6.2.x – Security Hardening Guide,*** published by VMware Community, last modified 10 June 2016.
12. https://communities.vmware.com/docs/DOC-27674: ***Securing of NSX vSphere***, published by VMware Community, last modified 15 September 2014.
13. ***Security Risks in SDN and Other New Software Apps***, Anthony Lim, 2015 RSA Conference.
14. ***Enhancing Security in OpenFlow***, Niketa Chellani, Prateek Tejpal, Prashant Hari, Vishal Neeralike. University of Colorado Boulder "http://www/colorado.edu/itp/sites/default/files/attached-files/70088-130943_-_vishal_neeralike_-_apr_25_2016_1154_pm_–_enhancing_security_sdn.pdf"
15. ***Clarifying Guidance Regarding Open Source Software (OSS) DoD CIO Memorandum***, 16 Oct 2009, http://dodcio.defense.gov/Portals/0/Documents/FOSS/2009OSS.pdf

Disclaimer

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact Information

Industry Inquiries
410-854-6091
email: bao@nsa.gov

CLIENT REQUIREMENTS AND GENERAL IA INQUIRIES
Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov