A Survey on Security in Network Functions Virtualization

Wei Yang and Carol Fung
Department of Computer Science
Virginia Commonwealth University
Email: {yangw3, cfung}@vcu.edu

***Abstract*—Network functions virtualization (NFV) is an emerging network technology. Instead of deploying hardware equipments for each network functions, virtualized network functions in NFV are realized through virtual machines (VMs) running various software on top of industry standard high volume servers or cloud computing infrastructure. NFV decreases hardware equipment costs and energy consumption, improves operational efficiency and optimizes network configuration. However, potential security issues is a major concern of NFV. In this paper, we survey the challenges and opportunities in NFV security. We describe the NFV architecture design and some potential NFV security issues and challenges. We also present existing NFV security solutions and products. We also survey NFV security use cases and explore promising research directions in this area.**

***Index Terms*—Network functions virtualization, NFV, security.**

I. Introduction

In modern days, with the increasing diversity and data rates from users, Telecommunications Service Providers (TSPs) must correspondingly and continuously purchase, store and operate new physical equipment. It leads to high expenditure costs for TSPs. Network Functions Virtualization (NFV) [1], [2] was proposed as a new technology to design, deploy and manage networking services with much lower costs, through decoupling physical network equipment from the functions that run on them. More specifically, NFV utilizes virtualization technologies to provide network functions (NFs) through running software on industry standard high volume servers, switches and storage [3]. The main contribution of NFV is to realize software-based NFs such as virtualized firewalls and virtualized gateways, instead of hardware appliances.

Compared to traditional network architectures, NFV has the following advantages [4]: (1) reduced equipment costs, (2) improved operating performance and operational efficiency, (3) optimized network configuration and resource allocation, (4) flexible network function deployment and dynamic operation, and (5) reduced energy consumption. However, NFV may contain various security issues. For example, components in NFV architectural framework, such as hypervisors and orchestrators, may be vulnerable to potential security threats. The shared storage and networking may introduce new security vulnerabilities [1]. Furthermore, hypervisors, hardware and VNFs are likely to be offered by different vendors, thus resulting in integration complexity and generating security loop-holes [4].

978-1-4673-9486-4/16/$31.00 © 2016 IEEE

Various approaches have been proposed to address the security problems in NFV [5], [6], [7], [8]. For example, NFV ISG provides guidances to ensure security in NFV's external operational environment and presents related technologies to supply security and trust for NFV [9], [10]. Alcatel-Lucent described existing security threats in NFV and introduced the corresponding mitigation methods. Huawei pointed out that providing effective security monitoring to discover threats and mitigate attacks was highly important [11].

This survey paper specially focuses on the security aspect of NFV. More specifically, the goals of this survey are to provide detailed information about security issues in NFV, introduce the latest development trends and newest research outcomes in NFV security, and provide users with guidances and methods to assure security in NFV. The survey consists of the following parts: (i) a survey of security problems in NFV and corresponding solutions; (ii) proposed security architectures for NFV; (iii) overview of commercial products designed for NFV security; and (iv) a prediction of future research challenges and directions in NFV security.

II. A Brief Overview of NFV

The first white paper on NFV was published in October 2012 soon after the foundation of the NFV ISG. Nowadays, NFV ISG has developed to over 270 companies containing 38 service providers and greatly forwarded the development of NFV. The first NFV ISG output documents were released in October 2013 to provide guidances on the industry progress on NFV. A call for Proof of Concept (PoC) was launched to build an open ecosystem for NFV, and 38 PoC projects have been conducted by NFV ISG since then.

