doi:10.3969/j.issn.1001-893x.2015.07.002
引用格式:国艳群,韩敏,孙林夫.一种基于SDN的开放SaaS平台网络安全体系设计[J].电讯技术,2015,55(7):718-724.[GUO Yanqun, HAN Min, SUN Linfu. Design of a Network Security Architecture for Open SaaS Platform Based on SDN[J]. Telecommunication Engineering, 2015, 55(7):718-724.]

一种基于SDN的开放SaaS平台网络安全体系设计*

国艳群[1,2],韩 敏[1,**],孙林夫[1]
(1.西南交通大学 信息科学与技术学院,成都 610031;2.西南电子设备研究所,成都 610036)

摘 要:为解决开放软件即服务(SaaS)平台下的网络安全问题,将软件定义网络(SDN)与开放SaaS平台建设相结合,提出了一种基于SDN的开放SaaS平台网络安全体系设计思路。在对系统物理模型、功能模型与协同模型进行分析的基础上,设计了系统体系结构,分析了体系构成关键要素,给出了系统典型应用示例。基于SDN开展SaaS平台网络安全系统建设,对提高系统的安全性与开放性、构建满足用户个性化需求的网络安全体系具有重要意义。

关键词:软件定义网络;软件即服务;网络防护;体系结构设计
中图分类号:TN918.91 **文献标志码**:A **文章编号**:1001-893X(2015)07-0718-07

Design of a Network Security Architecture for Open SaaS Platform Based on SDN

GUO Yanqun[1,2], HAN Min[1], SUN Linfu[1]
(1. School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China;
2. Southwest Institute of Electronic Equipment, Chengdu 610036, China)

Abstract: To solve the network security problem of open software as a service(SaaS) platform, this paper combines the software defined network(SDN) technology and the platform building, and puts forward an idea of building a network security architecture for open SaaS platform based on the SDN devices. According to the analysis of the physical model, the functional model and the cooperation model of the system, the architecture of the system is designed, the key elements of the architecture are analyzed, and then, the typical application of the system is provided. Building the network security system based on SDN has great significance on improving the security and expansibility of network security system and providing the user characteristic security service.

Key words: software defined network; software as a service; network defense; architecture design

1 引 言

开放软件即服务(Software as a Service, SaaS)平台[1-2]是一种开放的云计算体系架构,面向用户提供可动态扩展编程的软件即服务平台。SaaS在具有开放性、动态扩展性等优点的同时,对系统的网络安全防护体系也提出了更高的要求。为提高

* **收稿日期**:2015-06-15;**修回日期**:2015-07-16 Received date:2015-06-15;Revised date:2015-07-16
基金项目:国家科技支撑计划项目(2015BAF32B05);四川省科技支撑计划项目(2015GZ0076)
Foundation Item: The National Key Technology Support Program (2015BAF32B05); The Science and Technology Support Item of Sichuan Province (2015GZ0076)
** **通讯作者**:15908180960@163.com **Corresponding author**:15908180960@163.com

SaaS 平台的安全性,国内外开展了广泛的研究:文献[3]从架构、机制、与模型方面进行了云计算安全体系设计,文献[4-5]从 SaaS 数据安全的角度开展了相关研究工作,文献[6]则对 SaaS 业务流程定制安全技术进行了研究。

软件定义网络(Software Defined Network, SDN)是一种新兴的基于软件的网络技术[7-8],由于其特有的控制平面与数据平面分析、开放的可编程接口以及集中化的控制等特征[9],一经出现,在网络安全及云计算安全领域就引起了广泛关注。文献[10-11]提出了将 SDN 应用于云计算的框架结构,文献[12]对未来网络的体系架构进行了研究并提出将 SDN 应用于网络体系建设的思路。从发展趋势上看,探索基于 SDN 构建网络安全体系并将其应用于云计算平台建设,已成为当前及未来网络安全体系建设的一个重要方向,对提高云计算平台的安全性具有重要意义。然而,从组成的角度看,SDN 设备作为网络交换设备的一种,属于基础设施建设的范畴,对基于 SDN 的应用研究也大多基于 SDN 设备开展相关研究工作,未从应用体系上开展系统性的研究。

