

软件定义网络安全研究

王 月,吕光宏,曹 勇

(四川大学 计算机学院,四川 成都 610065)

摘 要:随着网络规模的扩大及业务的多样化,原有的网络架构难以满足未来发展需求,软件定义网络 (software defined networking, SDN) 作为一种新型网络架构被提出。将控制平面从数据平面中分离出来,控制平面的集中管控简化了网络配置管理,实现了灵活部署,提高了网络性能。利用 SDN 的集中获取信息的特性可对网络中的安全威胁进行监督检测,提高网络安全性。然而 SDN 在带来便利的同时也带来了新的安全问题。文中从 SDN 的各层及接口对网络安全问题进行分析,并对现有的解决方案进行了分类,分别从提升 SDN 控制器安全性、DoS/DDoS 攻击防御、流规则一致性、提升应用程序安全性、北向接口标准化这 5 个方面进行了探讨,进而得出结论,并对未来进行展望。

关键词:软件定义网络;OpenFlow;安全威胁;SDN 安全

中图分类号:TP393

文献标识码:A

文章编号:1673-629X(2018)04-0128-05

doi:10.3969/j.issn.1673-629X.2018.04.027

Research on Security of Software Defining Network

WANG Yue, LYU Guang-hong, CAO Yong

(School of Computer, Sichuan University, Chengdu 610065, China)

Abstract: With the expansion of the network and the diversification of the business, the original network architecture is difficult to meet the future development requirements, so software defined network (SDN) as a new network architecture is proposed. SDN separates the control plane from the data plane, and the centralized control of control plane simplifies the network configuration management, which enables flexible deployment and improves the overall network performance. The feature of SDN's concentrated accessing information can supervise and detect the threats in the network to improve its security. However, SDN also brings us new security problems as well as convenience. In this paper, we analyze the network security from SDN layers and interfaces and classify the existing solutions. And we make a discussion in five aspects including enhancing SDN controller security, DoS/DDoS attack defense, flow rules consistency, raising the application security and standardizing the north interface, then get a set of conclusion and prospects for the future.

Key words: software defined network; OpenFlow; security threat; SDN security

0 引 言

SDN 技术颠覆了传统网络的运行模式,将控制平面与数据平面解耦合,实现了控制层的集中管控,数据层的快速转发部署,具有灵活性、开放性、可编程性和虚拟化等特点,已经在云计算和虚拟化技术等领域中得到了广泛的应用^[1]。

传统网络将控制逻辑和数据转发紧密耦合在网络设备上,带来网络控制平面管理的复杂化。SDN 将控制功能从网络节点中独立出来,以开放的软件模式,基于控制器对网络进行统一状态获取和配置。SDN 这种集中获取网络资源信息的特性,有助于网络安全监控检测,借助 SDN 控制器实时获取网络全局信息对其

分析,可以更快地检测和防范网络中的攻击。也正是因为 SDN 控制器具有这种集中管控的特性,使得控制器遭受攻击的风险增加。

SDN 的可编程性和开放性也是其重要特性,用户在应用层可通过编程的方式,调用网络资源,从而动态管理配置底层资源,加快应用部署。SDN 在为第三方使用者带来便利的同时,也使攻击者能够更容易发起网络攻击。

随着业界对 SDN 研究的不断深入,SDN 的安全性问题逐渐受到重视。在分析 SDN 的基本架构、工作流程的基础上,对借助 SDN 的特性帮助解决网络安全威胁进行了探讨。另一方面从 SDN 架构自身特点入

收稿日期:2017-05-16

修回日期:2017-09-20

网络出版时间:2017-12-05

基金项目:国家“863”高技术发展计划项目(2008AA01Z105)