As shown in Fig. 1, NFV architectural framework includes multiple functional components such as NFV Management and Orchestrator, NFVI (Network Function Virtualization Infrastructure), VNF (Virtualized Network Functions), EMS (Element Management System), and OSS/BSS (Operations/Business Support System). Components interact with each other through reference points [12], [13]. Containing both hardware and software components, NFV infrastructure (NFVI) can be used to support various use cases, such as virtualization of mobile core network, virtualization of home environment, and virtualization of content delivery networks

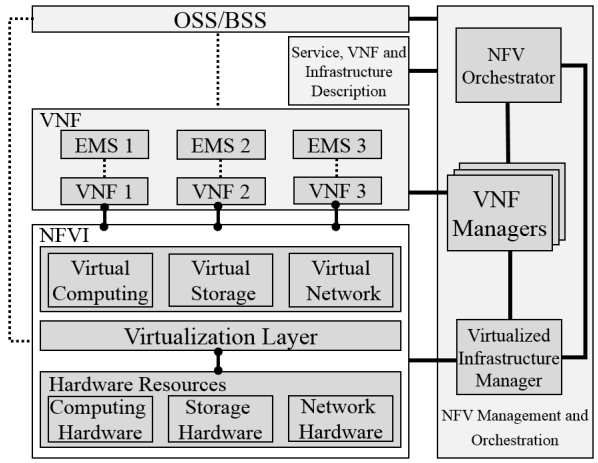

Fig. 1. NFV architectural framework.

[14]. A VNF runs over the NFVI and an EMS is used to manage it. NFV Management and Orchestration covers three functional blocks: NFV Orchestrator, VNF Managers, and Virtualized Infrastructure Manager. NFV Management and Orchestration performs the orchestration and lifecycle management of NFVI resources and VNFs [15]. The Service, VNF and Infrastructure Description component drives the whole NFV system.

The implementation of NFV faces a few major challenges. For example, how to manage and orchestrate all virtual resources and how to integrate the virtual resources so they are compatible with existing platforms. The implementation requirements are addressed by the NFV virtualization requirements document [16]. To guarantee the service availability and maintain resiliency in NFV, automated recovery from failures should be enabled [17]. Some related open source projects have made contributions to the growth of NFV, for example, OpenDaylight [18] and OpenStack [19], [20]. Open Platform for NFV (OPNFV) aims at developing open source projects to overcome the implementation challenges faced by NFV [21].

There has been a rapidly increasing interest in NFV. Current NFV trending research topics include secure, reliable, energy-efficient NFV architectures, and performance optimization for NFV. There are many use cases for NFV, such as virtualization of mobile core network and IMS, virtualization of home and enterprise networks, virtualization of content delivery networks, and fixed access NFV [14]. Cloud computing and industry standard high volume servers contribute to the realization of NFV.

Software Defined Networking (SDN) is another approach that aims at improving networking flexibility by separating the forwarding function and routing function into different planes. NFV and SDN are highly complementary at building a software-based solution to networking for more scalable, agile, and innovative networks, but they are different from each other. For example, SDN enables automated operations, flexible policy control and effective security management on all NFV resources, and NFV generates reliability and elasticity in SDN by implementing SDN controller as a VNF running on a virtual machine. Greater benefits can be achieved by combining NFV and SDN [22], [23], [24].

III. Security Challenges and solutions for NFV

NFV brings great opportunities such as reduced cost and less operational influence. However, there are challenges accompanying opportunities [25], [26]. Underlying areas of concern in NFV security include user/tenant authentication and authorization [9]. Security in NFV is discussed in [10] under three situations: security inside VNFs, security between VNFs, and security outside VNFs. Security and software management are the major challenges to NFV [11]. How to overcome the security problems from hypervisor, data communication, and APIs remains a challenge for applying NFV into telecommunication networks and mobile networks [4].

A. Security challenges from NFV infrastructure

Compute domain, hypervisor domain, and network domain constitute the NFV infrastructure (NFVI). The compute domain includes the generic servers and storage, the hypervisor domain moves the resources from the hardware to the virtual machines, and the network domain manages the VNFs. NFVI suffers from both internal and external security threats. Internal threats result from inappropriate operations of people and it can be avoided by following strict operational procedures. External threats exist because of design or implementation vulnerabilities. To solve this problem, the NFVI devices should have a security certification process to eliminate possible threats. The security of the NFVI should be ensured by the NFV framework. In addition, NFVI should adopt standard security mechanisms for authentication, authorization, encryption and validation [27], [28], [29]. Table I shows the security challenges and corresponding solutions to the three domains in NFVI. The security issues of NFVI can be caused by the lack of security evaluation for NFVIs, and the integration and the interoperability among different software can also raise security concerns. Table II compares the different fault injection technologies that can be used to test the robustness of virtual machine and cloud technologies. We can see that through fault injections the virtual systems may encounter failures such as memory corruptions and API exceptions.