本文在框架及应用研究的基础上,利用 SDN 对上提供编程接口的特点,将 SDN 与开放 SaaS 平台安全体系建设需求相结合,从体系建设的角度,自顶向下,对系统安全模型、体系结构进行了研究,对体系建设中涉及到的数据表示与协同、构件管理以及系统构建等关键要素进行了分析,并遵循 SaaS 平台集成标准,对基于 SDN 的网络安全应用进行了封装,使用户可以在不关心底层接口的情况下,按需调用 SaaS 编程接口,实现相应的网络安全功能。该体系兼具 SDN 路由可控、高安全性等特点以及开放 SaaS 平台动态可扩展、需求可定制等优点。遵循系统体系结构,通过系统的持续建设与构件的开放迭代更新,可形成开放 SaaS 平台下动态开放、按需定制的网络安全系统,并实现系统协同预警、协同识别、协同防护以及协同反击等能力的不断提升。

2　系统模型

2.1　物理模型

从构成网络安全系统的物理要素看,基于 SDN 的开放 SaaS 平台网络安全系统由网络服务提供商(Internet Service Provider, ISP)、交换设备(路由器、交换机等)、安全服务中心、SaaS 平台服务器以及应用客户端组成,如图 1 所示。交换设备、安全服务中心、SaaS 平台服务器为体系构成的关键物理要素。从理论上讲,交换设备应全部由支持 SDN 的交换机、路由器等网络设备组成,但在实际应用方面,不可能对所有的网络设备进行升级更换,交换设备在组成上为普通网络设备与 SDN 交换设备的组合,从安全体系构建的角度,可将普通网络设备与互联网络共同等效抽象成透明互联网络,将交换设备狭义定义为分布于互联网络的 SDN 设备(后文所提到的交换设备统一特指具备 SDN 功能的交换设备)。

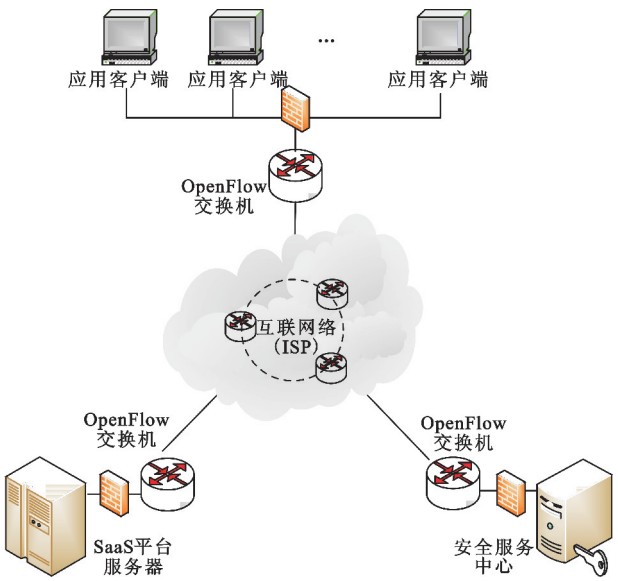

图 1　物理模型
Fig. 1 Physical model

2.2　功能模型

从系统可实现的功能层次,将系统功能分为控制域、功能域与服务域三个功能域。交换设备、控制器及定义的转发规则是控制域的主体,是网络安全体系的物理基础层;基于控制域实现的转发功能,按照典型网络安全系统功能要求,在功能域实现协同预警、协同识别、协同防护以及协同反击等网络防护功能;在服务域,按照面向服务的方式,对功能域安全功能进行封装,同时结合开放 SaaS 平台的功能,向用户提供虚拟网络服务、基础传输服务、网络防护服务以及基于平台的安全编程服务。系统功能模型如图 2 所示。

