SECURITY FOR SOFTWARE-DEFINED (CLOUD, SDN AND NFV) INFRASTRUCTURES – ISSUES AND CHALLENGES

Sara Farahmandian and Doan B Hoang

Faculty of Engineering and Information Technology, School of Computing and Communications, University of Technology Sydney, Australia Sydney
sarah.farahmandian@student.uts.edu.au
Doan.Hoang@uts.edu.au

ABSTRACT

Cloud computing has transformed a large portion of the IT industry through its ability to provision infrastructure resources – computing, networking, storage, and software - as services. Software-Defined Networking (SDN) has transformed the physical underlying network infrastructure into programmable and virtualized networks. Network Functions Virtualization (NFV) has transformed physical telecommunication infrastructures and network functions into virtualised network functions and services. Cloud, SDN and NFV technologies and their associated software-defined infrastructures all rely on the virtualization technology to provision their virtual resources and offer them as services to users. These new technologies and infrastructures invariably bring with them traditional vulnerabilities and introduce new technology-specific security risks. In this paper, we discuss extensively cloud-, SDN-, and NFV-specific security challenges as well as approaches for addressing integrated infrastructural issues where cloud, SDN, and NFV all play their integral parts.

KEYWORDS

Cloud computing, SDN, NFV, virtualization, security challenges, software-defined security, multi-tenancy

1. INTRODUCTION

With a huge increase in the acceptance and usage of cloud computing, the majority of IT services are now being deployed and operated in cloud environments. Cloud computing is a large scalable environment which consists of a large number of physical hosts and virtual machines (VMs) operating and communicating over the cloud network. Each physical server or host may serve as a host to multiple virtual machines by virtue of virtualisation. Since cloud computing supports a multi-tenant environment where each tenant has its own networking requirements based on its clients' demands, one of the challenges of a cloud network is to adapt its network resources dynamically in order to support scalability and maintain real-time configuration while virtual networks are provisioned and migrated dynamically on-demand or virtual machines move from one domain to another. Providing a dynamic and automatic virtual network for cloud multi-tenant

Natarajan Meghanathan et al. (Eds) : NETCOM, NCS, WiMoNe, GRAPH-HOC, SPM, CSEIT - 2016
pp. 13– 24, 2016. © CS & IT-CSCP 2016 DOI : 10.5121/csit.2016.61502

infrastructure is a significant challenge for future of networking architecture. In telecommunication networks, Software-Defined Network (SDN) and Network Function Virtualization (NFV) are two effective technologies with great impact in this area. SDN is based on the separation of the network control from the data forwarding functions, allowing the controller to directly program the underlying infrastructure and present it as a high level, network-functionality abstraction to applications and network services [1]. NFV offers a new approach to design, deploy and manage networking services. It decouples the network functions, such as firewalls, intrusion detection, etc. from proprietary hardware appliances so they can be implemented in software and deployed wherever and whenever needed [2]. Although these new technologies and their associated software-defined infrastructures (Cloud, SDN, and NFV) can solve existing limitations in providing cost effective, on-demand IT services and elastic but scalable network architectures/network services in software-defined, virtualized, multi-tenancy environments, they also present many critical challenges related to both traditional and technology-specific security. This paper presents major security challenges in cloud, SDN and NFV; and solutions for infrastructural security issues. The paper discusses the need for a software-defined security technology for handling software-defined integrated infrastructures and systems. Specifically, in an integrated infrastructure platform such as a data centre or a telecom cloud, where cloud, SDN and NFV functionalities are integrated, the paper discusses the compound security challenges and suggest possible solutions using virtualization technology.

The paper is organized as follows. Section 2 provides essential definitions and characteristics of cloud, SDN, NFV and virtualization technologies. Section 3 presents issues and challenges these technologies are facing. Section 4 presents software-defined security solutions for cloud and SDN. Sections 5 discusses security issues and a software-defined security solution for an integrated infrastructure platform with virtualization technology. The conclusion is in section 6.

2. CLOUD, SDN, NFV AND VIRTUALISATION TECHNOLOGIES

In this section we explain the essential characteristics of cloud computing, SDN, NFV, and Virtualization.