作者简介:王 月(1993-),女,硕士研究生,研究方向为软件定义网络;吕光宏,教授,研究方向为计算机网络与信息系统。

网络出版地址: <http://kns.cnki.net/kcms/detail/61.1450.TP.20171205.1436.138.html>

手,分析了该架构自身存在的安全问题,并对目前关于SDN 安全问题的解决方案进行阐述,最后对未来的SDN 安全研究进行展望。

1 SDN 架构

SDN 起源于2006 年斯坦福大学的Clean Slate 研究课题,2008 年Mckeown 教授提出了OpenFlow 技术并逐渐推广SDN 概念^[1],OpenFlow 实现了SDN 可编程网络的思想,代表了SDN 技术的实现原型和部署实例。SDN 技术打破了传统网络架构,实现了控制与转发的分离以及底层硬件的虚拟化,控制层通过维护全网视图更好地实现对网络流量的控制;底层硬件设备只专注于数据的转发,简化了部署,提高了效率;应用层业务通过编程方式调用所需的网络抽象资源,方便用户对网络的配置和快速部署^[2]。

针对不同需求,许多组织提出了相应的SDN 参考架构。开放基金会组织(open networking foundation, ONF)提出的SDN 架构已经为学术界和产业界普遍认可,其架构如图1 所示,自底向上可分为基础设施层、控制层和应用层。控制层的控制器和基础设施层的路由设备经由SDN 的南向接口通信,南向接口具有统一标准,目前采用的是OpenFlow 协议。控制器和应用层的应用程序是经由SDN 北向接口通信,北向接口允许用户按需求开发。控制器是控制层的核心组件,通过控制器用户可以逻辑上集中控制网络设备^[3]。基础设施层由OpenFlow 交换机等网络设备构成,执行简单的路由转发功能。OpenFlow 交换机由流表、安全通道和OpenFlow 协议三部分组成,OpenFlow 交换机的处理单元是流表,OpenFlow 协议是基于流的概念来匹配规则的,这使得网络设备在转发数据时更为灵活^[4]。

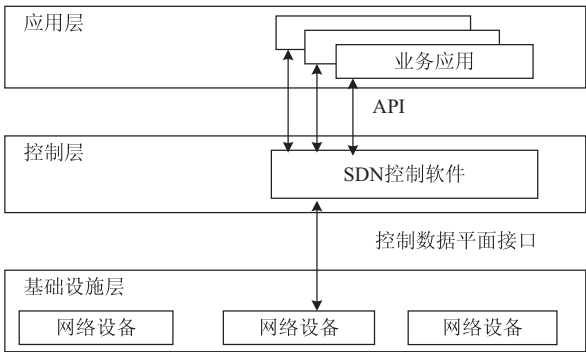


图1 SDN 体系架构

基于OpenFlow 的SDN 的工作流程如图2 所示。
Step1:当交换机1 收到主机A 发来的一条报文,首先查找本地流表;
Step2:当找不到匹配表项时,将报文转发给控制器;
Step3:控制器通过对全网视图的分析,做出转发

策略并下发,并通过OpenFlow 协议更新交换机中的流表,维护全网一致性;
Step4:交换机1 按照下发来的流表做出指定转发行为转发到交换机2;
Step5:交换机2 能在本地找到匹配项,就直接对其进行转发,直至目标端B。

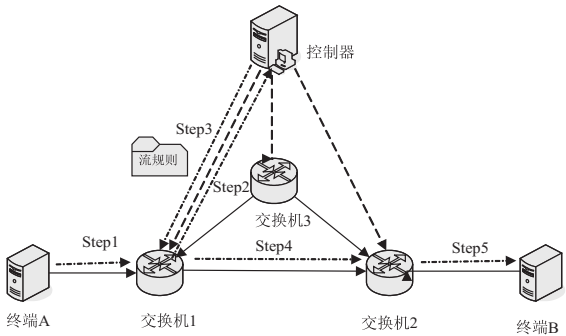


图2 SDN 工作流程

2 SDN 的网络安全性研究

由图2 可以看出,SDN 网络的数据流转发决定由SDN 控制器负责,SDN 网络具有更好地获取全局信息的能力和对网络统一管理的功能,SDN 网络利用集中管控的特点和自适应方式能够更快地检测攻击^[5]。