B. Security challenges from standard interface definition

Defining standard interfaces for various security functions is a big challenge when implementing security services in a virtualized network platform. Different security services can be developed on the basis of users' demands through the standard interfaces. For example, user authentication, user privilege control, and network configuration can be predefined before using these security functions [35]. The predefined virtualized network security functions can be used in access networks [36], mobile networks [37], data center [38], SDN [39], and NFV [40].

C. Security challenges from management and orchestration

Keeney, et al. [41] discussed the security challenges in managing and orchestrating VNFs when using NFV for mobile

TABLE I
NFV INFRASTRUCTURE SECURITY CHALLENGES AND SOLUTIONS [4]

	Security challenges	**Solutions**
Hypervisor domain	1. Unauthorized access. 2. Data leakage.	Virtual machines are only available to authentication controls.
Compute domain	Shared computing resources: 1. CPU. 2. Memory.	Data should be encrypted and accessed only by the VNFs.
Network domain	1. Shared logical networking layer (virtual switches). 2. Shared physical network interface controllers.	Secure networking techniques should be adopted, such as TLS, IPSec, and SSH.

TABLE II
COMPARISION OF FAULT INJECTION METHODS [2]

Method	**Used tool**	**Target**	**Fault injection technology**
Fault injection testing of virtual machines	D-Cloud [30]; DS-Bench Toolset [31]	Server software	Simulation of faulty devices; Virtual machine memory corruption
Fault injection testing of cloud management software	PreFail [32]; OpenStack [33]	Filesystems and algorithms	API exception injection
Fault injection testing of hypervisors	CloudVal [34]	Hypervisors	Memory corruption

telecommunications networks. They indicate that monitoring and managing the NFVI and VNFs for security reason is a challenge since NFVI and VNFs are much more complex and dynamic in the virtualized environment. Security issues also exist in the management of VNFs, such as managing and maintaining consistent configurations of VNFs, and seamlessly transfering the state information from one VNF to another.

D. Security challenges from elasticity of NFV

In spite of the great potentials of NFV, the security, privacy, and trust remain problems to be addressed. Szabo, et al.[42] identified the challenges on dynamic service scaling and elasticity of NFV. The emphasized challenges are from: (1) decomposing services for data plane and control plane, (2) enforcing policies and virtualizing resources for control functions, and (3) managing and controlling the whole network. To ensure the security in NFV during the NFV setup progress, the elasticity control signals should go through some trusted functional blocks such as NFV Orchestrator, VNF Managers, and Virtualized Infrastructure Manager.

IV. PROPOSED SECURITY PLATOFRMS FOR NFV

Many security platforms and architectures have been proposed and implemented to assure security in NFV. In this section, we overview some proposed platforms and products for NFV security from the industry.

A. Introduction of Policy Manager to NFV

Basile, et al. [43] proposed a framework to apply security policy management to NFV. In the framework, a new software component called Policy Manager is added to the NFV architecture as shown in Fig. 2. Security policies can be defined by users through the high-level policies (HLP) language and medium-level policies (MLP) language. First, the Policy Manager generates the needed configurations to meet the security requirements from users. Then the configurations are sent by the orchestrator to configure different VNFs and achieve the desired security VNFs. Integrating the Policy Manager with the NFV architecture allows users to specify their security requirements in a flexible, effective and convenient way.

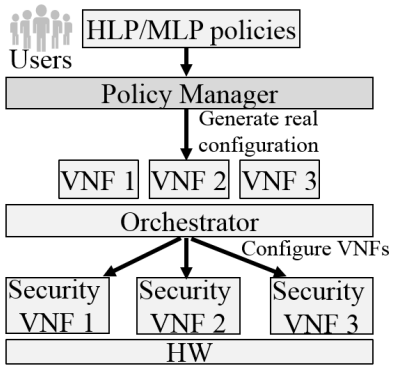

Fig. 2. NFV architecture with an additional Policy Manager.