2.1 Cloud Computing

Cloud computing has evolved into a key structure for IT industries for providing users on-demand services. Cloud architecture enables users to access cloud services over the Internet at any time regardless of their location through application software like web browsers. Cloud computing resources such as virtual servers, virtual storage, virtual networks and virtual services, are made available using virtualization technologies. The National Institute of standard and technology (NIST) recently offered an explanation for defining the cloud computing. In this definition, Cloud computing is a computing model that enables omnipresent, convenient and on-demand network access to a shared pool of configurable computing resources such as networks, storages, servers, applications, and services. Cloud computing offers three service models known as Software as a service (SaaS), Platform as a service (PaaS), and Infrastructure as a Service (IaaS) [3].

SaaS model enables users to access their services through a web application but without the ability to control the network infrastructure and operating systems. PaaS model provides a platform for software developers to use application development languages and tools such as java, .net, python and etc. for creating, compiling, designing, running, deploying, and testing their own software applications. IaaS is a form of cloud computing which provides access to computing resources in a virtualized environment. Virtualization is deployed to pool all underlying physical resources together and offer them as virtual resources on-demand and elastically in the form of

IaaS, PaaS, and SaaS [4]. OpenStack is a major open source cloud computing platform that orchestrates and manages shared storage, compute, and network resources using multiple hypervisors based on a set of applications and open-source. OpenStack is used as a cloud framework for creating public and private clouds.

2.2 Network Functions Virtualization (NFV)

Network Function Virtualization (NFV) is proposed recently aiming to virtualize an entire class of network component functions using virtualization technologies. NFV enables network functions to be realized and executed as software instances in a VM on a single or multiple hosts instead of customized hardware appliances. NFV offers a new means for creating, deploying and managing networking services. Network Function Virtualization can be applied to both data and control planes in fixed or mobile infrastructures. NFV provides telecommunication operators the ability to combine numerous different types of network equipment into high volume switches, servers, and storage inside data centres, network nodes, and end user premises. NFV implements network functions using software virtualization methods and performs them on top of underlying hardware equipment. These software-based virtual functions can be installed and deployed flexibly and strategically based on tenants' requirement without the need for new hardware equipment. A hypervisor is responsible for controlling network functions within a supporting NFV infrastructure. NFV technology helps cloud tenants to avoid vendor lock-in problem by allowing them to use multiple virtual appliances from different vendors while using different hardware platforms and/or hypervisors.

In today's market, NFV concentrates on providing four categories of software-based virtual network functions known as Virtual Switching, Virtualized Network Appliance (security functions such as IDS, Firewalls, and etc.), Virtualized Network Services (load balancers, network monitoring tools, traffic analysis tools), and Virtualized Applications (any available application in the network environment) [5]. Enable dynamic deployment of NFV within a networking platform is a big challenge. Traffic of a network function (NF) must be isolated at multiple levels - services, virtual networks and tenants' levels - and hence, a comprehensive controller is required to provide strict multilevel isolation within the NFV Infrastructure. The combination of SDN and NFV can solve these challenges in both dynamic network infrastructure and functionality of an integrated cloud-network environment.

2.3 Software-Defined Systems

Software Defined System (SDSys) is conceived to address control and management challenges which exist in cloud computing. SDSys is a concept that provides an abstraction of actual hardware at different layers based on software components. This type of abstraction enables system administrators to create a centralized decision-making system to handle and monitor all control and management decisions instead of having a decentralized system where each component only manages itself [6]. Among all SDSys subsystems, SDN is the most well-known.

2.4 Software-Defined Network (SDN)

Software-Defined Networking is developed as a technology to remove the current black box network infrastructure restrictions. This is done through the separation of the decision-making functions from the data forwarding functions, allowing them to evolve separately into a centralized and programmable control plane and a simple and high-performance data plane operation respectively [7]. According to [7], Software-Defined Network architecture consists of three layers known as Data Plane, Control Plane, and Application Plane. SDN devices are all placed at Data plane layer. SDN controller (or group of controllers) is located at the control plane

layer, and applications and network services are on the application plane layer. SDN devices simply forward packets according to instructions programmed by the SDN controller. An SDN application, gaining network capability abstraction from the controller, has the ability to determine traffic streams and routes on the network devices to fulfil the requirements responding to user's dynamic requests [7, 8].

