A Survey of Network Function Virtualization Security

Ahmed M. Alwakeel , Abdulrahman K. Alnaim and Eduardo B. Fernandez
Department of Computer and Electrical Engineering and Computer Science
Florida Atlantic University
Boca Raton, USA
Email: {aalwakeel2013,aalnaim2017,fernande}@fau.edu

***Abstract*—Network Function Virtualization (NFV) provides many benefits to consumers because it is a cost-efficient evolution of legacy networks, allowing the enhancement and extension of networks in quick and low cost manner since the functions of the network will be provided through virtualization. However, security issues are a major concern for NFV users. This paper goes over different security threats of NFV and some of the countermeasures to mitigate these security threats. Also, we define patterns as a way of describing security solutions in an abstract and generic way. Lastly, we provide some of the security research directions in this area.**

***Index Terms*— Network Function Virtualization; network security; security patterns; secure software; cloud computing**

I. Introduction

With the advances of technology, new solutions have been introduced to the telecommunications industry. One of these solutions is Network Functions Virtualization (NFV). Traditionally, network operators must deploy physical proprietary equipment and devices for every part and function of the network. This leads to high installation costs and restrictions for changing or enhancing the network. Also, with the increase of user demands on network functions, Telecommunication Service Providers (TSPs) are required to acquire more hardware devices to provision users requirements, and it is difficult to manage these devices when added; which results in high Capital Expenditure (CAPEX) and Operational Expenditure (OPEX). However, TSPs can overcome these challenges with NFV, which provides agility and dynamic services.

NFV implements network functions virtually by decoupling hardware appliances (firewalls, gateways, etc.) from the functions that are running on them. It represents the implementation of Network Functions (NFs) through software that is executed on a set of high-end hosts which provide virtualized gateways, virtualized firewalls and even virtualized components of the network, leading to providing flexible network functions deployment. Achieving that makes the setup of the network more flexible based on the user needs as well as making the process of scaling the network easier since all the functions will be software based, not hardware based like in traditional networks. A practical scenario of NFV is when users dynamically alter the rules of a virtualized firewall based on their requirements; or the functions of a virtual router/virtual switch can be dynamically configured based on network needs. NFV promises the following benefits [1]: 1- *Independence:* software is no longer integrated with hardware in NFV. As a result, their evolution will be independent from each other. 2- *Flexibility:* the decoupling of software from hardware helps to reassign and share the same infrastructure resources, which allows to perform different functions at various times. As a result, the deployment of network functions and their connections becomes more flexible. 3- *Scalability:* decoupling software from hardware provides more flexibility to dynamically scale the actual performance of VNFs with finer granularity. 4- *Reduced energy consumption:* with the ability of scaling resources up and down, TSPs will be able to reduce the OPEX needed to run network devices which could be up to 10% of the current power consumption right now [2]

NFV consists of three main architectural components, which are: *Network Function Virtualization Infrastructure* (NFVI) which supports the execution of VNFs, *Virtualized Network Functions* (VNFs), which are the functions that run on the NFVI, and *Management and Network Orchestration* (MANO), that cover the lifecycle management and orchestration of physical and/or software resources.

NFV introduces several security threats since it relies on software, which makes attacking it or manipulating its services easier than having the network functions provided by hardware only. A threat exploits a vulnerability in the network and the networking misuse affects the security of the users of the network. The hardware part of the NFV creates the backbone for the service; yet many of the resources could be from different service providers that are combined together to create VNFs. Therefore, the complexity of how these components integrate with each other raises, which also raises the possibility of threats in the network. This also introduces trust management issues between different VNF entities.

The threats that could affect NFV could be either internal or external; protecting these components requires strict security evaluation as well as adopting security mechanisms to counter the threats [3]. Different virtual operating systems and virtual functions could be integrated; if a part of the virtual system is compromised, this may affect the entire network and other entities since they all are connected together and may compromise each other.

