doi:10.3969/j.issn.1003-3106.2016.04.04
引用格式:邵延峰,贾 哲.软件定义网络安全技术研究[J].无线电工程,2016,46(4):13-17.

软件定义网络安全技术研究

邵延峰[1],贾 哲[2]
(1.中国电子科技集团公司第五十四研究所,河北 石家庄 050081;
2.通信网信息传输与分发技术重点实验室,河北 石家庄 050081)

摘 要 随着网络规模的快速扩大及网络业务的多样化,原有的网络架构难以满足未来发展需要。软件定义网络(Software Defined Network,SDN)作为一种新兴技术,实现了控制面与数据面的解耦,能够提供网络的集中控制与流量的灵活调度,将引起通信领域的巨大变革。研究了SDN架构的特点及其面临的安全威胁;针对SDN安全技术研究现状进行了综述;从网络动态防御、软件定义监控和自身安全性增强3个方面提出了SDN安全技术的发展方向。在加强SDN自身安全性的同时提高了网络安全资源的动态调度能力。

关键词 SDN;安全威胁;动态防御;软件定义监控
中图分类号 TN915.02 **文献标志码** A **文章编号** 1003-3106(2016)04-0013-05

Research on Software Defined Network Security Technology

SHAO Yan-feng[1], JIA Zhe[2]
(1. *The 54th Research Institute of CETC, Shijiazhuang Hebei* 050081, *China*;
2. *Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory, Shijiazhuang Hebei* 050081, *China*)

Abstract With the rapid development of network scale and the diversification of network services, the original network structure is difficult to meet the needs of the future development. Software Defined Network (SDN) as a new technology realizes the separation of control plane and data plane, which can provide centralized network controll and the flexible traffic management. This will take place great changes in communication field. This paper firstly analyses the features of SDN architecture and the security threat; then gives a survey on the present development of SDN security; and finally propose the development orientation of SDN security technology including network dynamic defense, software defined monitoring, and security enforcement, which can reinforce the security of SDN, and enhance the dynamic arrangement of security resources.

Key words SDN; security threat; dynamic defense; software defined monitoring

0 引言

SDN[1]将网络设备控制平面与数据平面分离,数据平面专注于数据包的转发处理,控制平面实现对网络的集中控制。用户通过应用平面进行自定义的软件编程,实现了基于“硬件转发+软件应用”的模式,大大提高了网络流量的灵活调度能力、业务的快速部署能力以及运维成本的降低[2],受到了学术界和产业界的广泛关注。Google在2013年宣布[3]其内部骨干网上已实现SDN的全面部署,实现了链路利用率的显著提升。

然而,SDN作为一种新兴技术,其实是一个框架,一个网络设计理念[4],需要考虑利用SDN的相关优势和如何规避它的潜在风险[5]。SDN采用集中控制的方式,是否意味着更大的安全风险?SDN架构中是否存在安全问题,可采用哪些安全防护手段等问题亟待解决。本文对SDN架构的各层进行了安全威胁分析,对基于SDN的网络动态防御、软件定义监控和SDN自身安全性增强等技术进行了研究,提出了软件定义网络安全技术的发展方向。

1 软件定义网络架构及安全威胁分析

软件定义网络的思想[6]起源于斯坦福大学的Clean State项目,通过把原有封闭的体系解耦为数据平面、控制平面和应用平面,提供了一种可编程的

收稿日期:2016-01-20
基金项目:国家高技术研究发展计划(“863”计划)基金资助项目(2015AA015701)。

网络实现，从而将革命性地改变现有网络架构，成为未来网络发展的新方向。

SDN 架构及安全威胁分析如图 1 所示，包括数据平面、控制平面和应用平面。通过控制平面和数据平面的解耦，SDN 从基础的网络设备中剥离了控制平面，并将控制平面的工作转移给一个集中式、可编程的软件控制器，从而简化了底层硬件的复杂度。SDN 定义了统一的控制层面与数据层面接口，抽象了底层硬件，从而屏蔽了底层硬件的区别。上层应用可以通过软件控制器提供的 API 操作底层设备从而控制整个网络，由于软件控制器的数量远远小于传统网络中网络设备的数量，配置和检查工作均被大大简化；另外，由于软件控制器一般由第三方实现，使得控制平面脱离了硬件厂商的限制，修改和添加新特性只需在软件控制器上修改或者添加应用即可，相比于传统网络简单很多。

