International Journal of Research in Engineering and Applied Sciences(IJREAS)
Available online at http://euroasiapub.org/journals.php
Vol. 7 Issue 5, May-2017, pp. 134~141
ISSN (O): 2249-3905, ISSN(P): 2349-6525 | Impact Factor: 7.196 | Thomson Reuters Researcher ID: L-5236-2015

Security Issues in Network Function Virtualization

Bharti Bansal [1],

Shweta Rana [2]

[1,2]Assistant Professor & Amity University Haryana

ABSTRACT

Network Function Virtualization (NFV) is an emerging solution that aims at improving the flexibility, the efficiency and the manageability of networks, by leveraging virtualization and cloud computing technologies to run network appliances in software. NFV decreases hardware equipment costs and energy consumption, improves operational efficiency and optimizes network configuration. However, potential security issues are 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 promising research directions in this area.

Keywords—Network functions virtualization, Software Defined Networking.

1. Introduction

Building on a well established trend in the IT industry, virtualization is rapidly entering the telecom market, network functions virtualization being its latest incarnation [1]. In modern days, as there is an increase in diversity and data rates from users, Telecommunications Service Providers (TSPs) must purchase, store and operate new physical equipment. It leads to high expenditure costs for TSPs. Currently; most telecom equipment is sold in the form of vertically integrated systems with applications running on, and tightly coupled with, middleware and hardware. Network Functions Virtualization (NFV) [2],[3] was proposed as a new technology to design, deploy and manage networking services with 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 [4]. The main contribution of NFV is to realize software-based NFs such as virtualized gateways and virtualized firewalls, instead of hardware appliances. NFV may contain various security issues, such as components in NFV architectural framework, like hypervisors and orchestrators, may be vulnerable to potential security threats. The shared storage and networking may introduce new security vulnerabilities [2].

NFV has the following advantages over the traditional network architectures [5]: (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. Furthermore, hypervisors, hardware and VNFs are likely to be offered by different vendors, thus resulting in integration complexity and generating security loop-holes [5].

Various approaches have been proposed to address the security problems in NFV [6], [7], [8], [9]. For example, NFV ISG provides guidance to ensure security in NFV's external operational environment and presents related technologies to supply security and trust for NFV [10], [11]. 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 [12].

In this survey paper security aspect of NFV are discussed. The detailed information about security issues in NFV are discussed in this survey.

In this survey security problems in NFV and corresponding solutions are discussed, proposed security architectures for NFV is explained. An overview of commercial products designed for NFV security is presented followed by a prophecy of future research challenges in NFV security.

2. A BRIEF OVERVIEW OF NFV

As shown in Fig. 1, NFV architectural framework includes multiple functional components such as NFV Management and Orchestrator, NFVI (Network Function Virtualization Infrastructure) and VNF (Virtualized Network Functions). 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, and virtualization of content delivery networks [13]. 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 [14]. 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 [15]. To guarantee the service availability and maintain resiliency in NFV, automated recovery from failures should be enabled [16]. 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 [17]. 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.

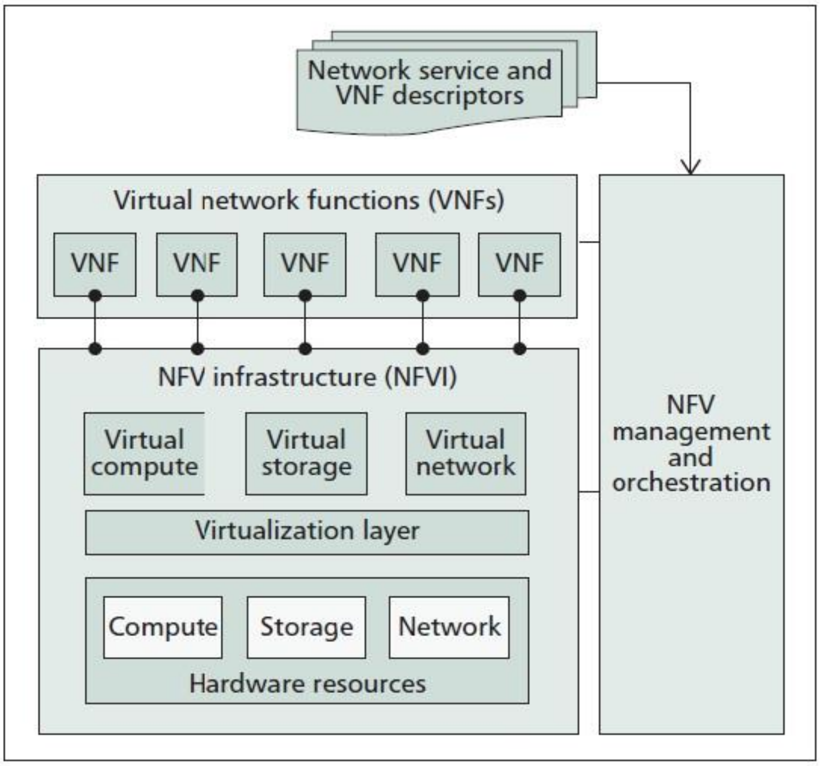

Fig. 1. NFV architectural framework.

3. SECURITY CHALLENGES AND SOLUTIONS FOR NFV

NFV brings great opportunities such as reduced cost and less operational influence. However, there are challenges accompanying opportunities [18], [19]. Underlying areas of concern in NFV security include user/tenant authentication and authorization [10]. Security in NFV is discussed in [11] under three situations: security inside VNFs, security between VNFs, and security outside VNFs. Security and software management are the major challenges to NFV [12]. How to overcome the security problems from hypervisor, data communication, and APIs remains a challenge for applying NFV into telecommunication networks and mobile networks [5].