2.1 SDN 作为IDS 和IPS

传统网络易受到入侵攻击,而不易被及时检测到,利用SDN 的集中管控特性和可编程性,可以将SDN 作为入侵检测系统(IDS)和入侵防御系统(IPS),监控网络活动,检测网络攻击并防御攻击媒介^[6]。

Shin、Gu 团队提出的CloudWatcher^[7],是一种在云环境中,基于SDN 控制层监控网络中的流量,使其通过基础设施层中指定的安全组件(如IDS、防火墙等),可以防止可能构成威胁的恶意数据包输入到网络。

Chung 等提出一种网络入侵检测及策略选择系统NICE^[8],利用SDN 控制器获得的完整网络状态信息这一特性,将获取的网络安全相关状态信息转交给攻击分析器,由攻击分析器对其分析并做出相应策略,达到预防攻击的作用。

Porras 研究团队设计出了一种面向SDN 控制器的安全模块框架FreSco^[9],开发人员可以基于FreSco 框架在控制器上进行安全模块开发。FreSco 提供了很多API,开发人员可根据自身要求编写相应的安全监控检测模块,对网络安全状态进行实时监控。

2.2 SDN 提供网络虚拟化

Sherwood 等提出的FlowVisor^[10],是在控制器和交换机之间实现了基于OpenFlow 的网络虚拟层,使得基础设施层的硬件能够被多个逻辑网络切片共享,

每个网络切片拥有不同的转发策略,在这种独立的切片模式下,多个应用可以同时运行在网络中而彼此不受影响。利用这种方式构建出相互隔离的虚拟网络,这种隔离可以防止由任何虚拟网络工作负载可能发起的攻击对底层物理基础设施的影响。

3 SDN 自身的安全问题分析

SDN 作为新架构,具有的新特性能够大大提高网络性能,同时也存在一定的安全问题。下面从 SDN 的架构角度出发,分别从应用层、控制层和基础设施层,以及这些层面间的接口来分析 SDN 面临的安全问题。

3.1 控制层安全威胁

SDN 的控制器能获取到全网的状态信息,它是整个网络的指挥中心,这种集中管控获取全网信息的特点使得控制器很容易成为攻击目标。攻击可以从 SDN 架构的任何一处发起,攻击者一旦控制了控制器,就可以控制整个网络,控制器面临着被劫持的威胁。DoS/DDoS 攻击是在控制层上容易发生的入侵攻击。

3.2 应用层威胁

SDN 的控制器为应用层提供了开放性可编程接口,方便第三方人员根据各自需求,定制私有化应用,网络管理者可以通过应用程序来配置、管理网络,使网络管理更加灵活可控。攻击者正是利用 SDN 架构的这一特性,通过安装某些恶意应用,利用开放接口实施对控制器的攻击,进而攻击全网络。这一层主要面临的是恶意程序安装、虚假的身份冒用以及非法访问的威胁。

3.3 基础设施层威胁

基础设施层由交换机等硬件设备组成,负责单一的数据转发和收集工作。这些硬件设备完全是按照控制器下发的流规则进行转发的,所以该层主要有虚假的流规则注入、虚假的身份冒用等安全问题^[11-12],同时该层还面临着因流表冲突造成基础设施层转发混乱的威胁。

3.4 北向接口威胁

SDN 北向接口负责控制器和各个应用之间的通信,用户可以通过编程方式调用所需网络资源,掌握全网状态,实现网络的快速配置和部署。然而由于应用的多样性,使得北向接口也呈现多样性,目前提供的北向接口尚没有统一标准,应用程序通过北向接口连接控制器也没有认证机制,使得攻击者能轻易对控制器进行控制,使网络面临非法访问、数据泄露的威胁。

3.5 南向接口威胁

南向接口安全威胁主要是由 OpenFlow 协议的本身安全无保证造成的。控制器和交换机之间负责通信

的安全信道是采用安全传输层协议 TLS 对消息进行加密的,在会话的初始阶段容易受到攻击,攻击者通过连接交换机和控制器来控制全网络。因此南向接口面临着假冒控制器、数据窃取等威胁^[13]。