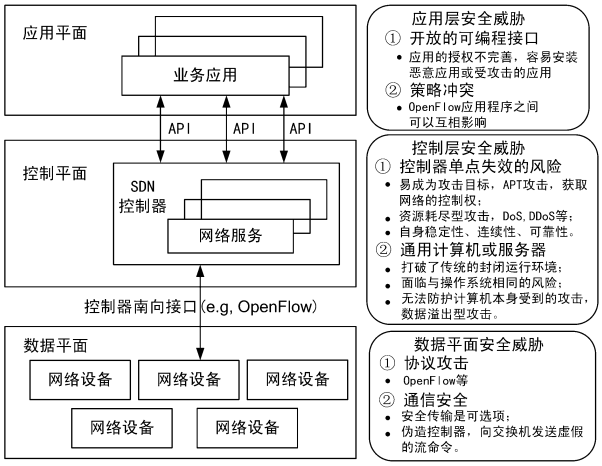

图 1　SDN 架构及安全威胁分析

虽然 SDN 为网络引进了控制面和数据层分离，具有简化底层硬件实现、简化网络配置过程以及向上层应用提供网络全局视图等优点，但是，作为一个尚在起步阶段的体系结构，SDN 是一把双刃剑，在简化网络管理、缩短创新周期的同时，也引入了不可低估的安全威胁。

1.1　控制层安全威胁

管理集中性使得网络配置、网络服务访问控制和网络安全服务部署等都集中于 SDN 控制器上。SDN 的集中式控制方式，使得控制器存在单点失效的风险[7]。首先，控制器的集中控制方式，容易成为攻击目标，攻击者一旦成功实施了对控制器的攻击，将造成网络服务的大面积瘫痪，影响控制器覆盖的整个网络范围；其次，集中控制方式使得控制器容易受到资源耗尽型攻击，如 DoS、DDoS 等；同时，开放性使得 SDN 控制器需要谨慎评估开放的接口，以防止攻击者利用某些接口进行网络监听、网络攻击等。此外，控制器的自身安全性、可靠性也尤为关键。

由于 SDN 的控制器通常部署在通用计算机或服务器上，打破了传统的封闭运行环境。因此，SDN 控制器面临与操作系统相同的风险，且也无法防护攻击者针对计算机本身发起的攻击，如数据溢出型攻击。

1.2　应用层安全威胁

SDN 架构通过 SDN 控制器给应用层提供大量的可编程接口，该层面上的开放性可能会带来接口的滥用，由于现有的对应用的授权机制不完善，容易安装恶意应用或安装受攻击的应用，使得攻击者利用开放接口实施对网络控制器的攻击；其次，缺乏对各种应用的策略冲突检测机制，OpenFlow 应用程序之间下发的流量策略可以互相影响，从而导致恶意应用对已有的安全防护策略产生影响。

1.3　基础设施层安全威胁

SDN 标准组织定义了控制面和数据面的标准接口协议 OpenFlow，有可能受到攻击者发起的协议攻击；同时，由于 OpenFlow 协议中，安全传输方式为可选项，在普通的传输模式下，攻击者能够伪造控制器或者篡改策略信息，向交换机发送虚假的流命令。

2　软件定义网络安全技术研究成果

2009 年，SDN 入围 Technology Review 十大前沿技术。随着 SDN 研究的深入和厂商的大量参与，SDN 的安全问题越来越受到重视。

2.1　国外研究成果

在 2015 年 ITU 标准大会中，SDN 安全方面标准建议主要分为 2 类：基于 SDN 的安全（Security by SDN）和 SDN 自身安全（Security of SDN）。