The main responsibility of the SDN controller is to program and centrally control SDN devices forwarding behaviours with the support of a comprehensive information database of all underlying network infrastructure operations. The SDN controller uses interfaces for communicating with other layers. To communicate with the data/infrastructure layer, a Southbound Application Interface (API) Interface is used for programming and configuring network devices. To communicate with the application layer a Northbound Interface is provided for the interaction between the SDN controller and applications. East/West Interfaces are for information exchange between multiple or federated controllers. The OpenFlow protocol has been developed and widely adopted as one of the southbound interfaces between SDN controllers and SDN switches. OpenFlow uses a secure channel for message transmission over the transport layer security (TLS) connection.

2.5 Virtualization

Virtualization is the technology that simulates the interface to a physical object by multiplexing, aggregation, or emulation. With multiplexing, it creates multiple objects from one instance of a physical object. With aggregation, it creates one virtual object from multiple physical objects. With emulation, it constructs a virtual object from a different type of physical object.

Virtualization is critical to cloud computing, SDN and NFV as it allows abstraction of the underlying resources for sharing with other tenants, isolating of users in the same cloud/network, and isolation of services and functions running on the same hardware. It also plays an important role in the development and management of services offered by a provider. Virtualization is often introduced as a software abstraction layer placed between operating systems and the underlying hardware (computing, network, and storage) in the form of a hypervisor. In cloud data centres since the hypervisor manages the hardware resources, multiple virtual machines each with its own operating system and applications and network services, can run in parallel within a single hardware device [9]. Virtual technology thus allows multi-tenancy, isolate workloads, enhances server utilization and provides elastic and scalable resources/services to its users.

Virtualization technology has been deployed by enterprises in data centres storage virtualization (NAS, SAN, database), OS virtualization (VMware, Xen), software or application virtualization (Apache Tomcat, JBoss, Oracle App Server, Web Sphere), and Network Virtualization [10]. Virtualization technology enables each cloud tenant to perform its own services, applications, operating systems, and even network configuration in a logical environment without any consideration about physical underlying infrastructure [11]. The technology enables Network Functions Virtualization (NFV) and Software-Defined Network (SDN) the ability to create a scalable, dynamic, and automated programmable virtual network functions and virtual network infrastructures in integrated cloud platform such as telecom clouds.

3. SECURITY ISSUES AND CHALLENGES IN CLOUD, SDN, AND NFV

3.1 Cloud computing security challenges

As a cloud has become a large-scale and complex infrastructural environment, it becomes more vulnerable to both traditional and new security threats related to its structure and elements. NIST

declares security, portability, and interoperability as main obstacles for adopting to cloud environment completely. Some of traditional security issues found in the cloud infrastructure are data access control (illegal access to confidential data), loss and data leakage, trust, isolation. Cloud-specific security issues include insecure interfaces and APIs, malicious insider, account or service hijacking, virtualization security, and service interruption. We discuss these critical and significant security challenges below.

Insecure interfaces and APIs. Cloud providers deliver services to their customers through software interfaces mostly integrated with the web application layer. The stability of cloud components is dependent upon the security level of these APIs within the cloud infrastructure. Insecure cloud APIs can cause various threats related to confidentiality, availability, integrity, and accountability. These API functions and web applications share a number of vulnerabilities which may result in high level security problems. Consequences of any malfunction in APIs may allow malicious codes to be imported inside the cloud and expose user confidential data. Although strong authentication methods, proper access controls, and encryption methods may solve some of the above problems, still, there are serious gaps especially related to the inability of massive auditing and logs. Any APIs that will interact with sensitive data within cloud infrastructure must be protected with a secure channel such as SSL/TLS.

Malicious insider. This type of threats is one of the most serious cloud-specific security challenges according to the Cloud Security Alliance (CSA) cloud security threat list. It happens when an employee of cloud service providers (CSPs) abuses his/her level of access to gain confidential information of cloud customers for any nefarious purposes. The worst case is when a malicious system administrator has access to client resources hosted on virtual machines and data stores. So detecting such indirect accesses to client data is one of challenging tasks in cloud infrastructure.