B. A User-Centric Approach

Montero, et al. [8] introduced a user-centric model to protect users' securities in NFV. In the model, the security is ensured by a trusted virtual domain located in the access network. An architecture named SECURED is presented to afford a safe environment for providing secure applications for users. Main components of the SECURED architecture include security module, authentication system, security policy manager, and SECURED app. These security related components work together to provide security and trust in NFV.

C. OpenNF

OpenNF [5] is designed as a control plane architecture to provide efficient and safe allocation of data flows across network function instances in NFV. OpenNF provides efficient, coordinated control of both internal network function state and network forwarding state. It overcomes the existing challenges for secure NFs control: it addresses the race conditions problem, bounds the overheads, and uses the least changes to accommodate many different VNFs. OpenNF aims at providing security and flexibility for VNFs control in NFV with minimum overheads.

D. Cisco Evolved Services Platform

Cisco Evolved Services Platform (CESP) was introduced as a secure and low cost NFV solution in 2014 [44]. Fig. 3 provides the overview of the CESP. The Service Broker

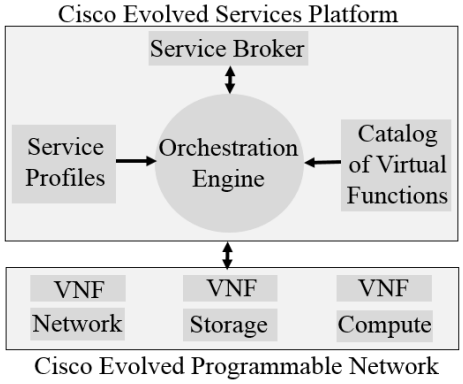

Fig. 3. Cisco Evolved Services Platform.

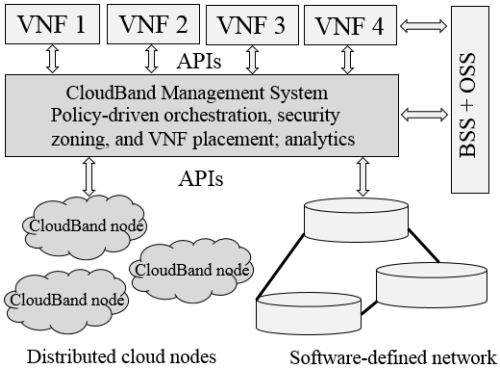

Fig. 4. Alcatel-Lucent CloudBand.

connects services orchestration and business logic to assure efficient and secure service delivery. The Service Profiles include different service attributes and policies to enable secure and dynamic delivery of personalized services. The Catalog of Virtual Functions defines available VNFs and services to customers. The employment of OpenStack [45] to the open architecture makes the Catalog of Virtual Functions extensible, which allows more VNFs and services to be added into the NFV solutions [46], [47].

E. Alcatel-Lucent CloudBand

In 2014, Alcatel-Lucent developed a secure NFV platform called CloudBand [48], which is presented in Fig. 4. The framework of CloudBand includes a centralized CloudBand management system and multiple distributed CloudBand nodes [49], [50]. To provide secure VNFs, the CloudBand management system manages and orchestrates resources in the NFVI, and affords processing and analysis for historical and real-time data, such as anomaly detection and event prediction [51].

F. VMware vCloud NFV

VCloud NFV was developed by VMware in 2015 to cope with increased service agility and security. Fig. 5 represents the architecture of the VMware vCloud NFV platform. The VMware vCloud Director for Service Providers allows secure Communication Service Providers (CSPs) commercial-scale deployments. The VMware Integrated OpenStack is responsible for QoS and placement of VMs, it guarantees the performances of VNFs and makes the OpenStack clouds