2.1.1　基于 SDN 的安全技术研究

① 德克萨斯州 Texas 大学和 SRI 公司的研究团队针对 SDN 的安全进行了研究，提出了多种安全解决方案。其中，CloudWatcher[8] 是一种云环境中基于 SDN 控制平台执行安全监控的方法。该方法通过一种新的策略语言，控制器可以直接监控指定设备之间的流量，还可以自动将云环境中的虚拟机迁移流量及其他动态事件的流量转发到其他网络位置，如入侵防御系统（IDS）。同时，该团队还提出一个面向 SDN 安全用例的新开发框架 FRESCO[9]。

这个框架的脚本功能允许安全人员创建新的模块化库，整合和扩展安全功能，从而使用 OpenFlow 控制器和硬件进行控制和管理流量，在 SDN 网络中快速实现和部署多个通用网络安全功能，从而替代防火墙、IDS 和流量管理工具。

② Radware 公司基于 SDN 技术开发了一套可以防止拒绝服务攻击的软件 DefenseFlow™，能够帮助网络运营者通过网络编程以纯网络服务的形式，为客户提供自动的 DoS 以及 DDoS 检测和防护。该技术充分利用控制器的数据搜集功能，对流量分布进行检测，从而实现对攻击行为的发现。

③ 微软宣布了它在内部使用了一种自行开发且基于 OpenFlow 的网络分流聚合平台(称为分布式以太网监控，DEMON)，可用于处理微软云网络的大规模流量。通过使用可编程的灵活交换机和其他网络设备，让它们作为数据包拦截和重定向平台，安全团队就可以检测和防御目前的各种常见攻击。

④ 文献[10]描述了采用 OpenFlow 探测 DDoS 攻击的方法，该方法通过自组织映射实现流量模式的分类从而实现恶意流量的发现。

⑤ 文献[11]提出了一种采用 OpenFlow 实现网络移动目标防御的系统，该系统将内部主机的 IP 地址呈现频繁变化，从而增加外部网络探测和攻击的难度。

2.1.2 SDN 自身安全技术研究

① 德克萨斯州 Texas 大学和 SRI 公司的研究团队在 SDN 安全研究方面，提出了 SDN 安全操作系统 FortNOX[12]。这是一个由美军研究中心(Army Research Center)资助的项目，能够为 Openflow 控制器提供基于角色授权和安全限制这 2 种安全增强措施。

② 斯坦福大学博士 Martin Casado 和其研究团队提出了 Ethane 架构[13]，该架构通过一个中央控制器向基于流的以太网交换机下发策略，从而对流的准入和路由器进行统一管理。在 Ethane 中，主机入网和用户入网都需要通过主机认证和用户认证过程，集中式控制器建立起服务、用户、主机、IP 地址、MAC 地址以及交换机端口的绑定关系。

③ 在 Openflow 协议安全性研究方面，文献[14－15]分别针对 OpenFlow 协议的脆弱性及安全性进行了分析。

2.2 国内研究现状

国内对 SDN 的研究主要集中在 SDN 的体系架构方面，典型的项目包括 2012 年国家 863 项目“未来网络体系结构和创新环境”等。该项目主要由清华大学牵头负责，清华大学、中科院计算所、北邮、东南大学和北京大学等分别负责各课题，项目提出了未来网络体系结构创新环境(Future Internet Innovation Environment，FINE)[16]，并提出一种协作式的新型域间 SDN 互联技术 WE-Bridge[17]。基于 WE-Bridge 建立了首个跨洲际的域间 SDN 实验床，不同的试验者通过虚拟化云平台开发新体系和新协议，构建试验所需的特定虚拟网络环境。通过网域操作系统，控制不同开放网络设备实现不同数据平面的需要。