A. Security challenges from NFV infrastructure

The NFV infrastructure (NFVI) is constituted by compute domain, hypervisor domain, and network domain. 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 [20], [21], [22].

B. Security challenges from standard interface definition

Defining standard interfaces for various security functions is also 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 [23]. The predefined virtualized network security functions can be used in access networks [24], mobile networks [25], data center [26], SDN [27], and NFV [28].

C. Security challenges from management and orchestration

Keeney, et al. [29] discussed the security challenges in managing and orchestrating VNFs when using NFV for mobile 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 transferring 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. [30] 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.

4. 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. [31] proposed a framework to apply security policy management to NFV. In the framework, a new software component is added to the NFV architecture named as Policy Manager. Security policies can be defined by users. The high-level policies (HLP) language and medium-level policies (MLP) language are used to define the policies. First, the Policy Manager generates the needed configurations to meet the security requirements from users and then the configurations are sent by the orchestrator to configure different VNFs to achieve the desired security VNFs. Integration of the Policy Manager with the NFV architecture allows users to specify their security requirements in a flexible, effective and convenient way.

B. A User-Centric Approach

A user-centric model to protect users' securities in NFV is introduced by Montero, et al. [10]. 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, security policy manager, authentication system, and SECURED app. These security related components work together to provide security and trust in NFV.

C. OpenNF
It is designed as control plane architecture to provide efficient and safe allocation of data flows across network function instances in NFV [6]. 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. The aim of OpenNF is 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 [33].The Service Broker connects services orchestration and business logic to assure efficient and secure service delivery. Different service attributes and policies are included in service profiles 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 [34] to the open architecture makes the Catalog of Virtual Functions extensible, which allows more VNFs and services to be added into the NFV solutions [35], [36].

E. VMware vCloud NFV
It was developed by VMware in 2015 to cope with increased service agility and security. 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 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 [37].

F. Alcatel-Lucent CloudBand
In 2014, a secure NFV platform called CloudBand id developed by Alcatel-Lucent [38]. The framework of CloudBand includes a centralized CloudBand management system and multiple distributed CloudBand nodes [39], [40]. 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 [41].

5. FUTURE CHALLENGES IN NFV SECURITY

Although many solutions have been proposed to overcome the security challenges in NFV, many potential security challenges are still remaining. Some of the research challenges and future directions for NFV security are:
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, there will be in an increase in the likelihood of one or few services to be compromised. To detect compromised components

and mitigate their impact remains a challenge is a challenge in NVF.

2) Distributed Denial-of-service attacks: Distributed Denial of service attacks (DDoS) can cause tremendous damage to NFV supported network. Hence it need to be 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: 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.

6. 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 discussed the background of NFV and highlight the security issues related to NFV. A summary of NFV security challenges and corresponding solutions to address the security problems is presented. 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.

7. References

[1] "NFV: An Introduction, Benefits, Enablers, Challenges & Call for Action," NFV white paper; http://portal.etsi.org/NFV/NFV_White_Paper.pdf

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.
[10] "ETSI Group Specification: Network Functions Virtualization (NFV) NFV Security Problem Statement," Oct. 2014.
[11] "ETSI Group Specification: Network Functions Virtualization (NFV) NFV Security and Trust Guidance," Dec. 2014.
[12] Huawei White Paper, "Observation to NFV," Nov. 2014.
[13] "ETSI Group Specification: Network Functions Virtualization (NFV) Use Cases," Oct. 2013.
[14] "ETSI Group Specification: Network Functions Virtualization (NFV) Management and Orchestration," Dec. 2014.
[15] "ETSI Group Specification: Network Functions Virtualization (NFV) Virtualization Requirements," Oct. 2013.
[16] "ETSI Group Specification: Network Functions Virtualization (NFV) Resiliency Requirements," Jan. 2015.
[17] "ETSI Group Specification: Network Functions Virtualization (NFV) Use Cases," Oct. 2013.
[18] 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.
[19] 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.
[20] "ETSI Group Specification: Network Functions Virtualization (NFV) Infrastructure Compute Domain," Dec. 2014.
[21] "ETSI Group Specification: Network Functions Virtualization (NFV) Infrastructure Hypervisor Domain," Jan. 2015.
[22] "ETSI Group Specification: Network Functions Virtualization (NFV) Infrastructure Network Domain," Dec. 2014.
[23] 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.
[24] A. Pastor and D. Lopez, "Access Use Cases for an Open OAM Interface to Virtualized Security Services," Oct. 2014.
[25] K. Wang and X. Zhuang, "Integrated Security with Access Network Use Case," Feb. 2015.
[26] M. Zarny, S. Magee, N. Leymann, and L. Dunbar, "I2NSF Data Center Use Cases," Oct. 2014.
[27] 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.
[28] C. Price and S. Rivera, "OPNFV: An Open Platform to Accelerate NFV," Oct. 2012.
[29] J. Keeney, S. van der Meer, and L. Fallon, "Towards Real-time Management of Virtualized Telecommunication Networks," in CNSM, Nov. 2014.
[30] 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.
[31] 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.
[32] Cisco and/or its affiliates, "Cisco Evolved Services Platform At-a- Glance," Oct. 2014.
[33] 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.

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

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

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

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

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

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

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

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