We analyze the security threats of NFV technology and how

978-1-5386-6133-8/18/$31.00

NFVs unique characteristics introduce new security threats. We identify the main threats found in the literature for NFV technology as well as some of the suggested solutions that can prevent jeopardizing the security of NFV. There are several protection techniques in the literature to mitigate the threats in NFV [4], [5], [6], [7], surveyed security threats in NFV and proposed practical solutions for these threats; also, [8] proposed best security practices to protect against these threats; yet, no survey in the literature has considered the use of patterns as effective and convenient ways to describe countermeasures. Rather, the surveys described several NFV security solutions and industry products; we intend to use patterns as a solution for NFV threats. A pattern encapsulates a solution to a recurring problem in a specific context. A pattern can be a design pattern, a security pattern, or a misuse pattern, as well as other varieties of patterns [9].

This paper is structured as follows: section II provides an overview of the NFV infrastructure explaining the different layers of the NFV. Section III discusses NFV threats. Section IV discusses countermeasures to NFV threats. Section V provides an overview of patterns and current and possible research directions in NFV security. Finally, section VI provides a conclusion for this paper.

II. NFV INFRASTRUCTURE OVERVIEW

The European Telecommunications Standards Institute (ETSI) has developed standards for NFV as a framework that consist of three main components (Figure 1).This framework is used here as a reference for possible threats toward NFV.

I- Network Function Virtualization Infrastructure (NFVI) is a type of cloud data center that contains both hardware and virtual resources that build the base environment for NFV, including servers, networks and virtual machines. NFVI contains additionally three main components, which are: virtualized resources, virtualization layer and hardware resources. Hardware resources contain all the resources to build the network as well as computing and storage resources. The virtualization layer abstracts the hardware resources and decouples the software from the hardware enabling the software to execute independently from the hardware part. Virtualized resources include virtual networks, storage and processors.

II-Virtualized Network Functions (VNF) are the basic building blocks in the NFV architecture; they are software implementations of the network functions. VNFs can be connected or combined as composite building blocks to offer full-scale network communication services; this is known as Service Chaining. Elements management system (EMS) take care of management of the functionality for one or several VNFs [1].

III-The Network Functions Virtualization Management and Orchestration architectural framework (NFV-MANO) contains three main parts; the first is a virtualized infrastructure manager that controls and manages the interaction of the VNF and NFVI as well as computes and stores network resources; It also has the necessary deployment and monitoring capability for the virtualization layer. The second is the VNF

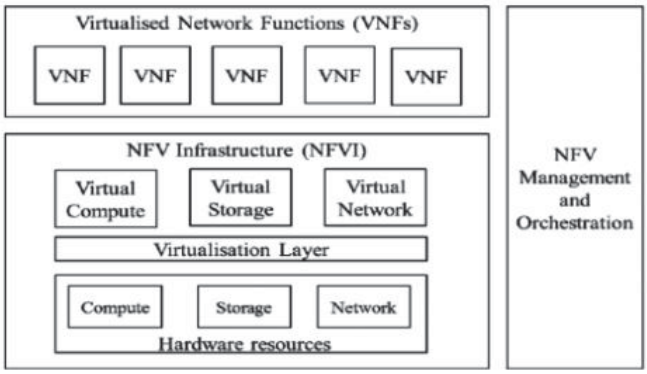

Fig. 1: High Level NFV Framework [1]

manager, which is responsible for managing the lifecycle of VNF instances and initializing, updating, querying, scaling and terminating these instances. The last part is the orchestrator that manages the lifecycle of network services that includes policy management, instantiation, performance management and Key Performance Indicator (KPI), which is a measurable value used to evaluate how effectively a company is achieving key business objectives. Moreover, VNF descriptor is one of the components of NFV-MANO which takes care of giving descriptions regarding different VNF deployment and operational requirements[8].

III. NFV THREATS

Several threats exploit vulnerabilities that may affect the functionality of NFV as well as may expose the sensitive and private information of business and indvisuals. As indicated, due to the unique characteristics of NFV, some new threats may affect the system that werent possible in the legacy network systems. This section covers some of the main threats that affect the security of NFV. We list them according to their effect on the framework of Figure 1.