2013 年 4 月底，中国首个大型 SDN 会议—中国 SDN 大会在北京召开，中国电信主导提出在现有网络(NGN)中引入 SDN 的需求和架构研究，已成功立项 S-NICE 标准。中国移动提出了“SDN 在 WLAN 网络上的应用”等课题。三大国内运营商的研究机构都高度重视 SDN 研究，并在部分网络中进行 SDN 组网测试。而华为、阿尔卡特朗讯、爱立信和中兴通讯等厂商纷纷推出针对运营商数据中心和移动核心网的方案，SDN 在电信行业的发展前景广阔。

在 SDN 安全方面，目前国内高等院校和研究机构正在积极跟进研究，包括 SDN 网络安全面临的威胁及挑战，以及 SDN 思想和架构在网络安全方面的应用[18－20]。以华为、中国电信和绿盟等为代表的企业也在投入资源开展 SDN 安全及 SDN 安全应用方面的研究，绿盟提出了分布式的软件定义安全架构(Software-defined Security Architecture，SDSA)[21]，将安全功能从 SDN 控制器解耦到专有的安全控制器和安全 APP，从而提供全局的流调度能力，以实现对各类攻击的抵御。虽然国内一些高校和厂商进行了 SDN 安全机制的探索，但是总体而言还处于起步阶段，仍需进行大量的研究与实践工作。

3 SDN 安全技术发展方向

通过对 SDN 的安全威胁及其安全研究现状进行分析，可以得出 SDN 安全技术主要包括 3 大发展方向：

3.1 基于 SDN 的网络动态防御

基于 SDN 的网络动态防御架构如图 2 所示，就是利用 SDN 集中管控的特性，通过基于通用硬件和

特定软件的重新配置，根据当前网络性能及安全事件制定安全策略，动态调整网络防护措施，淘汰落后的安全防护产品，实现网络安全防护能力的动态调整和重构更新。

同时，通过将安全应用从基础设施中分离出来，可以使得网络安全防护的方法变得更加灵活，在支持现有安全防护能力的同时，能够灵活地、可扩展地部署新的安全应用，提供新的安全防护方法，保障网络安全防护能力的连贯性。

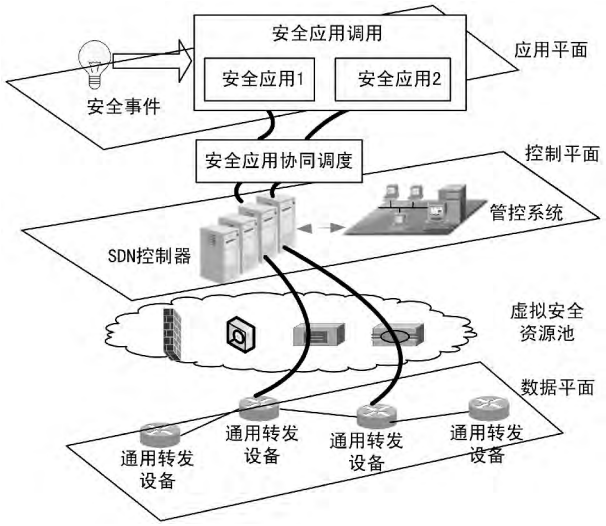

图2 基于 SDN 的网络动态防御架构

3.2 软件定义监控

软件定义监控就是依托 SDN 架构，通过使用可编程交换机和其他网络设备，使其作为数据包拦截或重定向平台，根据网络安全态势将网络流量重定向到安全设备中进行检测和监控，从而实现对全网流量的集中分析，以及对常见攻击的检测，如图 3 所示。

