Implementation Problems Facing Network Function Virtualization and Solutions

Krishna Gandhi
School of Information Technology
Illinois State University
Normal, IL, USA
e-mail: kgandh1@ilstu.edu

Jihad Qaddour
School of Information Technology
Illinois State University
Normal, IL, USA
e-mail: jqaddou@ilstu.edu

Abstract- **Network administrators prefer the Network Function Virtualization (NFV) concept as it is cost-efficient and easy to maintain. However, the new technologies based on this concept might lead to security threats, such as denial of service attacks, availability attacks, exploitation, malware injection, or other undiscovered threats. Network Functions Virtualization represents a very large paradigm shift in the development and the deployment of network services. Many research works on NFV address the virtual concept. It can be a cloud or a virtual private server. The security is the most important thing since the virtual environment can also be compromised by cyber-attacks. The paper focuses on the problems facing NFV implementation and offers ways of navigating through the main security related problems stated above.**

Keywords-Network Function Virtualization (NFV); Virtual Network Function (VNF); Cloud Security Alliance (CSA); Software-Defined Networking (SDN).

I. INTRODUCTION

The evolution of cloud computing has led to an increase in cyberattacks targeted towards individuals, corporations or any vulnerable entity within the cloud system. The increase in the attacks forces bodies such as the Cloud Security Alliance (CSA) to convene and deliberate on the best ways to secure the systems, making them impervious to cyber attacks. One area facing the blow of cyber attacks is the network function virtualization. In computing, the term virtualization can be applied to storage devices, operating systems, hardware platforms, computer network resources and much more. The evolution of technology allows the virtualization of nearly all computer software and hardware. Basically, nearly all network functions can be virtualized. In this article, we explore virtualization in network functions. Moreover, there will be mentions of Software-Defined Networks (SDN), which alter the network function behaviors and allow dynamic changes in the configurations of a network [1]. Network function virtualization, commonly referred to as NFV, is a concept recently introduced with numerous goals, like reducing overall cost, ease of management, scalability, and also reducing the proprietary hardware required during the launch or operation of network services [2]. If the concept is implemented successfully, most of the network services will launch and operate virtually decoupling the functions of dedicated hardware devices in a network, such as firewalls, routers, and load balancers.

The concept relies on a hypervisor that controls the network functions making it easier to run them on the standard X86 servers. The implementation of the NFV makes the network administrators work easier by eliminating the need for dedicated hardware devices when building a service chain, thus reducing the operating expenses (OPEX) and capital expenses (CAPEX) since the services will run on a virtual machine. Moreover, NFV gives the network administrators agility and flexibility when troubleshooting errors in the system or when performing the routine maintenance. SDN and NFV are different, yet complementary techniques applicable by network administrators: the NFV infrastructure allows SDN to run, enabling it to forward data packets to and from network devices, while the control functions run on a Virtual Machine (VM) [3]. The implementation of NFV creates various challenges and complexities in the security controls of networks.

According to Amogh et al. [4], the CSA addresses some problems that exist when implementing NFV, regardless of the benefits it conveys such as cost reduction, agility, and flexibility. There are six problems evident according to the authors, and they include (1) scalability of available resources, (2) stateful versus stateless inspection, (3) service insertion, (4) hypervisor dependencies, (5) dynamic workloads, and (6) elastic network boundaries. The six problems revolve around the security of network function virtualization and if each of them is not addressed individually, the incompleteness of configurations, lack of integrity and lack of clearness defining security policies can lead to attacks like denial-of-service. In NFV implemented environments, stateful inspection of data-flow in the network requires asymmetric flows which allow seeing every data packet in transit, granting access controls to NFV, and stateless inspection fails to see all the data packets in transit making it difficult to grant access controls to NFV. The problem brings about security issues since the NFV does not know or have access to the data packets in transit. Service insertion into the NFV relies on overlay models that fail to coexist across the vendor boundaries, allowing the implementation of NFV to be vulnerable to the security breach. Insertion of services in NFV requires existing layered services in the hypervisor, causing it to be difficult to deal with asymmetries in the network, which arise from their creation by redundant network devices and paths. To ensure security is top-notch, vendors must all agree on standards addressing security issues. The implementation of NFV