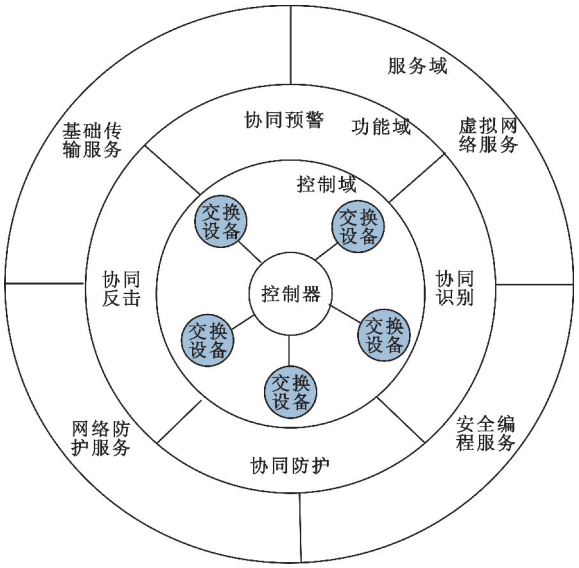

图 2 功能模型
Fig. 2 Functional model

2.3 协同模型

从协同原理的角度,协同过程主要包含了协同群组的建立/解除、信息获取请求、信息发送动作等三部分,对于基于 SDN 的安全体系,发送的信息除网络原始数据外,还包含了元规则信息(即转发规则)。根据以上协同过程,将分布于网络节点的交换设备作为协同对象,由各级安全中心作为发起协同的主题,通过协同原语的方式,对系统进行建模分析,设计了网络管理、数据获取及数据发送三种原语。

2.3.1 网络管理原语

功能:以虚拟方式建立或注销虚拟网络。

语法:NetEstablish(NetID, <sdn-ist>,<net-center>, <purpose-describe>,flag)。

语义:当 flag 为 1 时,建立以 NetID 为唯一标识的分布式虚拟网络群落,sdn-list 为虚拟网络中涉及的 sdn 设备 ID 集合,net-center 为本网络安全中心用户集合,可为一个或多个中心,purpose-describe 为组建本网络的功能描述,可空;当 flag 为-1 时,注销以 NetID 为标识的网络。

2.3.2 数据获取原语

功能:以主动获取的方式,从交换设备获取网络数据。

语法:GetMessage($netcenter_i$, <sdn-set>, <data-character-set>,<time-requirment>)。

语义:$netcenter_i$为采样数据的安全中心的统一编号;sdn-set 为需要提供数据的交换设备集合;data-character-set 为采样数据的样本特征要求,由(sdnid,[关键词$_i$,约束条件$_i$]^n)的约束对组成,其中关键词及其约束规则包括协议、数据前序位置、数据后序位置乃至数据包内关键字等,其形式由系统预先设定,并可根据需要动态进行扩展;time-requirement 为采样的时间要求,为空时代表长期采样。

2.3.3 数据发送原语

功能:交换设备发送网络数据给安全中心。

语法:PutMessage($targetid_i$, message-type, <data-set>)

语义:$targetid_i$代表目标编码,可以为交换设备 id,也可以为安全中心 id;当 message-type 为 0 时代表推送的是网络数据,当 message-type 为 1 时,代表推送的是安全规则;data-set 为推送数据的集合。

3 体系结构设计

3.1 体系框架

基于系统模型,按照面向服务、分层设计的思想,基于 SDN 的开放 SaaS 平台网络安全体系由设备层、控制层、虚拟层、功能层及服务层组成。图 3 是系统体系结构组成,其中设备层为 SDN 交换设备,控制层为支持 SDN 的 Controler 模型,虚拟层为当前流行的网络虚拟化技术。利用 SDN 提供的网络传输、交换控制、虚拟组网等服务,在功能层基于统一的数据描述及数据获取、信息协同共享等基础功能,构建威胁预警、攻击识别、网络防护、定位反击等应用,并在平台层面对各类应用进行服务封装,依托开放 SaaS 平台提供的动态编程服务,为各类用户提供基于平台的体系级网络安全防护。