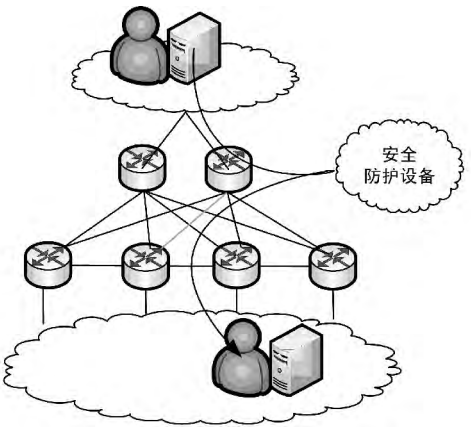

图3 软件定义监控原理

3.3 SDN 自身安全性增强

SDN 自身安全性增强则是针对 SDN 本身的脆弱性进行安全防护能力的增强，从而抵御 SDN 架构带来的安全风险。SDN 架构自身安全防护体系具体研究内容包括：

① 控制器安全增强技术，包括策略冲突检测、控制器安全基线检查、日志分析及事件关联措施等；

② 北向应用认证机制，实现对应用的权限分级及应用的可信认证等；

③ 针对南向接口，针对 OpenFlow 协议，提供协议安全防护功能；并通过采用 SSL/TLS 加密传输机制，保障控制器下发的策略的可靠传输，防止中间人攻击；

④ 控制器采用通用的计算服务器，因此对增强计算服务器本身安全防护能力也是需要考虑的问题。

4 结束语

SDN 体系架构的出现会对通信领域产生巨大变革，但基于其集中控制、开放的应用层等特性，如何实现安全功能的集中管控与灵活调配等问题，成为各研究机构、安全设备厂商等关注的热点。在加强 SDN 自身安全性增强的同时，还应主要在网络动态防御、软件定义监控等方面入手，以提高 SDN 的安全性。

参考文献

[1] Open Networking Foundation. Software-defined Networking: The New Norm for Networks [S], 2012.

[2] 蒋林涛. 软件定义网络为宽带网络创新提供平台 [J]. 世界电信, 2013(5): 20 - 21.

[3] JAIN S, KUMAR A, MANDAL S, et al. B4: Experience With a Globally-deployed Software Defined WAN [C] // China: Proc. of ACM SIGCOMM'13, 2013: 3 - 14.

[4] 张卫峰. 深度解析 SDN 利益、战略、技术、实践 [M]. 北京: 电子工业出版社, 2014.

[5] 赵慧玲. SDN—未来网络演进的重要趋势 [J]. 电信科学, 2012(11): 1 - 5.

[6] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, et al. OpenFlow: Enabling Innovation In Campus Networks [C] // USA: Proc. of ACM SIGCOMM'08, 2008: 69 - 74.

[7] 刁兴玲. SDN 崭新架构下网络安全如何保障 [J]. 通信世界, 2015(1): 33 - 34.

[8] 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] //USA: Proc. of the 20 th IEEE International Conference on Network Protocols (ICNP),2012: 1 - 6.

[9] SHIN S, PORRAS P, YEGNESWARAN V, et al. FRESCO: Modular Composable Security Services for Software-defined Networks [C] //USA: Proc. of NDSS 2012: 1 - 5.

[10] BRAGA R, MOTA M, PASSITO P. Lightweight DDoS Flooding Attack Detection Using NOX/OpenFlow [C] // USA: Proc. of IEEE LCN,2010: 408 - 415.

[11] JAFARIAN J H, AL-SHAER E, DUAN Q. Open Flow Random Host Mutation: Transparent Moving Target Defense Using Software Defined Networking [C] // Finland: Proc. of HotSDN'12,2012: 127 - 132.

[12] PORRAS P, SHIN S, YEGNESWARAN V, et al. A Security Enforcement Kernel For OpenFlow Networks [C] // Finland: Proc. of HotSDN'12,2012: 121 - 126.

[13] CASADO M, FREEDMAN M J, PETTIT J, et al. Ethane: A Logically-centralized Network Architecture for Managing the Security Policies of Enterprise Networks [C] //Japan: Proc. of ACM SIGCOMM'07,2007: 1 - 12.

[14] BENTON K, CAMP L J, SMALL C. OpenFlow Vulnerability Assessment [C] // USA: Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, 2013: 151 - 152.