Account or service hijacking. It is a kind of identity theft that aims to deceive end-users to obtain their sensitive data. If an attacker gains control of a user account it can snoop on all customer's activities, manipulate and steal their data, or redirect the customer into inappropriate sites. This kind of threats can be accomplished through phishing email, faux pop-up windows, spoofed emails, buffer overflow attacks which result in the loss of control of the user's account.

Virtualization security. Since virtualization is a crucial technology in cloud infrastructure, any vulnerability can place the whole system in a high-security breach. For example, any error and vulnerability inside the hypervisor can allow an attacker to launch VMs attacks (shutting down VMs) or monitor others VMs and their shared resources. A compromised VM can inform an attacker of the underlying network operation for exploitation of existing network vulnerabilities. It also enables an adversary to compromise the hypervisor and achieve control over the whole system. Local users and malicious codes can bypass security boundaries or even gain privileges to cause damages to the infrastructure and its users through vulnerabilities found in virtualization software.

Service interruption. It is a vital security issue in cloud computing since everything in the cloud is defined as service. Service interruption is placed in the category of threats related to the availability of cloud services. DDoS attack is usually attempted against Internet services with large population of users and it is more so against cloud as a centre of high number of cloud services and users. These attacks may render services and computing resources unavailable. A DDoS attack may occur when an attacker gains access to tenant's VMs credentials due their vulnerabilities.

3.2 NFV Security Challenges

Most critical security challenges in NFV are related to network function generator/hypervisor, security of virtual functions, performance isolation, communication and functional/service interfaces, multiple administrative isolation, and secure crash of virtual network functions.

Hypervisor security. The main security issue in virtualized environments and especially NFV is related to hypervisor vulnerabilities. A hypervisor creates VMs inside the infrastructure and has the ability to monitor each VM's operating system. According the European Telecommunications Standards Institute (ESTI), this feature introduces high security risk to NFV in terms of Confidentially, Integrity and Availability (CIA). It may allow an attacker to view, inject, or modify operational state information connected with NFV in direct/indirect method and as a result the attacker is able to read/write contents of resources such as memory, storage, and other components of NFV. Hypervisor hijacking is a type of attacks that allow an adversary to take control of a hypervisor and access all VMs created by that particular hypervisor, or other less insecure hypervisors inside the infrastructure. In the worst case it may even introduce misconfigurations in SDN controllers when integrated with NFV technology. Furthermore, existing errors or bugs inside a virtual function or a hypervisor may allow an attacker to compromise other virtualized network functions for more serious attacks.

Virtual network function security. Virtual network functions encounter attacks common to those on physical network functions such as sniffing, denial of service, and spoofing. Insider attacks are possible on virtual network functions when a malicious administrator, who has a specific access right, gains access through other virtual functions within the infrastructure. Insider attacks can modify data in network equipment and introduce unauthorized configuration of network functions. In a public deployment of NFV it is possible for a malicious third-party or remote client to gain access through the network to control the VNFs. A malicious or compromised virtual network function inside the NFV infrastructure can monitor activities of other virtual functions or even send fraudulent instructions through the hypervisor to disrupt their operations.

Performance Isolation. Lack of inappropriate isolation among virtual functions can cause data leakage similar to the way a VM can access through another VM data (VM-to-VM attack). Performance isolation is one of many specific security concerns in NFV infrastructure. A proper virtualization technology has to isolate VMs from one another to ensure that crashes, hangs, loops, or compromises in one VM do not affect others, however, VMs isolation is difficult to achieve due to variable usage of resources and workloads among them. According to the ESTI, network and I/O partitioning and shared core partitioning are two major issues in performance isolation. Isolating network workload from other functions is a difficult task since it can be placed over various distributed network resources and can be dynamically changed at any point in time, particularly when numerous virtual functions in the NFV Infrastructure (NFVI) share resources [12]. Lack of complete isolation can be exploited by an adversary to gain information about a compromised victim. Insufficient isolation mechanism may allow cross virtual network side-channel attacks that threaten VNFs hosted in a NFV shared infrastructure. It is possible that a side-channel attack can bypass compulsory access controls to violate resource isolation.