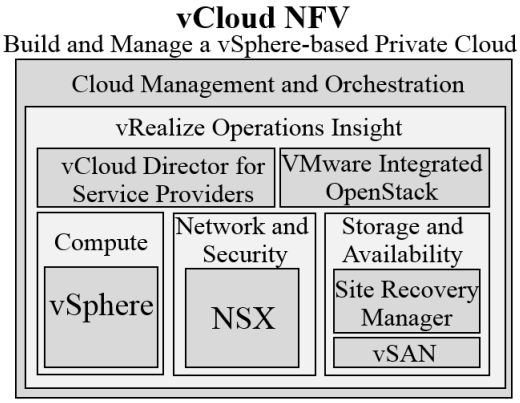

Fig. 5. VMware vCloud NFV platform.

more scalable, secure and resilient. The VMware vRealize Operations Insight assures network functions and services for multiple tenants. VMware NSX realizes the benefits of NFV and VMware Sight Recovery Manager enables disaster recovery and business continuity [52].

V. Future challenges in NFV security

Although many solutions have been proposed to overcome the security challenges in NFV, many potential security challenges remain. In this section, we discuss some of the research challenges and future directions for NFV security.

1) Compromised VNF: In a NFV network, hardware and software are likely to be provided by different vendors to prevent from large scale security failure. However, the likelihood of one or few services to be compromised increases. How to detect compromised components and mitigate their impact remains a challenge.

2) Distributed Denial-of-service attacks: Distributed Denial of service attacks (DDoS) can cause tremendous damage to NFV supported network if not handled properly. NFV provide new opportunity for TSPs to launch new defending strategy against DDoS attacks. How to utilize the flexibility of VNF to defend against DDoS attacks in the network is another challenge.

3) Trust management in NFV: The merge of NFV provides opportunities for various vendors to enter the networking infrastructure market by providing NFV compatible hardware and software. It will be common to have multiple vendors involved in a NFV supported network. However, how to manage the trust chain and evaluate the trustworthiness of products is another research challenge. Also how to adaptively configure VNFs by choosing software to minimize security risk of the network is another research topic.

VI. Conclusions

NFV reduces equipment costs and improves operational efficiency. However, security remains an obstacle to overcome for the rapid development of NFV. In this survey, we introduce the background of NFV and highlight the NFV security issues. We summarize the NFV security challenges and provide corresponding solutions to address the security problems. Some

proposed security architectures for NFV are described to form secure NFV environments. Finally we present various use cases of NFV security and discussed future challenges of NFV.

REFERENCES

[1] B. Han, V. Gopalakrishnan, L. S. Ji, and S. J. Lee, "Network Function Virtualization: Challenges and Opportunities for Innovations," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 90–97, Feb. 2015.

[2] D. Cotroneo, L. De Simone, A. K. Iannillo, A. Lanzaro, R. Natella, F. Jiang, and P. Wang, "Network Function Virtualization: Challenges and Directions for Reliability Assurance," in *ISSREW*, Nov. 2014.

[3] ETSI NFV ISG, "Network Functions Virtualization Introductory White Paper: An Introduction, Benefits, Enablers, Challenges & Call for Action," in *SDN and OpenFlow World Congress*, Oct. 2012.

[4] H. Hawilo, A. Shami, M. Mirahmadi, and R. Asal, "NFV: State of the Art, Challenges, and Implementation in Next Generation Mobile Networks (vEPC)," *IEEE Network*, vol. 28, no. 6, pp. 18–26, 2014.

[5] A. Gember-Jacobson, R. Viswanathan, C. Prakash, R. Grandl, J. Khalid, S. Das, and A. Akella, "OpenNF: Enabling Innovation in Network Function Control," in *SIGCOMM '14*, Aug. 2014, pp. 163–174.

[6] J. Soares, C. Goncalves, B. Parreira, P. Tavares, J. Carapinha, J. P. Barraca, R. L. Aguiar, and S. Sargento, "Toward a Telco Cloud Environment for Service Functions," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 98–106, Feb. 2015.

[7] W. Ding, W. Qi, J. Wang, and B. Chen, "OpenSCaaS: An Open Service Chain as a Service Platform Toward the Integration of SDN and NFV," *IEEE Network*, vol. 29, no. 3, pp. 30–35, May/Jun. 2015.