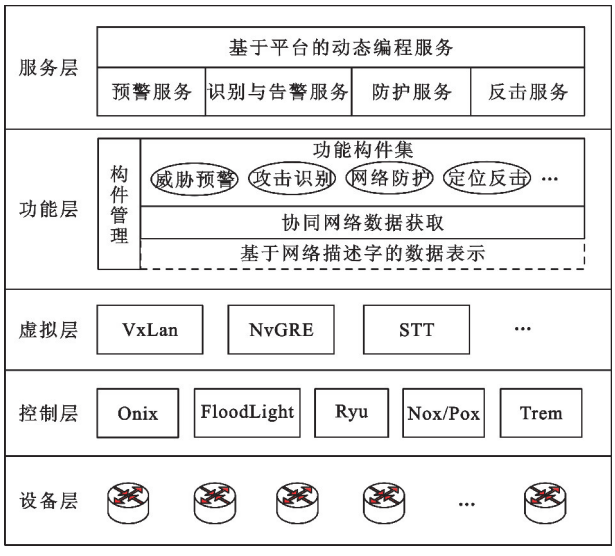

图 3 系统体系结构
Fig. 3 System architecture

3.2　基于网络描述字的信息获取与协同

3.2.1　定义与结构

为便于描述从 SDN 设备获取的数据包信息,定义网络描述字(Net Describe Word,NDW)对其进行描述,可用五元组表示,即 NDW:=(Wid_i,$ProtocalSet_i$,$Area_{vipre-vi-viback}$,T_i,$DataPack_i$),在 NDW 中,包含了该数据包的协议维、区域维、时域维信息,并包含了具体的数据内容,其中:

(1)Wid_i为 NDW 的网络唯一标识;

(2)$ProtocalSet_i$为 NDW 所包含的协议的集合,如 TCP/IP、ICMP 等;

(3)$Area_{vipre-vi-viback}$为数据包的区域位置及上下文信息,其中 vipre、viback 分别为该数据包的前向交换设备节点编号及后向交换设备节点编号;

(4)T_i为该数据包的获取时间;

(5)$DataPack_i$为获取的原始数据包信息,可以是由一个数据包或一组数据包组成。

3.2.2　协同网络数据获取

传统网络安全系统主要在核心入口交换设备节点上部署防火墙与网络预警系统,将收到的可疑数据送往安全中心进行分析,存在安防节点固定、以"点防护"为主的问题,而在本体系中,不需要专门设置防火墙,按照既定的转发规则,每一个 SDN 设备都可以成为一个信息获取设备。全网的 SDN 设备组成协同网络,则可实现网络攻击信息的全网预警与协同数据获取。图 4 为协同网络数据获取的时序示意。

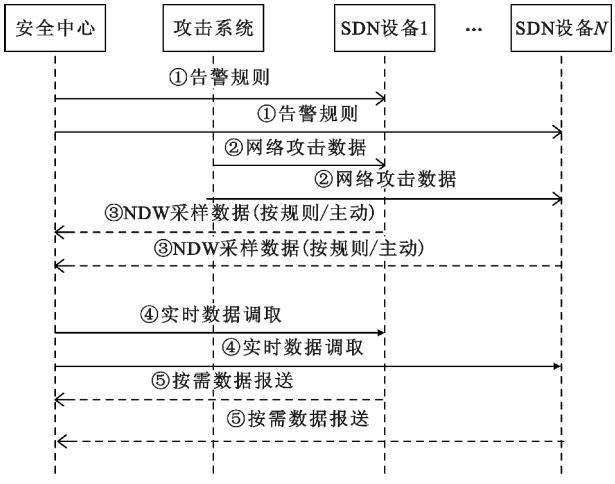

图 4　数据采样时序

Fig. 4 Time sequence of data sampling

从图 4 可以看出,安全中心获取 NDW 的方式主要有以下三种:

(1)按统一规则报送:安全中心利用 PutMessage 原语向 SDN 设备推送告警规则,当出现与告警规则匹配的数据包时 SDN 设备根据告警规则,利用 PutMessage 原语向安全中心推送采样数据;