Communication and functional/service interfaces. New security threats associated with new interfaces present other critical challenges related to interconnectivity between NFV end-to-end components, such as communication between VNF components, communication between VNF and VNF manager, communication between VNF and NFVI, and communication between VNFs. NFV encompasses different types of network and security functions, so defining standard interfaces for different security functions is one of the security challenges in a virtualized network infrastructure. Each tenant may have different security services with different user authentication

methods, privilege control schemes, and network configurations. So the way a network function communicates with one another and other tenants' functions through a standard interface is a huge challenge in NFV technology. Currently, there is no standard communication interfaces in NFV technology.

Multiple administrative isolation. It is an NFV security challenge related to the existence of multiple administrative domains in the same platform. Multiple administrator domains imply different administrator privilege domains for network, hypervisor, storage, compute, NFV orchestration, VFNM (Virtual Function Network Manager), and network services running in the platform. Requirements for an administrative role for each of the above domains are different and involve various levels of policies. Security is even more critical when there are virtualization infrastructure administrator roles with higher privileges than the administrator of existing virtualized function within the NFVI.

Secure crash of virtual network functions. Components crash in any infrastructure and system can cause security problems and in virtual environment the impact is more severe. According to the ETSI, a crash of any virtualized function within NFVI can bring about critical security issues which allow attackers to gain access to information through existing insecure data on that particular component [12]. It is so critical that a VNF component should be reinstalled securely after a crash. It should be noted that many important components in the NFV framework might be at high risk states during a crash; these include VNF component instances, network and storage resources attached to virtual network functions. Availability of services is also will be affected due to a function crash [12].

3.3 SDN Security Challenges

As with other new technologies, SDN suffers from both existing security threats in traditional networks and new challenges due to SDN architecture. Since SDN uses virtualization technology to virtualize networks (VNs), it inherits traditional security problems related to the virtualization of virtual machines as well as new security issues related to the virtualization of network hypervisors and their isolation. It also suffers threats such as Dos/DDoS attack, with higher impact because of the centralized architecture of SDN control. SDN introduces new and critical security challenges due to its architecture, including security of SDN controllers, forwarding plane security issues, unauthorized access, routing policy collision, fraudulent flow rules insertion or tampering in switching level, insecure interfaces, and system level SDN security challenges.

SDN controllers. Since SDN controller is a core element in the SDN architecture; if it is compromised the whole system is placed in a high risk of failure. The majority of security challenges related to SDN controller are around the vulnerabilities at the controller plane where an attacker can get hold of the control function to compromise integrity, confidentiality, and availability of SDN [13]. Since SDN decouples the data plane from the control plane, it is the responsibility of centralized controller to deal with all incoming network flows. As a consequence, the controller itself is a key bottleneck and is the target for various attacks such as flooding and DDoS attacks. An SDN controller can be implemented in a virtual or physical server with associated resources. An attacker can launch a kind of resource consumption attack on the controller to render it unavailable in response to flow rules coming from underlying switches and force it to respond extremely slowly to packet-in events or sending packet-out messages. A DoS/DDoS attack is one of the most serious security threats against SDN controller when an attacker endlessly sends IP packets with different headers to the controller to put it in the nonresponsive state.

Forwarding plane security issues. There are two specific security challenges in the forwarding plane of SDN architecture. The first and most critical issue is related to identifying genuine flow rules from malicious or fake rules within the infrastructure where the SDN controller is responsible for all decision making functions. A compromised controller can simply transmit false flow rules within underlying virtual network elements. The second security challenge is that it in vulnerable to saturation attack [14] due to the limited storage capacity for flow rule entries in flow tables of SDN OpenFlow switches.

Unauthorized access. A critical security challenge in SDN is related to unauthorized access in an SDN architecture- unauthorized access through the SDN controller or unauthorized access through the applications- where a large number of third-party applications operate. One of the serious security breaches in SDN is when an authorized SDN component accesses SDN services or controller without having the appropriate level of access and modifies network data or reprograms the SDN controller components [15].

Routing policy collision. Policy collision is another specific security challenge in SDN architecture when various vendors and third party applications using different configurations and programming models. This is critical since a malicious component can delete, insert, or modify existing and predefined policies of flows inside the SDN controller. Separate servers or application with different policy rules may result in policy conflict with each other.