[8] D. Montero, M. Yannuzzi, A. Shaw, L. Jacquin, A. Pastor, R. Serral-Gracia, A. Lioy, F. Risso, C. Basile, R. Sassu, M. Nemirovsky, F. Ciaccia, M. Georgiades, S. Charalambides, J. Kuusijarvi, and F. Bosco, "Virtualized Security at the Network Edge: A User-Centric Approach," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 176–186, Apr. 2015.

[9] "ETSI Group Specification: Network Functions Virtualization (NFV) NFV Security Problem Statement," Oct. 2014.

[10] "ETSI Group Specification: Network Functions Virtualization (NFV) NFV Security and Trust Guidance," Dec. 2014.

[11] Huawei White Paper, "Observation to NFV," Nov. 2014.

[12] "ETSI Group Specification: Network Functions Virtualization (NFV) Architectural Framework," Dec. 2014.

[13] "ETSI Group Specification: Network Functions Virtualization (NFV) Infrastructure Overview," Jan. 2015.

[14] "ETSI Group Specification: Network Functions Virtualization (NFV) Use Cases," Oct. 2013.

[15] "ETSI Group Specification: Network Functions Virtualization (NFV) Management and Orchestration," Dec. 2014.

[16] "ETSI Group Specification: Network Functions Virtualization (NFV) Virtualization Requirements," Oct. 2013.

[17] "ETSI Group Specification: Network Functions Virtualization (NFV) Resiliency Requirements," Jan. 2015.

[18] J.-L. Izquierdo-Zaragoza, A. Fernandez-Gambin, J.-J. Pedreno-Manresa, and P. Pavon-Marino, "Leveraging Net2Plan planning tool for network orchestration in OpenDaylight," in *SaCoNeT*, Jun. 2014.

[19] S. Ristov, M. Gusev, and A. Donevski, "Security Vulnerability Assessment of OpenStack Cloud," in *CICSyN*, May 2014.

[20] A. Mayoral, R. Vilalta, R. Munoz, R. Casellas, R. Martinez, and J. Vilchez, "Integrated IT and network orchestration using OpenStack, OpenDaylight and active stateful PCE for intra and inter data center connectivity," in *ECOC*, Sep. 2014.

[21] https://www.opnfv.org/.

[22] J. Matias, J. Garay, N. Toledo, J. Unzilla, and E. Jacob, "Toward an SDN-Enabled NFV Architecture," *IEEE Communications Magazine*, vol. 53, no. 4, pp. 187–193, Apr. 2015.

[23] R. Cannistra, B. Carle, M. Johnson, J. Kapadia, Z. Meath, M. Miller, D. Young, C. Decusatis, T. Bundy, G. Zussman, K. Bergman, A. Carranza, C. Sher-DeCusatis, A. Pletch, and R. Ransom, "Enabling autonomic provisioning in SDN cloud networks with NFV service chaining," in *OFC*, Mar. 2014.

[24] G.-Y. Liu and T. Wood, "Cloud-Scale Application Performance Monitoring with SDN and NFV," in *IC2E*, Mar. 2015.

[25] C. C. Liang and F. R. Yu, "Wireless Network Virtualization: A Survey, Some Research Issues and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 1, pp. 358–380, Aug. 2015.

[26] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. D. Turck, and R. Boutaba, "Network Function Virtualization: State-of-the-art and Research Challenges," *IEEE Communications Surveys & Tutorials*, no. 99, DOI: 10.1109/COMST.2015.2477041.

[27] "ETSI Group Specification: Network Functions Virtualization (NFV) Infrastructure Compute Domain," Dec. 2014.

[28] "ETSI Group Specification: Network Functions Virtualization (NFV) Infrastructure Hypervisor Domain," Jan. 2015.

[29] "ETSI Group Specification: Network Functions Virtualization (NFV) Infrastructure Network Domain," Dec. 2014.