[15] KLOTI R, KOTRONIS V, SMITH P. OpenFlow: A Security Analysis [C] //Germany: Proc. of IEEE International Conference on Network Protocol,2013: 1 - 6.

[16] 毕 军. SDN 体系结构与未来网络体系结构创新环境 [J]. 电信科学,2013(8): 7 - 15.

[17] 毕 军. 域间 SDN 互联技术 WE - Bridge 及其实验床的研究进展 [J]. 电信科学,2014(8): 28 - 46.

[18] 何 恩,张德治,郝 平. 软件定义网络安全研究 [J]. 通信技术,2014(1): 86 - 90.

[19] 王淑玲,李济汉,张云勇,等. SDN 架构及安全性研究 [J]. 电信科学,2013(3): 117 - 122.

[20] 郭春梅,张如辉,毕学尧. SDN 网络技术及其安全性研究 [J]. 信息网络安全,2012(8): 112 - 114.

[21] 刘文懋,裘晓峰,陈鹏程,等. 面向 SDN 环境的软件定义安全架构 [J]. 计算机科学与探索,2015(1): 63 - 70.

作者简介

邵延峰 男,(1973—),硕士,高级工程师。主要研究方向: 通信网络安全。

贾 哲 女,(1984—),博士,工程师。主要研究方向: 网络安全。

(上接第 8 页)

文章把 WDF 驱动程序技术应用于航天测控系统的数字基带设备,完成了设备驱动程序的设计和实现; 为方便上层应用程序访问基带板卡,设计了基于基带板卡驱动程序的 API 接口模块; 最后开发了测试程序,对 API 接口模块、驱动程序和基带设备集成性能进行测试。

由于受数字基带板硬件条件限制,DMA 数据传输测试使用 20 Mbps 的发送速率。在以后的应用中,随着硬件系统的升级,DMA 数据传输速率能够得到大幅度的提升[11],以更好地满足航天测控发展的需要。

参考文献

[1] 唐 军,谢澍霖. 测通通信系统综合基带设备的发展和应用 [J]. 电讯技术,2001(4): 6 - 9.

[2] 房鸿瑞. 导弹航天测控新技术管窥 [J]. 遥测遥控,2006,36(5): 1 - 8.

[3] 张丽君. 基于 IP 核的 PCI 接口 FPGA 设计实现 [J]. 无线电通信技术,2013,39(1): 91 - 93.

[4] 王兰英,居锦武. Windows 平台驱动程序新架构分析 [J]. 计算机系统应用,2008(1): 109 - 112.

[5] 李正平,徐 超,陈军宁,等. WDF 设备驱动程序的设计与实现 [J]. 计算机技术与发展,2007,17(5): 228 - 230.

[6] 张小磊,孟李林,崔晨琪. 基于 KMDF 的 PCI Express 设备驱动设计 [J]. 西安航空学院学报,2014,32(1): 59 - 63.

[7] 王孝国,王 凌,张雄伟. 高速数据采集系统中的 PCI 中断处理机制和 DMA 编程 [J]. 军事通信技术,2004,25(1): 44 - 47.

[8] 滑 伟. 一种 PCI 总线接口的数据接收卡设计 [J]. 无线电通信技术,2013,39(4): 53 - 55.

[9] 马 进. 数控工业以太网系统设计及驱动程序开发 [D]. 上海: 上海交通大学,2010: 31 - 32.

[10] 信 侃. 基于 Xilinx FPGA 的 PCIe 总线接口设计与实现 [J]. 无线电通信技术,2014,40(4): 94 - 96.

[11] 王 波,郭 建. 基于 PCI 设备的 DMA 传输建模与分析 [J]. 计算机测量与控制,2011(4): 972 - 974.

作者简介

何 帅 男,(1986—),助理工程师。主要研究方向: 航天测控。

王文基 男,(1978—),硕士,工程师。主要研究方向: 武器装备质量控制与监督检验。