4 SDN 安全问题现有解决方案

针对以上列出的 SDN 各个层面及接口可能存在的安全威胁,国内外都有相应研究,现有如下解决方案。

4.1 提升 SDN 控制器安全性

SDN 管控集中性使得网络配置、访问控制、全局状态信息都集中于控制器,所以提高控制器的安全性十分必要,主要解决方案是在控制器上增加安全检查、权限管理的能力,来解决应用层非法访问及数据层虚假身份冒用的问题。

Porras 等针对开源控制器 NOX 设计了一种安全内核 FortNOX^[14],是在 NOX 控制器上增加了认证功能,确保了流规则的来源具有可认证性。并且 FortNOX 在 NOX 基础上增加了状态管理、流冲突检测及超时回调等功能。这些功能上的改进提升了控制器自身的安全性,同时 SDN 网络对流规则冲突检测能力也有增强。

Porras 等对 Floodlight 控制器也进行了安全扩展并提出了 SE-Floodlight^[15]。SE-Floodlight 同样具有角色认证功能和流冲突检测功能,并在此基础上增加了安全审计功能和权限管理功能,实现了对控制器的安全相关操作的审计跟踪和控制层对数据层的消息管理。

因控制器在开发之初,并没有充分地研究安全问题,现有的研究更多是在原有的控制器基础上进行了改进设计,增加安全模块,但控制器的多样性使得这种改进方式在推广上具有局限性。

4.2 DoS/DDoS 攻击防御

DoS/DDoS 攻击是 SDN 控制器面临的主要安全威胁。攻击者可以利用交换机发送大量虚假请求给控制器,占用控制器资源,造成控制器产生过量负荷,导致控制器无法为其他合法用户服务,使得整个系统瘫痪。针对 DoS/DDoS 攻击,主要解决方案是加强控制器与交换机的响应,利用 SDN 控制器集中获取状态信息特征,及时对 DoS/DDoS 攻击做出检测和防范。

Braga 等利用 SDN 集中管控的特点,提出一种轻量级 DDos 检测方法^[16],由流量收集、特征提取和分类三个阶段构成。利用自组织映射算法(self organizing map, SOM)对信息流分类,提取 OpenFlow 流统计信息中与 DDos 攻击相关的六元组,从而检测其是否具有攻击行为。该方案在攻击检测特征提取方面,具有低

消耗高效率的特点。

Shin 等提出一种可以检测 DDoS 攻击的安全架构 AVANT-GUARD^[17],该架构对 SDN 的数据层做了功能扩展,增加了连接迁移和激励触发功能。利用连接迁移方式帮助检测恶意用户,激励触发增强了控制层与数据层的交互响应,提高了响应效率,利于尽早发现 DDoS 攻击。

Radware 公司基于 SDN 技术开发的安全应用 DefenseFlowTM,可以对网络进行编程,防御 DoS/DDoS 攻击。该技术利用了 SDN 控制器能够收集到全网状态信息的特点,对流量的分布进行检测,发现其攻击行为,为用户提供自动的 DoS/DDoS 的检测和防护。

4.3 流规则一致性保证

基础设施层对控制器下发的流规则绝对信任,直接进行转发,当攻击者对控制器窃取信息并下发错误的流规则时,会造成流规则冲突的情况,进而造成交换机流表混乱,对 SDN 基础设施层安全性造成威胁。所以需要网络中流规则的合法性和一致性进行检测,以防止流规则混乱扩散带来基础设施层转发混乱,给网络造成的威胁。

Reitblatt 等提出了针对多个交换机之间流规则一致性的检测处理机制^[18],利用 OpenFlow 的标记更新功能,提出了一种两阶段更新方法,来解决新旧规则冲突的问题^[19]。这种方式的缺陷在于,在同一时间段新旧两种策略会同时存在于流表中,这会额外地消耗空间、占用资源。

FortNox^[14]架构是基于实体角色为流规则划分优先级,当需要下发并插入某条新的流规则时, FortNox 控制器会根据其优先级,将流规则更新到总流表中,发