Denial of service (DoS) attack: affects the service availability for legitimate users of a network by flooding servers with useless traffic. This type of attack usually affects the different virtualized network functions making them temporarily unavailable for users; it could also affect the entire system. DoS, or in its more complex case, Distributed Denial of Service (DDoS), mostly impacts large sites, and may cause financial and reputation loss. According to [10] 37% of attacks targeting networked systems were DDoS attacks in 2013, and they rose up to 65% on 2015, which makes them a serious concern for network service providers in the near future. In a VNF such as a vSwitch, the attacker overwhelms its virtual memory by sending fake requests making the service unavailable to the other users who intend to use the service. The issue here is that VMs have limited allocated memory; the switch will accept as many flows as it can if there is free memory on the VM [11]; even if the memory has higher capacity, it will just take more time to fill it with malicious requests. Moreover, due to the shareability of resources among VMs, attackers can launch a DoS/DDoS attack to let a malicious VM exhaust most of

its computing resources, which results for other VMs running on the same host to starve for resources. This will prevent the scalability and shareability of resources, which are critical features of an NFV environment.

Infrastructure integrity threats: as mentioned earlier, NFV requires the integrity of several providers and platforms; this introduces new threats to the service [12]. If a specific provider fails to secure its platform, this may lead to a failure in the computing process of NFV service [13]. An attacker can perform a spoofing attack to appear as a service provider to gain access to users data or knowledge about other services in the system [14].

Misuse of resources: in NFV, all physical resources are shared; while this provides a wider variety of computing resources for the users to choose from, it introduces a new challenge. Some of the computing resources dont fully support the multi-tenancy requirements that are demanded by NFV users. This leads sometimes for the components to act abnormally causing data leakage or even unavailability of service. Moreover, the hypervisor takes care of the communication and isolation of different entities that create the VNFs. If the hypervisor lacks enough security, an attacker may be able to alter the hypervisor giving himself extra resources. Another example is if the hypervisor failed to isolate between two users, user A (the attacker) could send intensive traffic to user B in order to stop that user from accessing the service freeing up the resources for the attacker. This type of attacks is called resource freeing attack [15]. In this type of attack, the attacker aims to free up resources for his own benefit accessing unauthorized resources which may cause bottlenecks in the resources, adding more load to other users using the same service and causing latency of the service, or even having the service fully blocked for other users. This attack is aimed toward the virtualization layer in the NFV architecture.

Change in NFV function definition: it is also a threat to the hypervisor and its VMs; a hypervisor allows multiple virtual entities to communicate and integrate with each other, taking care of managing the virtualization layer of the system. An example of an attack that may change the functionality definition of NFV is malware injection, which aims to affect the virtualization layer in the infrastructure of NFV via altering its internal code. The degree of how a malware attack affects the system varies, including slowing down the response time for the system and how the service functions [16]. Malware-injection attacks implemented on virtual machines can also cause modification to the permissions of the virtual service. A similar situation happened to Amazon EC Public IaaS cloud service when a malware-injection attack performed on it led to having sensitive data of users visible to other users using the same service in unauthorized ways [16]. Also, this attack could affect the NFV hypervisor, which may lead to dysfunction of CPU, virtual machines (VMs) and memory of the system. Typically having VMs running on a single server could create vulnerabilities that an attacker can take advantage of and use in order to implement malware injection attacks. Servers contain several VMs, having all the VMs in one place means that if any of them is not isolated enough from the others, this may lead to having the VMs attacked and modified [17].

Privileges modification: another type of attack that could jeopardize the security of NFV is known as privileges modification attack. This attack affects the virtualization layer of the NFV infrastructure, specifically the hypervisor. VMs deployed on single servers lead to a vulnerability that attackers can exploit; this vulnerability allows attackers to change the privileges of users of the system by upgrading their access to system entities in unauthorized manner [18], [17]. Also, they will be able to change the access allowed to resources for a specific user giving that user unauthorized access to more resources of the system, such as memory and CPU; this not only will affect the system but it will also affect availability of resources for other users of the system.