Fraudulent flow rules insertion or tampering in switching level. A compromised or malicious application can generate fraud flow rules while communicating with the controller. An attacker can inject fake flow rules through the switches by exploiting vulnerabilities of southbound interfaces. It is possible for attacker to tamper with network information by modifying flows in flow tables. These malicious flow rules can cause network to behave abnormally. For instance, [16] introduced an attack in which an attacker generates forged link layer discovery protocol (LLDP) packets through an OpenFlow network to create vulnerabilities on internal links between two switches. An adversary can also insert malicious flow rules by monitoring the traffic from OpenFlow Switches.

Insecure interfaces. Another critical security challenge in SDN infrastructure is related to insecure Application Programming Interfaces (APIs): Northbound, Southbound, and East and West Interfaces. This security issue is critical since all communications between the SDN controller and the application layer, the underlying forwarding layer, or even the communication between multiple controllers, go through these interfaces. For instance, vulnerabilities and the lack of standard protocol in northbound interface may enable attackers to interfere with the operation of both the application and the controller and send malicious request through the controller or network elements or even generate flooding attack with purpose of disrupting its operation. An adversary is also capable of sending a large number of requests through the northbound interface to occupy the interface bandwidth. In a multi-domain multi-controller environment, controller's communication goes through the East/West APIs. These SDN controllers may be from different vendors and do not have a common secure channel between them. Message among them may be sniffed by an attacker through vulnerabilities of East-West APIs and sensitive information may be exposed.

System level SDN security challenges. A specific SDN system level security concerns auditing processes. As it is essential to keep comprehensive state information of network devices in the infrastructure to prevent unauthorized access, providing an auditing and accountability mechanism in SDN is a critical security challenges [15].

4. RECENT SOFTWARE-DEFINED SECURITY SOLUTIONS FOR CLOUD AND SDN

In this section we discuss and tabulate a number of software-defined security solutions for SDN and cloud infrastructures. As SDN and NFV are relative new technologies, infrastructures based on them are still being adopted and developed, security issues are being explored and discovered. Currently, only a limited number of solutions exists. Most of them adopt the logically centralized control paradigm of SDN in building software-defined security solutions. Several efforts are described below.

[17] proposed a Software Defined Security Architecture (SDSA) that has the ability to separate security controls from security executions, improves scalability and security of systems and decreases the costs of software developments. The authors provided two structures (Physical and Logical) for the architecture to allow both business logical providers and security developers to only work within their scope of expertise without concern about the design and implementation of security structures or development of business logic programs.

[18] proposed a framework for protecting network resources via SDN-based security services using an Interface to Network Security Functions (I2NSF). The aim was to create a self-governed protection system against network attacks, capable of providing rapid responses to new threats.

In [19], a comprehensive security architecture was proposed to deliver a range of security services including enforcing mandatory network policies, packet data scan detection, transforming network policies into flow entries, authentication, and authorization for solving security challenges related to policy enforcement and attack detection for SDN architecture.

[20] proposed an architecture for enhancing network security using network monitor and SDN control as separated functions. The OrchSec architecture adopts the separation principle of SDN by decoupling of monitoring and control functions. This allows flexible and more comprehensive and intelligent control over security functionality and activities and also reduces overhead on SDN controller.

The table 1 provide a summary of other recent efforts in providing software-defined security solutions for cloud and SDN.

5. SECURITY ISSUES AND CHALLENGES IN AN INTEGRATED CLOUD-SDN-NFV INFRASTRUCTURE PLATFORM

Cloud computing demonstrated how best computing and storage resources can be virtualised and provisioned on demand and offered as IT services. More importantly, its effective orchestration of services offers an excellent model for resources and service management. SDN and NFV demonstrated most effective way network resources and services (network infrastructures, network functions, and connectivity services) can be created and managed. Cloud needs SDN and NFV to be integrated seamlessly to be able to offer truly any resource as a service. SDN and NFV need to include cloud management infrastructure to offer network services and functionality. For example, existing telecommunications network infrastructures and service models are too rigid and they have to evolve into a form of telecom cloud to be able to offer emerging and flexible services to its customers. An integrated software-defined infrastructure that seamlessly integrates cloud, SDN and NFV will certainly create a powerful service model that incorporates all the best features of these technologies.