 ISBN: 978-1-61208-625-5

makes the understanding of the underlying architecture difficult for the vendors, leading to the production of different hypervisors for different systems. It is imperative for the vendors to come in unison to ensure the security vulnerabilities are non-existent such as, patching vulnerable code that risks security breaches. Recent changes in network topology make it difficult for traditional security methods to evolve as per the current demand; additionally, traditional methods are static compared to NFV, which is dynamic and agile in its capabilities. Unlike the traditional methods, NFV has no defined boundaries; its capabilities can expand as far as the network administrators can fathom. Traditional methods are bound by cable lengths, location and much more, creating a definite boundary. The lack of clear boundaries puts the network systems at risk in matters pertaining to security.

In the paper, the focus is on the security issues that may arise or exist during or after the implementation of NFV. The paper is organized into four sections: Section II discusses literature review, Section III presents a comparative study, Section IV performs an analysis and discussion, Section V describes the proposed solution, while Section VI concludes the paper and suggests possible future developments.

II. LITERATURE REVIEW

According to research, NFV is a major milestone in the networking and telecommunications sector. Stringent laws govern the administration of NFV enabling the availability, security, and superb performance of the concept. NFV revolutionizes the telecommunications and construction networks by reducing the costs incurred purchasing new gadgets or hardware and increasing the automation of systems. Some challenges of NFV implementation include the reliability of additional software, the effective key escrow for the functions of the hosted network, reduced isolation of the functions in a network, and fate-sharing resulting from multi-tenancy [5].

According to the article by Yang and Fung [6], *a survey on security in network functions virtualization*. The authors acknowledge NFV as an emerging innovation that focusses on the removal of hardware equipment responsible for various network functions. The removal of the hardware equipment gives room for the implementation of virtual machines running on cloud computing infrastructure that takes on the tasks tasked with the hardware equipment. As a result, there is a reduction in the energy consumption and equipment costs. Additionally, the authors acknowledge that the rate of innovation poses risks for the NFV and they focus their paper on the emerging security challenges and issues. Yang and Fung present various techniques for overcoming the challenges by offering security products and solutions to tackle the rising insecurities. They explore future works applicable to the security issues accompanying NFV implementation after conducting a survey on NFV security use cases. The paper is in line with what our research entails and therefore is a chief resource in our work. The use of various research methods gives insight on the directions we should take while tackling the topic. The authors suggest that the main contribution of NFV is the realization of software-based NFs such as virtual gateways and firewalls, unlike the traditional methods where hardware appliances were key to the realization of networking.

The paper addresses most of our research and offers research methodologies used in the conclusion of the findings. Moreover, the paper focusses on the security issues revolving around the implementation of NFV in the modern systems and offers various ways of mitigating past the security issues. The information is crucial to our research as it gives us a guideline on how the paper should be and what it should address unlike other related research papers published by different authors. Yang and Fung conducted a survey similar to what the paper will use to gain credible data on the issue of security in the network function virtualization implementation.

According to Raina et al. [7], the implementation of NFV has resulted in the adoption of advanced security measures to curb the rise in security vulnerabilities resulting from the amalgamation of the traditional methods and NFV. Virtualization addresses some of the deployed network security functions focused on reducing the vulnerabilities arising from the adoption of NFV [7]. The security measures focus on malware protection, access control, denial-of-service protection, access and identity management, intrusion prevention and detection, and cryptography. Malicious computer experts target systems with poor security measures in the hope of accessing valuable information that they may use to their gain or conduct fraudulent activities. For example, a bank scenario where the bank has recently adopted the use of NFV with little or no security measures may compromise the personal information of its clients. Malicious people may try to secure crucial data linked to the customers' accounts and transfer huge amounts of funds to their accounts making the bank vulnerable to litigations, customer distrust, or closure. The data presented is credible to some extent since most the stated challenges are still a challenge to date. The paper addresses the problems and challenges related to the paper thus it is a vital reference material.