生冲突时,优先级高的流规则会直接覆盖优先级低的流规则。对于网络中过期的流规则, FortNox 会开启超时回调,防止错误的流规则扩散。在小型网络环境中该方案具有实施性,但在大型网络场景中会因流规则很多,规则优先级划分复杂,该方案可能会不具有普遍适用性。

4.4 提升应用程序安全性

SDN 中应用层的应用程序利用北向接口,通过控制器获取底层资源信息进行交互,如果应用出现错误,例如被植入恶意代码,会使整个网络受到威胁,因此需要确保每个应用的安全性、合法性。

目前对 SDN 应用层安全的研究工作主要集中在控制器的访问控制、权限管理等方面。代表性的如 FortNOX, SE-Floodlight。Wen 等设计了一个应用程序访问权限管理系统 PermOF^[20],其对应应用层调用的相关命令进行了更细粒度的权限分配,并实现了应用程序和控制层内核的隔离,保证了上层无法对底层网络的破坏。但这种更细粒度的权限分配方式的缺陷就是效率降低。

此外,针对北向接口的安全性问题,因北向接口语言都是针对特定场景提出的,应用的多样性造成了北向接口的多样性。目前 SDN 北向接口还未形成一个统一标准,攻击者利用其中的漏洞能够发起攻击,这就需要制定一套适合北向接口的通用语义,要求开发者需根据标准化语义进行开发^[21-22]。北向接口的标准化对提升应用层和控制层间认证以及流规则的冲突一致性具有很大的帮助作用。

将以上分析的 SDN 存在的安全威胁及已有解决方案用表格形式进行总结,如表 1 所示。

表 1 SDN 安全问题及对应解决方案

安全问题	影响层面或接口	解决思路	解决方案
非法访问	应用层	角色认证 应用权限管理	FortNOX
	北向接口		SE-Floodlight
虚假身份冒用	控制层	角色认证 控制层与数据层间认证	PermOF
	应用层		FortNOX
	北向接口		SE-Floodlight
DDoS/DoS 攻击	南向接口	加强控制器与交换机的响应 对异常信息及时检测发现	AVANT-GUARD
	数据层		DefenseFlow
	控制层		轻量级 DDos 检测方法
流规则冲突	数据层	流规则合法性、一致性进行检测	AVANT-GUARD
	控制层		DefenseFlow
	数据层		流规则一致性的检测
			FortNOX
			SE-Floodlight

5 结束语

SDN 将控制平面和数据平面分离,实现了网络可

编程性和集中管控,对检测网络状态,及时发现网络威胁,提高网络安全性具有很大帮助。但同时其新特性也为网络安全带来了新的挑战。文中基于 SDN 的基

本架构和特性,从利用 SDN 的优势解决网络安全问题和 SDN 架构自身存在的安全问题这两方面进行分析,并探讨了当前 SDN 安全防护的研究进展。

目前来看,SDN 的发展尚处于初级阶段,有关 OpenFlow 协议的研究还需要进一步完善。SDN 架构中控制器的地位十分重要,从分析中可看出 SDN 的安全问题主要集中于控制层,因此提升控制器的安全性会是未来 SDN 网络安全进一步的研究方向。此外,北向接口的标准化能为控制层和应用层间的认证及权限管理提供更统一的方法,也将是未来的研究重点。

参考文献:

- [1] 左青云,陈 鸣,赵广松,等. 基于 OpenFlow 的 SDN 技术研究[J]. 软件学报,2013,24(5):1078-1097.
- [2] 张顺森,邹复民. 软件定义网络研究综述[J]. 计算机应用研究,2013,30(8):2246-2251.
- [3] 张朝昆,崔 勇,唐嵩祯,等. 软件定义网络(SDN)研究进展[J]. 软件学报,2015,26(1):62-81.
- [4] 黄 韬,刘 江,魏 亮,等. 软定义网络核心原理与应用实践[M]. 北京:人民邮电出版社,2014:28-32.
- [5] SCOTT-HAYWARD S, O'CALLAGHAN G, SEZER S. SDN security: a survey[C]//IEEE SDN for future networks and services. [s. l.]: IEEE, 2013:1-7.
- [6] RAWAT D B, REDDY S R. Software defined networking architecture, security and energy efficiency: a survey[J]. IEEE Communications Surveys & Tutorials, 2017, 19(1): 325-346.
- [7] SHIN S, GU G. Cloud watcher: network security monitoring using OpenFlow in dynamic cloud networks (or: how to provide security monitoring as a service in clouds?) [C]//20th IEEE international conference on network protocols. Washington DC, USA: IEEE Computer Society, 2012:1-6.
- [8] CHUNG C J, KHATKAR P, XING T, et al. NICE: network intrusion detection and countermeasure selection in virtual network systems[J]. IEEE Transactions Dependable and Secure Computing, 2013, 10(4): 198-211.
- [9] SHIN S, PORRAS P, YEGNESWARAN V, et al. FRESCO: modular composable security services for software-defined networks[C]//Network and distributed system security symposium. [s. l.]: [s. n.], 2013.
- [10] SHERWOOD R, GIBB G, YAP K, et al. Flowvisor: a network virtualization layer [EB/OL]. 2009. <http://OpenFlowSwitch.org/downloads/technicalreports/openflow-tr-2009-1-flowvisor.pdf>.
- [11] 王蒙蒙,刘建伟,陈 杰,等. 软件定义网络:安全模型、机制及研究进展[J]. 软件学报,2016,27(4):969-992.
- [12] 孙冬冬,杨龙祥. 基于软件定义的未来网络节能算法[J]. 计算机技术与发展,2017,27(3):70-74.
- [13] 左青云,张海栗. 基于 OpenFlow 的 SDN 网络安全分析与研究[J]. 信息安全,2015(2):26-32.
- [14] PORRAS P, SHIN S, YEGNESWARAN V. A security enforcement kernel for OpenFlow networks[C]//Proceedings of the first workshop on hot topics in software defined networks. New York, NY, USA: ACM, 2012:121-126.
- [15] PORRAS P, CHEUNG S, FONG M, et al. Securing the software-defined network control layer[C]//Annual network and distributed system security symposium. [s. l.]: [s. n.], 2015.
- [16] BRAGA R, MOTA E, PASSITO A. Lightweight DDoS flooding attack detection using NOX/OpenFlow [C]//Proceedings of the 2010 IEEE 35th conference on local computer. Washington, DC, USA: IEEE Computer Society, 2010: 408-415.
- [17] SHIN S, YEGNESWARAN V, PORRAS P, et al. AVANT-GUARD: scalable and vigilant switch flow management in software-defined networks[C]//Proceedings of the 2013 ACM SIGSAC conference on computer & communications security. New York, NY, USA: ACM, 2013:413-424.
- [18] REITBLATT M, FOSTER N, REXFORD J, et al. Consistent updates for software-defined networks: change you can believe in[C]//Proceedings of the 10th ACM workshop on hot topics in networks. New York, NY, USA: ACM, 2011.
- [19] REITBLATT M, FOSTER N, REXFORD J, et al. Abstractions for network update[C]//Proceedings of the ACM SIGCOMM 2012 conference on applications, technologies, architectures, and protocols for computer communication. New York, NY, USA: ACM, 2012:323-334.
- [20] WEN X, CHEN Y, HU C, et al. Towards a secure controller platform for OpenFlow applications[C]//Proceedings of the second ACM SIGCOMM workshop on hot topics in software defined networking. New York, NY, USA: ACM, 2013:171-172.
- [21] 于 洋,王之梁,毕 军,等. 软件定义网络中北向接口语言综述[J]. 软件学报,2016,27(4):993-1008.
- [22] 孙茂鑫,钱红燕. SDN 网络环境下的 MPTCP 的移动切换机制[J]. 计算机技术与发展,2016,26(6):11-15.