(2)SDN 设备主动报送:各 SDN 设备根据自身状态,如数据满足本地 Controler 规定的告警规则或出现设备异常等,则利用 PutMessage 原语主动向安全中心推送采样数据;

(3)安全中心按需采样:安全中心根据处理需要,利用 GetMessage 原语向 SDN 设备发送采样需求,SDN 设备收到采样需求后,采集满足需求的数据并利用 PutMessage 原语向安全中心报送。

3.2.3　基于矩阵的数据存储与协同

以网络内交换设备 ID 为行列,在处理中心,可将获取的数据用矩阵表示,矩阵的列代表数据的前序交换设备节点,矩阵的行代表后序交换设备节点,行列的组合即代表的数据的流向及唯一位置信息。矩阵数据表示具有直观、求精及相关运算简便等优点,通过行列运算可实现网络获取数据的快速相关。同时,利用矩阵结构与树形结构易相互转换的特点,可方便地应用于数据包全路径树的获取,对攻击源的跟踪与定位具有重要意义。

以对攻击源定位为例,图 5 是对 1、2、3 号节点对 11 号节点攻击的路径图,将采样数据按照矩阵方式进行描述,如图 6 所示。

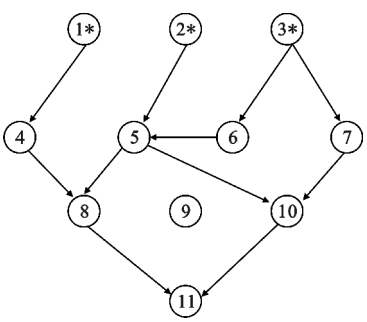

图 5　攻击路径示意图

Fig. 5 Sketch map of attacking routes

	V_1	V_2	V_3	V_4	V_5	V_6	V_7	V_8	V_9	V_{10}	V_{11}
V_1	0	0	0	1	0	0	0	0	0	0	0
V_2	0	0	0	0	1	0	0	0	0	0	0
V_3	0	0	0	0	0	1	1	0	0	0	0
V_4	0	0	0	0	0	0	0	1	0	0	0
V_5	0	0	0	0	0	0	0	1	0	1	0
V_6	0	0	0	0	1	0	0	0	0	0	0
V_7	0	0	0	0	0	0	0	0	0	1	0
V_8	0	0	0	0	0	0	0	0	0	0	1
V_9	0	0	0	0	0	0	0	0	0	0	0
V_{10}	0	0	0	0	0	0	0	0	0	0	1
V_{11}	0	0	0	0	0	0	0	0	0	0	0

图 6　NDW 的矩阵

Fig. 6 Matrix of NDW

依据图 6 所示矩阵,以 11 号被攻击节点作为根节点,按照列对攻击路径进行逐级回朔,即可以 $O(n^2)$ 的时间复杂度生成图 7(左)所示的攻击图。在算法中加入裁剪算法,即可形成攻击树。

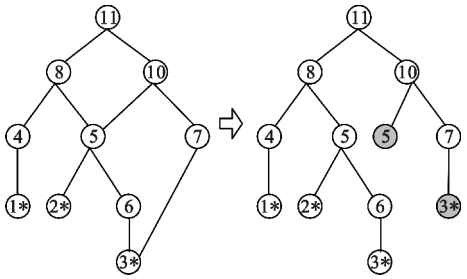

图 7 攻击路径
Fig. 7 Attacking routes

3.3 面向服务的网络防护功能构建

从网络安全应用的角度,典型的网络功能包括威胁预警、攻击识别、网络防护以及定位反击[13]等维度,相应功能的防护系统也主要由以上几类构件组成,虽然采取的技术体制与算法不同[14-16],但在开放 SaaS 平台下,可通过对各种算法的服务化封装,形成开放的构件管理与运行环境,并通过不断的迭代与升级,实现系统防护功能的持续提高。