[30] T. Banzai, H. Koizumi, R. Kanbayashi, T. Imada, T. Hanawa, and M. Sato, "D-Cloud: Design of a Software Testing Environment for Reliable Distributed Systems Using Cloud Computing Technology," in *10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing (CCGrid)*, May 2010, pp. 631–636.

[31] H. Fujita, Y. Matsuno, T. Hanawa, M. Sato, S. Kato, and Y. Ishikawa, "DS-Bench Toolset: Tools for Dependability Benchmarking with Simulation and Assurance," in *42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Jun. 2012, pp. 1–8.

[32] P. Joshi, H. S. Gunawi, and K. Sen, "PREFAIL: A Programmable Tool for Multiple-Failure Injection," in *2011 ACM international conference on Object oriented programming systems languages and applications (OOPSLA '11)*, Oct. 2011, pp. 171–188.

[33] X. Ju, L. Soares, K. G. Shin, K. D. Ryu, and D. D. Silva, "On Fault Resilience of OpenStack," in *4th annual Symposium on Cloud Computing (SOCC '13)*, Oct. 2013, pp. 1–16.

[34] C. Pham, D. Chen, Z. Kalbarczyk, and R. K. Iyer, "CloudVal: A Framework for Validation of Virtualization Environment in Cloud Infrastructure," in *IEEE/IFIP 41st International Conference on Dependable Systems & Networks (DSN)*, Jun. 2011, pp. 189–196.

[35] H.-S. Jang, J.-H. Jeong, H.-S. Kim, and J.-S. Park, "A Survey on Interfaces to Network Security Functions in Network Virtualization," in *WAINA*, Mar. 2015.

[36] A. Pastor and D. Lopez, "Access Use Cases for an Open OAM Interface to Virtualized Security Services," Oct. 2014.

[37] K. Wang and X. Zhuang, "Integrated Security with Access Network Use Case," Feb. 2015.

[38] M. Zarny, S. Magee, N. Leymann, and L. Dunbar, "I2NSF Data Center Use Cases," Oct. 2014.

[39] J. H. Jeong, J. H. Seo, G. H. Cho, H. S. Kim, and J.-S. Park, "A Framework for Security Services Based on Software-Defined Networking," in *WAINA*, Mar. 2015.

[40] C. Price and S. Rivera, "OPNFV: An Open Platform to Accelerate NFV," Oct. 2012.

[41] J. Keeney, S. van der Meer, and L. Fallon, "Towards Real-time Management of Virtualized Telecommunication Networks," in *CNSM*, Nov. 2014.

[42] R. Szabo, M. Kind, F.-J. Westphal, H. Woesner, D. Jocha, and A. Csaszar, "Elastic Network Functions: Opportunities and Challenges," *IEEE Network*, vol. 29, no. 3, pp. 15–21, May/Jun. 2015.

[43] C. Basile, A. Lioy, C. Pitscheider, F. Valenza, and M. Vallini, "A novel approach for integrating security policy enforcement with dynamic network virtualization," in *NetSoft*, Apr. 2015, pp. 1–5.

[44] Cisco and/or its affiliates, "Cisco Evolved Services Platform At-a-Glance," Oct. 2014.

[45] F. Callegati, W. Cerroni, C. Contoli, and G. Santandrea, "Implementing Dynamic Chaining of Virtual Network Functions in OpenStack Platform," in *ICTON*, Jul. 2015.

[46] ACG Research, "Business Case for Cisco Evolved Services Platform and NFV White Paper," 2014.

[47] Cisco and/or its affiliates, "Cisco NFV Solution for the Cisco Evolved Services Platform," Sep. 2014.

[48] Alcatel-Lucent White Paper, "Providing Security in NFV: Challenges and Opportunities," May 2014.

[49] Alcatel-Lucent Strategic White Paper, "Model-based orchestration in NFV," Mar. 2015.

[50] Collaborative White Paper between Alcatel-Lucent and Red Hat, "CloudBand with OpenStack as NFV Platform," Aug. 2014.

[51] Alcatel-Lucent White Paper, "Network Functions Virtualization: Challenges and Solutions," Jun. 2013.

[52] VMware, "Datasheet: VMware vCloud NFV," Sep. 2015.