According to Han, Gopalakrishnan, Ji, and Lee [8], the introduction of NFV was to reduce the time taken to market novel services and improve the flexibility of the provision of the network system. NFV aids in the decoupling of software implementations from underlying dedicated hardware. In the article, the authors explain the architectural framework and requirements of NFV and later discuss the challenges experienced and the available opportunities for innovation. In relation to the topic, we will look into the challenges of NFV. The authors clearly state that network administrators ought to be careful when implementing NFV in existing systems to ensure security features are unaffected. Elements such as hypervisors and orchestrators pose a security threat to the network system when wrongly implemented and lead to a rise in the intrusion. An increase in intrusion forces the system to concentrate on intrusion prevention mechanisms, which lead to an overload of the intrusion detection systems. However, when correctly implemented, NFV makes work easier for all concerned parties and allows the possibilities of virtualized firewalls creation and domain protection thus increasing the security of the network system. Virtualizing network resources poses risks since applications and services

 ISBN: 978-1-61208-625-5

rely on the virtual machine to complete commands, for instance, when a service is bugged and requires certain resources from the virtual machine, it can easily infect the core of operations thus increasing the spread of the bug or virus within the network.

According to T. Qasim [9], research on NFV machine learning the huge population communication services is leading to the heavy loaded signaling system. It uses Signaling System No 7 (SS7). SS7 was protected due control owned by state-owned telecommunication operators. SS7 and network function virtualization have introduced many new security challenges. There can be some vulnerability in a virtualized environment. There should be many methods that mitigate machine learning techniques from gathering network traffic [9]. The research done by A. Kalliola and S. Lal developed security orchestration in NFV environment and is crucial. It represents Distributed Denial of Services attacks and other cyber-attacks. The most important finding is that it can mitigate future variation of attacks. These are all done by machine learning orchestrating virtualized network functions around the affected components to isolate those components and redirect, capture and filter the traffic for further analysis. This would allow maintaining a high quality of service to given network functions [10].

Network Function Virtualization security is a vast area of concern in many forms. Most of the NFV researches done with an example are scenarios, especially research conducted for Distributed DoS attack mitigation [9]. It implements an SDN enable network in the OpenStack environment and demonstrates and explains the effectiveness with various kinds of attacks [Figure 1]. The mitigation architecture was designed and implemented for the cloud environment. It used underlying software-defined network elements for attack mitigation and view of traffic.

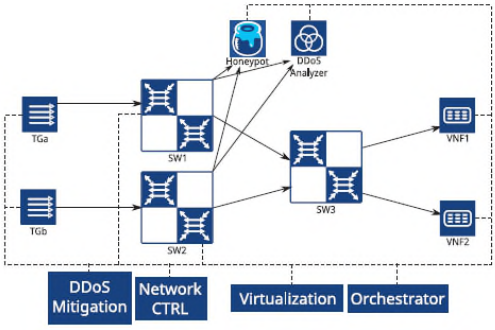

Figure 1. DDoS attack mitigation scenario.

SS7 network vulnerability detection of NFV using machine learning [10] also uses proper simulation to present the many attacks. Machine learning techniques are proposed as a detection mechanism. The experimental setup has implemented to provide proof of concept [Figure 2]. SS7 traffic is generated in a properly setup virtual environment. DoS and man in the middle attacks are launched on the network.

There are many advantages if it presents in a virtual environment because real devices do not get the actual effect of the attacks. Using automation software such OpenStack provides real benefits to visualize the real attack.

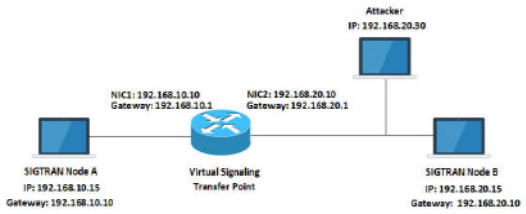

Figure 2. Simulation Setup.

According to F. Reynaud et al. [16], the network functions come to resolve many network several issues which come with the growth of the infrastructure, as power consumption, difficulties to manage the environment, elevated costs, low dynamism and scalability and misconfiguration proneness. To break those paradigms the virtualization and softwarization emerged. European Telecommunications Standard Institute (ETSI) created it to simplify the management and reduce costs of networking hardware as well since before it the companies have to buy one or more equipment for each network function. The clearest advantage of using it is the reduction of costs, but it has also many advantages as a facility on the network management using a centralized programmable controller. It reduces the complexity of management and allows more flexible and fewer errors on network configuration. However, there are some problems related to attack vulnerabilities when using the standard. One of them is DDoS, which brings many problems as opened ports and direct denial of services running since the resources are not really unlimited. The traffic can be identified, but it needs a 3rd party resource to work. Another Man in the Middle attack which is possible when a proper authentication mechanism does not exist is a case of an attack that will fatally put the NFV down.