对网络防护算法进行封装的示意如图 8 所示,从图中可以看出,首先按照统一的平台接口标准,对低层的防护算法进行封装,通过 SaaS 平台构件管理功能,将服务进程实例化,形成可供多用户并发访问的服务资源池。对于访问用户,首先通过数据接口适配,将访问需求转换成满足服务调用的数据接口,通过调用服务实例,实现网络防护功能的服务化访问。

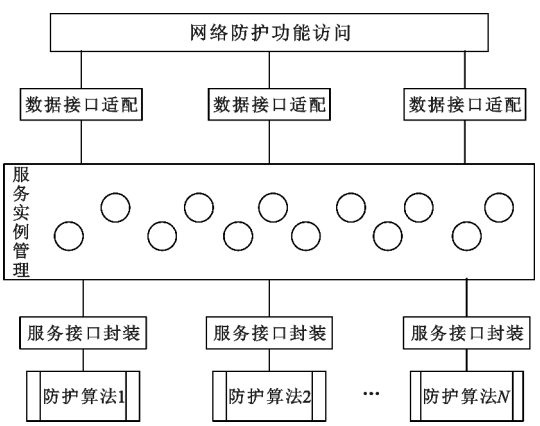

图 8 服务封装示意图
Fig. 8 Sketch map of service encapsulation

3.4 基于平台的动态安全编程

按照开放 SaaS 平台设计思想,系统建设者与使用者均可参与系统开发,其中系统使用者可通过自己开发的方式对系统功能进行个性化定制,并面向其他用户提供个性化服务,安全系统的开发也不例外。为便于维护管理,可将安全构件的开发分为平台级、专业级和应用级 3 类,如图 9 所示,其中:

(1)平台级构件为系统提供基础安全服务,由平台开发者提供并维护;

(2)专业级构件由信息化能力较强的应用者提供(如龙头企业的信息安全部门),在平台级构件提供的安全服务基础上,根据企业需要,开发专业性较强的网络安全构件;

(3)应用级构件利用平台级构件、专业级构件提供的安全服务,通过安全措施组合、安全规则配置等方式,提供应用级安全构件,开发者一般为信息化能力较弱、但又有信息化安全个性化需求的系统使用者,如子公司等。

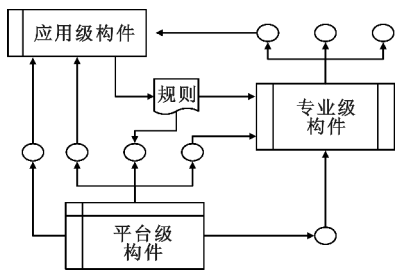

图 9 系统构件组成及接口关系
Fig. 9 Composition and interface relationship of components

4 系统典型应用

图 10 是一个基于 SDN 构建的开放 SaaS 平台网络安全应用示例,不失一般性,对具体的节点名称进行了符号化处理。在实际建设中,在云端由平台开发者建立平台级安全中心,对为全系统提供安全服务,同时依托服务平台,依次构建涵盖企业级、商业级及设备级的网络安全应用平台,各级系统间通过基础网络及 SDN 节点设备互联,形成了物理上无中心分散、逻辑上有中心按需组网的安全防护网络,为系统运行提供体系性防护保障。在系统运行效率方面,从前文网络攻击追踪的分析可以看出,基于 SDN 构建的开放 SaaS 平台应用可利用 SDN 作为定位源,快速对攻击者进行追踪,同样,在系统运行效率方面,由于云计算中心掌握全系统的拓扑状态,可

大幅提高路由收敛时间,并可根据系统状态,制定预先解决方案部署于 SDN 节点,因而,可在提高网络安全性能的同时,以更高的效率实现比传统方式更大规模的网络,对提高系统的效率与扩展性也具有广泛意义。