Two major issues concerning cloud, SDN, NFV and the integrated software-defined infrastructures are the security of the virtualization technology itself and the complexity of the virtualized interconnecting infrastructure. Cloud and SDN networks are facing an increasing complexity of emerging social networks, applications and services and their associated security problems. The whole range of problems include scalability of cloud networks, the complexity of the way network function communicates to each other, the lack of a centralized infrastructure control component, policy enforcement, dynamic workloads, multi-tenancy, isolation of tenants, services, resources (virtual networks, virtual machines, virtual storage). SDN and NFV allow tenants to share the underlying physical network to create their own virtual networks, network functions and services with their policy in a cloud environment. Integrating cloud, SDN and NFV into a software-defined infrastructure provides a truly scalable, dynamic, and automatic programmable platform for creating *everything as a service* on demand.

All these infrastructures rely on virtualization as the core technology. Virtualization is pervasive in almost all components of the service infrastructures: virtual machines, virtual networks, virtual storage, virtual network functions, and virtual services. Virtualization, however, brings with it new security challenges in the way virtual elements are created and maintained. For the security of the infrastructure, all virtual elements have to be secure for their whole lifecycle; their creators (hypervisors) must be trusted and secure; appropriate isolation among servers, among services, and among tenants must be preserved.

Clearly, although integration of cloud, SDN, and NFV into a truly service infrastructure provides is beneficial to both service providers and service users, the complexity of security of each technology, of virtual components, of individual infrastructures present a major obstacle for a comprehensive integration. One important aspect of virtualization is that it introduces boundaries that are invisible to traditional security mechanisms at various levels. In order to deal with this integrated software-defined infrastructure, one should use the very virtualization technology to provide security of the overall infrastructure; one should deploy the logically centralized paradigm of SDN and NFV to separate security control from functionality of security network functions. We suggest Software-Defined Security (SDSec) in that spirit to create a centralized security infrastructure for the cloud-SDN-NFV infrastructure platform. SDSec provides a centralized security controller over the infrastructure. The SDSec controller will possess the ability to create its own flexible interconnecting infrastructure for connecting its security function elements. It will have the ability to program and manage its security function elements autonomously. Security function elements are both virtual and physical: networks, and security functions. However, there are many open questions on how best to secure a software-defined integrated infrastructure related to all the security issues and challenged discussed in previous sections.

6. CONCLUSION

Cloud computing has been most effective in orchestrating and provisioning IT resources and offer them as on-demand services. SDN and NFV are most effective in provisioning network infrastructures and network services. Seamlessly integrated, these provide a most powerful software-defined infrastructure to provision *everything as a service*. The main obstacle is the security of the underlying virtualization technologies and their virtualized resources. This paper discussed at length specific security issues and challenges concerning cloud, SDN, and NFV. The paper discussed the need for a software-defined security technology and software-defined control paradigm to handle software-defined integrated infrastructures and systems.

Table 1. Proposed Security solution for SDN

Security solution methods	Year	purpose	Target Layers		
			APP	Controller	Data
SDSA: A Software-Defined Security Architecture	2016	• Separate security control from a security operation • Divide middleware from security programming interface for enabling programmable services • Deliver on-demand security components for software developers	✓	✓	✓
SDN-based security services using an Interface to Network Security Functions (I2NSF)	2015	• Propose centralized firewall system and DDoS attack mitigation mechanism	✓	✓	✓
A comprehensive security architecture for SDN	2015	• Deliver security services like enforcing mandatory network policies, packet data scan detection, transforming network policies into flow entries, authentication, authorization		✓	✓
SDN-based architecture for analyzing network traffic in clouds	2015	• Provide collaboration between the cloud control plane and SDN controller • Proposed traffic monitoring		✓	✓
SDSecurity	2015	• Provide an experimental security framework by using SDN		✓	✓
FLOWGUARD	2014	• Build a robust firewall in SDN • Provide accurate detection and high resolution of firewall policy violation by real-time monitoring		✓	✓
Building firewall over the software-defined network controller	2014	• Generate an adequate logic and a proper user interface for creating firewall inside the SDN		✓	
AuthFlow: Authentication and Access Control Mechanism for SDN	2014	• Create a host authentication system • Develop access control based on host privilege using a credential-based authentication • Provide SDN controller ability to control applications with each host identification as a new entry	✓	✓	
OrchSec	2014	• Reduce overhead on SDN controller by the decoupling of monitoring and control function • Provide flexibility and ability to detect different types of attacks	✓	✓	
CLOUDWATCHER	2012	• Provide security monitoring service for dynamic and scalable cloud networks using SDN	✓	✓	

REFERENCES

[1] A. Manzalini and N. Crespi, "SDN and NFV for Network Cloud Computing: A Universal Operating System for SD Infrastructures," in Network Cloud Computing and Applications (NCCA), 2015 IEEE Fourth Symposium on, 2015, pp. 1-6.