The last attack we refer to here is the Network Visibility Poisoning, an attack that may come from several security breaches as Host Location Hijacking, Link Fabrication Attacks or insufficient protection from the northbound applications. There is another 3rd application which can work side by side with NFV and helps it to check the integrity of the packets.

According to T. Dimitrakos [17], NFV brings even more advantages to the users such as the increase of time to market and services fast deployment, the scalability of services that can be up or down rapidly as required. Based on the document [17], the standard makes the virtualized infrastructure go along with the market challenges delivering good features, fast, reliable and easier than traditional solutions. One of the main quotations of T. Dimitrakos [17] is if the NFV standard can maintain traceability to threats, challenges and customers, standards and compliance requirements. Since we are very near to the big expansion of Internet of Things (IoT), the NFV must come as an interesting solution for decentralized environments and networks, since it can be deployed inside or together with the virtual machine and its components.

 ISBN: 978-1-61208-625-5

Some of the NFV challenges according to him are that it would be very hard to put high-end security functions, the intelligent management of the specific traffic designated to Virtual Network Functions. Another challenge is that, since the SDN (controller) must intercept, steer and mirror traffic for security inspection since it is asynchronous, maybe the NFV function cannot work properly.

T. Thanh et al. [18] built a specification called MANO, which consists in automatization of known NFV that makes it more reliable when in use. MANO seeks to automate the learning of NFV model and resolve many security problems. The simple security framework consists of Security Planning, Security Enforcement, and Secure Monitoring, and every part of this schema feeds the other, making a stronger and faster security solution for NFV. The Security Enforcement and Monitoring work together mitigating the risks and feeding the Security Planning layer for better updates and deployments. They had some success making a two-sided management system, which could work with Access Control and Decision-making lists, using OpenBaton, a toolkit that implements a current ETSI NFV MANO. They provided virtual infrastructure and monitored it using ZABBIX. They had great results using it with the developed application and there were gains on Embed Security Functions, a security protection that can be embedded automatically and transparently to a virtual infrastructure. Security Management Lifecycle Support, which makes the security policy, adapts itself to application lifecycle and Dynamic Security Incident Response that adapts in case of DoS attack or other unforeseen events (Zero-Day Threats).

The article does not address all the challenges we identified arising from the implementation of NFV. However, the paper gives a comparative study of the work done so far and also gives the direction on the future works possible from the implementation of network function virtualization.

III. COMPARATIVE STUDY

A comparative study is presented in TABLE 1. The table is showing different security problems in NFV and the solution proposed as a summary.

TABLE I. COMPARATIVE STUDY IN NFV SECURITY

Year	Security Problems in NFV	Solutions	Challenges
2017	Security Adaptability of NFV environment [18]	A toolkit named OpenBaton was used which consists in identifying network threats, generating security policies and makeing an active monitoring of network packets, adapting the rules according to the properties of packets on the ports monitored.	Build a Hypervisor using this feature embedded and transparent, it could be expensive and take some time to be made.
2015	Network visibility poisoning of NFV standard	Two 3rd solutions can be used within NFV standard to solve this problem. One of those is Rosemary [19] that is an SDN controller that resolves the lack of access control and authentication for the applications responsible for the Link Deletion attack by employing a sandbox approach (App Zone). Another solution is TopoGuard [20] that uses Topology Update Checker to verify the legitimacy of a host migration, the integrity/origin of an LLDP packet and switch the port property once detecting a topology update	The complexity of implementing the two 3rd party applications must be a problem since no Hypervisor is using it.
2016	Side Channel Attacks to the VM frequency [16]	To defend against this attack it is required to eliminate or reduce the signal information generated by the channel or introduce some kind of noise to the channel.	Some organizations already have this functionality embedded into their systems. The only challenge is to find the most efficient system in the market.
2009	Denial of Services at forwarding plane level [16]	The feature FlowVisor [21] reads the traffic in slices, it learns and read the packets over the network and receive an update from the network controller and applies the new rules to a specific slice of the network. This feature can prevent the Denial of Services from affecting the whole environment since it can block the traffic at a small part of the packet or sequence.	When receiving a DoS attack it is hard to differentiate between the attack packets and normal packets.
2018	Signaling System 7 attacks in NFV [9]	SIGTRAN protocol and MTPSec, IPSec and an enhanced firewall combined with the intrusion detection feature are the proposed solutions to identify and mitigate the SS7 attacks.	The solutions for signaling system 7 attack are quite expensive and not easy to implement in the VM environment making it impracticable.
2017	Access Control Management in NFV[18]	ETSI NFV MANO specifications can automatically update the system policies, making the access control stronger and self-managed into the systems.	This is based on theoretical logic and did not process in actual NFV environment.