Confidentiality attack based on shared resources: side channel is a type of attack that take advantage of shared resources. Since different users share common resources in NFV, attackers could take advantage of that fact and try to pull some private informations from these users by creating some processes that affect the performance of other users processes in the same service, thus causing information leakage, denial of service, or accessing unauthorized resources. The information leakage basically occurs due to the vulnerability of shared memory across VMs [17]. Moreover, attackers can steal service time using the shared virtualized resources in unauthorized manner by exploiting a vulnerability of the hypervisor scheduler; this practice is known as theft-of-service attack [19]. Another vulnerability in the system that attackers use in order to implement side-channel attacks is because of flaws and complexity in the design of the system which may cause internal errors that gives some users unauthorized accessibility to resources or access to other users private data. These flaws are normally not visible or easy to detect by attackers; yet, brute force and overwhelming the system could lead to such errors [25].

Malicious insider: a malicious insider is typically a trusted member from inside the organization, such as: contractors, current or even former employees, who deliberately attempt to spy into private data, or even sabotage the organizations computing assets, driven by financial or personal motives. Lack of internal controls such as: security logging, security monitoring, security policies, are some of the main vulnerabilities that lead to such attacks [20]. A typical scenario is when an insider physically accesses a data center and damages the physical resources, but it can be done remotely which matters most with NFV. VNFs are possible targets for this type of threat, where a rogue administrator, who has privileged access rights, gains access and performs unauthorized configurations of VNFs. Also, an insider can exploit a compromised network function within the NFV infrastructure to monitor other network functions activities, or to disrupt their operations. [24] showed how it is possible for an insider, who has access rights to the hypervisor, to obtain a memory dump, or snapshots of a particular users VM, which then accesses the users passwords and private keys from memory snapshots, as well as confidential data from the

TABLE I: Vulnerabilities in NFV

ID	Vulnerability	Description
V01	Limited VM allocated memory	Attacker overwhelms VM allocated memory with fake requests causing service unavailable as long as vSwitch accepts as many flows as it can [11].
V02	Single server deployment	The virtualized guest environment is integrated with the host operating system; if there is lack of isolation, such integration allows guest to run malicious codes or bypass certain restrictions [17].
V03	Cross-VM shared memory vulnerability	When a malicious VM is co-resident with the target VM on the shared resources, an attacker can utilize a side channel to leak or learn information [17].
V04	Hypervisor scheduler failure	Attacker manipulates hypervisor scheduler and steals service time at the expense of co-residents in the shared virtualized resources [19].
V05	Lack of internal security	When the rules of administration for specific services are not clear and enforcement of role definition is poor, this may lead to having some insiders with unauthorized privileges. Moreover, inadequate physical security of resources may lead to this type of attacks [20].
V06	Integration complexity	Hypervisors, hardware, software add-ons, and VNFs could be offered by different vendors , and that may increase complexity during the communication and interaction process, which in turns creates security holes [21].
V07	Lack of hypervisor isolation	In NFV, hypervisor takes care of communication and isolation of different entities that create the VNF. If the attacker manages to hack into the hypervisor, he may be able to control the hypervisor giving himself extra resources. Another example is if the hypervisor failed to isolate two users, user A (the attacker) could send intensive traffic to user B in order to stop that user from accessing the service freeing up the resources for the attacker [15]. Possible reason for this threat is complexity in the hypervisor design or malicious device drivers [22].
V08	Unlimited allocation of resources	The service providers fail to model resources usage accurately and the usage of services may lead to overbooking or over-provisioning of the service, which may lead to unavailability of the service [20].
V09	Insecure interfaces and APIs	If the providers fail to secure the APIs, this may lead to jeopardize the system via weak credentials, insufficient authorization checks or insufficient validation that may make the service vulnerable [23].