[2] L. R. Battula, "Network security function virtualization (NSFV) towards cloud computing with NFV over Openflow infrastructure: Challenges and novel approaches," in Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on, 2014, pp. 1622-1628.

[3] C. Rong, S. T. Nguyen, and M. G. Jaatun, "Beyond lightning: A survey on security challenges in cloud computing," Computers & Electrical Engineering, vol. 39, pp. 47-54, 2013.

[4] M. Yang and H. Zhou, "New Solution for Isolation of Multi-tenant in cloud computing," 2015.

[5] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," IEEE Communications Surveys & Tutorials, vol. 18, pp. 236-262, 2015.

[6] Y. Jararweh, M. Al-Ayyoub, E. Benkhelifa, M. Vouk, and A. Rindos, "Software defined cloud: Survey, system and evaluation," Future Generation Computer Systems, vol. 58, pp. 56-74, 2016.

[7] D. Hoang, "Software Defined Networking–Shaping up for the next disruptive step?," Australian Journal of Telecommunications and the Digital Economy, vol. 3, 2015.

[8] K. Govindarajan, K. C. Meng, and H. Ong, "A literature review on Software-Defined Networking (SDN) research topics, challenges and solutions," in Advanced Computing (ICoAC), 2013 Fifth International Conference on, 2013, pp. 293-299.

[9] J. Sahoo, S. Mohapatra, and R. Lath, "Virtualization: A survey on concepts, taxonomy and associated security issues," in Computer and Network Technology (ICCNT), 2010 Second International Conference on, 2010, pp. 222-226.

[10] Y. Xing and Y. Zhan, "Virtualization and cloud computing," in Future Wireless Networks and Information Systems, ed: Springer, 2012, pp. 305-312.

[11] C.-J. Chung, "SDN-based Proactive Defense Mechanism in a Cloud System," ARIZONA STATE UNIVERSITY, 2015.

[12] N. F. V. NFV, "Draft ETSI GS NFV-SEC 001 V0. 2.1 (2014-06)," 2013.

[13] A. Feghali, R. Kilany, and M. Chamoun, "SDN security problems and solutions analysis," in Protocol Engineering (ICPE) and International Conference on New Technologies of Distributed Systems (NTDS), 2015 International Conference on, 2015, pp. 1-5.

[14] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," IEEE Communications Surveys & Tutorials, vol. 17, pp. 2317-2346, 2015.

[15] S. Scott-Hayward, S. Natarajan, and S. Sezer, "A survey of security in software defined networks," IEEE Communications Surveys & Tutorials, vol. 18, pp. 623-654, 2015.

[16] S. Hong, L. Xu, H. Wang, and G. Gu, "Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures," in NDSS, 2015.

[17] L. Yanbing, L. Xingyu, J. Yi, and X. Yunpeng, "SDSA: A framework of a software-defined security architecture," China Communications, vol. 13, pp. 178-188, 2016.

[18] J. Kim, M. Daghmehchi Firoozjaei, J. P. Jeong, H. Kim, and J.-S. Park, "SDN-based security services using interface to network security functions," in Information and Communication Technology Convergence (ICTC), 2015 International Conference on, 2015, pp. 526-529.

[19] Z. Hu, M. Wang, X. Yan, Y. Yin, and Z. Luo, "A comprehensive security architecture for SDN," in Intelligence in Next Generation Networks (ICIN), 2015 18th International Conference on, 2015, pp. 30-37.

[20] A. Zaalouk, R. Khondoker, R. Marx, and K. Bayarou, "Orchsec: An orchestrator-based architecture for enhancing network-security using network monitoring and sdn control functions," in 2014 IEEE Network Operations and Management Symposium (NOMS), 2014, pp. 1-9.