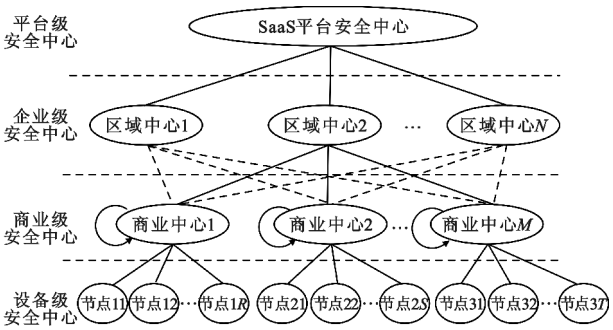

图 10　一个基于 SDN 的开放 SaaS 平台网络安全系统示例

Fig. 10 A sample of open SaaS platform network security system based on SDN

5　结束语

基于 SDN 的开放 SaaS 平台网络安全体系将 SDN 设备“转发与控制分离”、“对上提供编程接口”等特点应用于开放 SaaS 平台的建设,并在国内外研究的基础上,创新性提出了自顶向下基于 SDN 构建 SaaS 安全体系的思路,通过平台封装,使用户在不用了解底层编程接口及复杂网络安全技术的情况下,实现网络安全体系的设计,可满足平台建设对开放性、动态性及高安全性的要求,具备缩短预警时间、提高预警灵敏度、应对复杂攻击威胁等特点。但同时,由于 SDN 与开放 SaaS 都是比较新的技术,如何综合利用现有网络资源进行集成建设,将开放 SaaS 平台安全体系建设与企业现有安全体系相集成,构建统一的开发与集成标准并推广应用,都是亟待解决的问题,也是后续的研究方向。

参考文献:

[1] 国艳群,韩敏,孙林夫. 开放 SaaS 产业服务平台模型与体系结构[J]. 西南交通大学学报,2014,49(6):1068-1072.
GUO Yanqun, HAN Min, SUN Linfu. Research on Model and Architecture of Open SaaS Industry Service Platform [J]. Journal of Southwest Jiaotong University, 2014,49(6): 1068-1072. (in Chinese)

[2] 国艳群,韩敏,孙林夫. 基于开放架构的 SaaS 服务平台数据管理技术研究[J]. 电子科技大学学报,2015,44(2): 295-298.
GUO Yanqun, HAN Min, SUN Linfu. Research on the Data Manage Technology of SaaS Service Platform Based on Open Architecture[J]. Journal of University of Electronic Science and Technology of China, 2015, 44(2): 295-298. (in Chinese)

[3] 林闯,苏文博,孟坤,等. 云计算安全:架构、机制与模型评价[J]. 计算机学报,2013, 36(9):1765-1784.
LIN Chuang, SU Wenbo, MENG Kun, et al. Cloud Computing Security: Architecture , Mechanism and Modeling[J]. Chinese Journal of Computers, 2013, 36(9): 1765-1784. (in Chinese)

[4] 陈静,孙林夫. 基于 SaaS 的产业链写作公共服务平台数据安全解决方案[J]. 计算机集成制造系统,2011, 17(6):1318-1324.
CHEN Jing, SUN Linfu. Solutions of Data Security for Industrial Chain Collaboration Public Service Platform Based on SaaS[J]. Computer Integrated Manufacturing Systems,2011, 17(6): 1318-1324. (in Chinese)

[5] ZHANG Q, CUI D. Enhance the user data privacy for SAAS by separation of data[C]// Proceedings of 2009 International Conference on Information Management, Innovation Management and Industrial Engineering. Washington DC, USA: IEEE, 2009: 130-132.

[6] 曹帅,王淑营. 产业链协同 SaaS 平台业务流程定制安全技术研究[J]. 计算机科学,2014, 41(1): 230-234.
CAO Shuai, WANG Shuying. Research on Security Technology of Workflow Customization for Collaborative SaaS Platform of Industrial Chains [J]. Computer Science, 2014, 41(1): 230-234. (in Chinese)

[7] 邓书华,卢泽斌,罗成程,等. SDN 研究综述[J]. 计算机应用研究,2014,31(11):3208-3212.
DENG Shuhua, LU Zebin, LUO Chengcheng, et al. Outline of Software Defined Networking[J]. Application Research of Computers, 2014,31(11):3208-3212. (in Chinese)