TABLE II: Threats in NFV

ID	Threat	Description
T01	Denial of Service (DoS)	An attacker takes an excessive amount of resources making the system unable to satisfy requests from other users [11].
T02	Infrastructure integrity threat	An attacker pretends to be a service provider to try to appear as part of the real services of NFV to gain access to users' data [14].
T03	Misuse of resources	Using resource freeing attack, the attacker can free up some resources and uses them for his own benefit [15].
T04	Change in NFV function definition	An attacker modifies some of the operations in NFV functionality, definition, or even produces DoS. This is usually done by injection, [16].
T05	Privilege modification	Privileges of users can be changed using modifying non-control data attack, by upgrading or degrading their access to system entities in unauthorized manner [18].
T06	confidentiality attack based on Shared resources	Using side-channel attack, attackers can pull some private information about other users using a shared service in unauthorized manner [19].
T07	Malicious insider	Trusted members from inside the organization use their authority to access private data of users in unauthorized manner [24].

hard disk; or even relocates a users' VM to a malicious VM. Insiders are serious issue to service providers due to their possibly anonymous behaviour and knowledge of the system. Table 1 summarizes the vulnerabilities in NFV , and Table 2 summarizes the above threats .

IV. Countermeasures for NFV Threats

The described threats have countermeasures to mitigate them and prevent them from affecting the services; we describe some of them in this section.

DoS attack countermeasures: DoS/DDoS attacks can be mitigated using, for instance: firewalls, load balancers, etc.; however, these defences may not be successful due to the limited hardware resources of the target and the high traffic flow caused by such attack. Several papers have proposed various solutions to mitigate DoS/DDoS attacks on scalable and shareable systems. [26] has proposed a trace back model in cloud systems, called Cloud Trace Back (CTB), which aims to trace back and identify the source of the actual attacks. They also introduced Cloud Protector, a trained back propagation neural network, that detects and filters DDoS traffics; they claimed that their proposed model has successfully detected most the attacks within a short period of time. Also, [17] proposed a detection model that segregates VMs and its applications to a safer zone. In their approach, they have three types of traffics: normal, flash crowd, and DDoS traffic; when users send various service requests, the Decision Maker differentiates the three types of traffic using Outlier Analysis; the identified malicious traffic is sent to the Zone Manager, which in turn differentiates the flash crowd (overwhelmed legitimate) traffic from DDoS traffic. [27] proposed another approach to discriminate not only normal traffic, but even flash crowd traffic from DDoS traffic using hybrid probability metrics; also, their approach was able to detect the anomalous flows being DDoS flows or flash crowd flows. Moreover, [28] proposed a holistic two-stage mitigation framework by leveraging NFV and Software Defined Networks (SDN); the framework first screens and analyzes the flow traffic using algorithms and policies to classify the traffic based on the traffic pattern and packet features, then determines what next stage processes are needed for traffic flows; in case of malicious flood, the screener will request instantiation and scaling from the orchestrator in MANO for the required Virtual Security Function (VSF) based on the DDoS type of attack; however, in case of legitimate traffic flow, the screener will request to scale-up the capacity of the VNF to handle the traffic. Another mechanism that leverages the features of NFV is VFence; [29] used a DDoS traffic filtering agent to intercept packets and

verify their authenticity when the system is under attack. A load balancer technique is also used to direct the legitimate traffic to the right destinations, and the illegitimate one to the agent which then drops it down. [30], [31], [32] proposed other mitigation mechanisms for DoS/DDoS attacks that showed effective results. However, since DoS/DDoS is a broad topic on its own, there are several other mitigation mechanisms that are not mentioned in this paper.

Infrastructure integrity threat countermeasures: in order to ensure the security of different providers of VNF services, a suggested solution to achieve this security is creating a chain of trust as well as using a Trusted Platform Module (TPM) [8]; this includes introducing a new entity to take care of measuring the trustworthiness of each component of the system to ensure that all parts of the system are secure. [14] suggests an enhancement on MANO in NFV to include a trust manager in it. This particular enhancement should take care of the trust logic and automated control of the deployment of secure VNFs.