III. ANALISYS AND DISCUSSION

Based on the comparative study performed, we found that SS7 attack in NFV is the biggest security challenge because it is the newest released attack. Due to solution implementation cost and configuration complexity, the solution for SS7 becomes impracticable. This also has four

big breaches divided into User Information, Eavesdropping, Financial Thievery and Misuse of Service. Considering SS7 is a silent attack, it can leak multiple information and protocols, for example, Logical Application Part (CAP). When a Man-in-the-Middle attack is launched on the SS7 layer, the attacker intercepts the traffic and makes the router busy in processing inconsistent packets while it sends the attack packets to the full traffic. This action may steal data in various levels of communication since it can capture network packets and application layer packets as well.

IV. PROPOSED SOLUTION

NFV can be improved in many ways. One of them, which we consider most important, is putting encryption of the traffic across the NFV environment will protect it against many threats such as SS7. Our proposed solution is embedded integration of Hypervisors with IPS and IDS systems. Since they can monitor the network and auto create policies to defend the environment, this can be the best solutions for newer attacks as signaling systems 7. Another point is that with the data created by IPS and IDS systems, the researchers will have the capability to understand and improve security quickly and efficiently.

V. CONCLUSION AND FUTURE WORK

The NFV findings reveal that the concept is widely accepted by various individuals mainly due to its reduction in cost and dedicated hardware. However, NFV faces or gives rise to various security concerns as it is open to some security breaches and it is not capable to avoid a DDoS attack, for example. Organizations that use NFV systems can have better performance than those using the traditional computer networking systems. Since NFV is vulnerable to a dangerous attack such as SS7, it is highly recommended that the network specialist ensure to have a good firewall combining IPS and IDS features, since we do not have an embedded hypervisor OS yet. Also, there is a huge growth of IoT devices globally. Solutions such as NFV will often need to make new equipment connected to the Internet viable, so the investment in upgrades is needed, especially thinking about threats and concerns, for example, SS7 attack over NFV, since SS7 is one of the biggest security challenges for NFV environment since it exploits the vulnerability of the communication infrastructure.

To implement the proposed solutions it is required a dedicated research to improve the NFV capabilities and integrate with the market security solutions as Deep Packets Inspection and Intrusion Detection Systems so we can implement a fully embedded virtual network solution. We will also be customizing an OpenStack OS that uses its own native IPS when the NFV feature is enabled, so it can grant only genuine packets and users to access the systems behind it, making it more reliable and robust.

The focus will also be on the protocols such as SIGTRAN and MTPSec which can make it easier for the NFV host to identify the threat and take some action to avoid the breach. The IPSec protocol will also be used, so its capacity to ensure the origin and destination details inside the packet can be a good option to ensure the environment security.

In the future, the above features and protocols can be tested inside the NFV environment to validate the functionality and protect against the SS7 breach.

REFERENCES

[1] M. Odini, “NFV Testing. IEEE Software Defined Networks,” pp. 24 November 2016.

[2] R. Mijumbi, J. Serrat, J. Gorricho, N. Bouten, F. De Turck, and R. Boutaba. “Network Function Virtualization: State-of-the-Art and Research Challenges,” IEEE Communications Surveys and Tutorials, pp. 236-262, 2016.