[8] McKeown N, Anderson T, Balakrishnan, et al. OpenFlow: enabling Innovation in Campus Networks [J]. ACM SIGCOMM Computer Communication Review, 2008, 38(2):69-74. (in Chinese)

[9] 雷葆华,王峰,王茜,等. SDN 核心技术解剖和实战指南[M]. 北京:电子工业出版社,2013:2-7.
LEI Baohua, WANG Feng, WANG Qian, et al. SDN Core Technology Anatomy and Actual Combat Manual[M]. Beijing: Electronics Industry Press,2013:2-7. (in Chinese)

[10] Yen T C, Su C S. A SDN-based cloud computing architecture and its mathematical model[C]//Proceedings of 2014 International Conference on Information Science, Electronics and Electrical Engineering. Hokkaido: IEEE, 2014:1728-1731.

[11] Azodolmolky S, Wieder P, Yahyapour R. SDN-Based Cloud Computing Networking[C]//Proceedings of 2013 15th International Conference on Transparent Optical Networks. Cartagena: IEEE, 2013:1-4.

[12] 黄韬,刘江,霍如,等. 未来网络体系架构研究综述[J]. 通信学报,2014, 35(8):184-197.
HUANG Tao, LIU Jiang, HUO Ru, et al. Survey of Research on Future Network Architectures[J]. Journal on Communications,2014,35(8):184-197. (in Chinese)
[13] 周海刚,邱正伦,肖军模,等. 网络主动防御安全模型及体系结构[J]. 解放军理工大学学报(自然科学版),2005, 6(1):40-43.
ZHOU Haigang, QIU Zhenglun, XIAO Junmo, et al. Network Active Defensive Security Model and Architecture [J]. Journal of PLA University of Science and Technology (Natural Science Edition), 2005, 6(1):40-43. (in Chinese)
[14] 张峰,秦志光,刘锦德. 基于入侵事件预测的网络安全预警方法[J]. 计算机科学,2004, 31(11):77-79.
ZHANG Feng, QIN Zhiguang, LIU Jinde. Intrusion Event Based Early Warning Method for Network Security[J]. Computer Science,2004,31(11):77-79. (in Chinese)
[15] 高能,冯登国,向继. 一种基于数据挖掘的拒绝服务攻击检测技术[J]. 计算机学报,2006,29(6):944-951.
GAO Neng, FENG Dengguo, XIANG Ji. A Data-Mining Based DoS Detection Technique[J]. Chinese Journal of Computers,2006,29(6):944-951. (in Chinese)
[16] 田涛,鲁士文. 分布式 DoS 攻击及其反向追踪系统的实现[J]. 计算机应用与软件,2005,22(2):102-104.
TIAN Tao, LU Shiwen. DDos and the Realization of ITS IP Traceback[J]. Compute Application and Software, 2005, 22(2):102-104. (in Chinese)

作者简介:

国艳群(1980—),男,河北衡水人,高级工程师、博士研究生,主要研究方向为系统工程、云计算;

GUO Yanqun was born in Hengshui, Hebei Province, in 1980. He is now a senior engineer and currently working toward the Ph. D. degree. His research concerns systems engineering and cloud computing.

Email:82807578@qq.com.

韩 敏(1970—),女,重庆人,博士,副研究员,主要研究方向为产业链协同和云计算;

HAN Min was born in Chongqing, in 1970. She is now an associate researcher with the Ph. D. degree. Her research concerns industry chain collaboration and cloud computing.

Email:15908180960@163.com

孙林夫(1964—),男,浙江绍兴人,教授、博士生导师,主要研究方向为网络化制造和云计算。

SUN Linfu was born in Shaoxing, Zhejiang Province, in 1964. He is now a professor and also the Ph. D. supervisor. His research concerns networked manufacturing and cloud computing.

更正声明

本刊2014 年第 11 期发表的论文《美军战场频谱管理现状与发展》(doi:10.3969/j.issn.1001-893x.2014.11.024)作者“刘刚”应为“刘钢”。特此更正。

本刊编辑部