[3] E. Duarte and M. Hiltunen. “Workshop on Dependability Issues on SDN and NFV (DISN),” 2015 45Th Annual IEEE/IFIP International Conference On Dependable Systems And Networks, 2015.

[4] N. Amogh, A. Gelman, and M. Ulema. “IEEE SDN/NFV Standardization - IEEE Software Defined Networks,” sdn.ieee.org, pp.1-5, 24 November 2016.

[5] D. Bernardo and B. Chua. “Introduction and Analysis of SDN and NFV Security Architecture (SN-SECA),” 2015 IEEE 29Th International Conference On Advanced Information Networking And Applications, 2015.

[6] W. Yang and C. Fung, "A survey on security in network function virtualization,” IEEE Netsoft Conference And Workshops (Netsoft), pp.1-5, 2016.

[7] K. Raina, S. Chaudhry, A. Milenkoski, B. Jaeger, M. Harris, and S. Chasiri. et al. “Security Position Paper Network Function Virtualization,” Cloud Security Alliance, pp.5-26, 2016.

[8] B. Han, V. Gopalakrishnan.,L. Ji, and S. Lee. “Network Functions Virtualization: Challenges and Opportunities for Innovation,” pp.93-96, 2016.

[9] T. Qasim, M. H. Durand, A. Khan, F. Nazir and T. Qasim.”Detection of signaling system 7 attacks in NFV using machine learning,” IEEE 15th international bhurban conference on applied sciences & technology, 2018.

[10] A. Kalliola, S. Lal, K. Ahola, I. Oliver, and Y. Miche. “Testbed for security orchestration in an NFV environment,” IEEE Conference on Network Function Virtualization and Software Defined Networks, 2017.

[11] C. L Hwang and K. Yoon. “Multiple attribute decision making: methods and applications a state-of-the-art case,” Vol. 186, Springer Science & Business Media, pp.25-48, 2012.

[12] A. Tong. “An Inside Look at Winning SDN and NFV Case Studies (1st ed.),” pp.2-18, 2016.

[13] J. Buchmann. “Introduction to cryptography,” Springer Science and Business Media, pp. 1-5, 2013

[14] J. Katz and Y. Lindell. “Introduction to modern cryptography,” CRC Press, pp.2-4, 2014

[15] C. Buyukkoc. “SDN Initiative Creates Subcommittee to Address SDN, NFV Fragmentation-IEEE Software Defined Networks” Sdn.ieee.org, pp.1-4, 24 November 2016

[16] Reynaud, François, François-Xavier Aguessy, Olivier Bettan, Mathieu Bouet, and Vania Conan. "Attacks against network functions virtualization and software-defined networking:

 ISBN: 978-1-61208-625-5

state-of-the-art." In *NetSoft Conference and Workshops (NetSoft), 2016 IEEE*, pp. 471-476. IEEE, 2016

[17] T. Dimitrakos, “Security Challenges and Guidance for Protecting NFV on Cloud IaaS,” 2014.

[18] T. Thanh, S. Covaci, M. Corici, and T. Magedanz. Fraunhofer Institute FOKUS, 2 Technical University Berlin Germany,”Access Control Management and Orchestration in NFV Environment.”

[19] S. Hong, L. Xu, H. Wang, and G. Gu, “Poisoning Network Visibility in Software-Defined Networks: New Attacks and Countermeasures,” NDSS’15, Feb. 2015.

[20] S. Shin et al. , “Rosemary: A Robust, Secure, and High-performance Network Operating System,” CCS’14, Nov. 2014. Milenkoski, A., Jaeger, B., Raina, K., Harris, M., Chaudhry, S., Chair, S., ... & Liu, W. (2016). Security position paper network function virtualization. *Cloud Security Alliance-Virtualization Working Group*.

[21] R. Sherwood, G. Gibb, K.-K. Yap, G. Appenzeller, M. Casado, N. McKeown, and G. Parulkar, “FlowVisor: A Network Virtualization Layer,” OpenFlow Switch Consortium, Tech. Rep, Oct.

 ISBN: 978-1-61208-625-5

 ISBN: 978-1-61208-625-5