Misuse of resources countermeasures: A suggested solution is using an advanced hypervisor scheduler that provides fair share allocation among the processes, limiting the maximum amount allowed for each virtual service. However, this situation will affect the performance of the service [33].

Change in NFV function definition countermeasures: A suggested solution for malware-injection attacks is keeping a copy of the user virtual services on separate storage. A File allocation table (FAT) is utilized that contains information about the services and the software that the user is executing [34], [16]. Using that information the system can check for previous instances that had been executed by the user to ensure integrity and validity of the code. Other solutions to mitigate this attack is using frameworks such as CloudVal [35] that aims to validate the security of the hypervisor of the system by injecting faults into the system to detect vulnerabilities in NFVI.

Privilege modification countermeasures: A suggested solution is to use some framework that implements security layers on the virtualization environment, such as its done in the Xen Security Modules (XSM), which adds security constructs to protect the virtualization entity from unauthorized access by adding restrictive policies to access the resources [12]. [36] suggests using an additional restricted enterprise administration authorization system installed on user machines to prevent unauthorized access of the system, and prevent code altering of the system, yet giving the users some flexibility to configure the VMs to their needs .

Shared resources countermeasures: A suggested solution to mitigate side-channel attack is using a mechanism to limit the access to the Virtual Machine Images (VMI) and NFVI components and control the usage of the resources. This can be achieved by using a virtual firewall to prevent unauthorized access to the system [34]. Also, users can use a firewall to set some rules in order to filter activity in the service they are using and block it, thus preventing side channel attacks [37].

Malicious insider countermeasures: Insider attacks can be mitigated using several mechanisms; one of them is logging accesses within the NFV environment which can then be used for internal audits to detect suspicious activity [38]. Another mechanism is to set up strict policies for authentication and authorization for users who access VNFs beyond their access privilege, as well as applying the rule of least privilege where network service operators/managers should only have access to the necessary network resources. However, some of these mechanisms may detect the threat after it already took place. [39] proposes a framework that uses an attack tree to identify threats of authorized insiders by monitoring each users activity and map it to the possible activities that lead to compromise the system; they claimed that their approach detects malicious attacks from authorized insiders before they take place.

TABLE III: Relationship between threats and Countermeasures.

Threat	Threat description	Countermeasures
T01	An attacker takes an excessive amount of resources making the system unable to satisfy requests from other users [11].	Cloud Trace Back [26], outlier analysis traffic detection mechanism [17], traffic discrimination using probability metrics [27], traffic filtering mechanisms [28], [30], [31], [29], [32].
T02	An attacker pretends to be a service provider to try to appear as part of the real services of NFV to gain access to users data [14].	TPM and trust chains [8], and using MANO trust manager [14].
T03	Using resource freeing attack, the attacker can free up some resources and uses them for his own benefit [15].	Using advanced hypervisor scheduler [33].
T04	An attacker modifies some of the operations in NFV functionality, definition, or even DoS. This is usually done by injection [16].	A Using File Allocation Table (FAT) to keep a record of user activities [34], and CloudVal [35].
T05	Privileges of users can be changed using modifying non-control data attack, by upgrading or degrading their access to system entities in unauthorized manner [18].	Use firewalls on service [12], and apply a restricted enterprise administration authorization system in user machine [36].
T06	Using side-channel attack, attackers can pull some private information about other users using a shared service in unauthorized manner [19].	Use virtual firewalls on service [34].
T07	Trusted members from inside the organization use their authority to access private data of users in unauthorized manner [24].	Logging accesses within NFV environment to maintain privacy of user information from service operators [38]. Apply security policy and least privilege rule. Use attack tree approach [39].

Table 3 shows the mentioned threats and their possible countermeasures, and Table 4 shows the relationship between the threats, the vulnerabilities, and the possible countermeasures.

V. Research Directions & patterns

A. Trust Management of NFV

Trust management of NFV is a hot topic since there is no standard policy for trust and management of different NFVs.

TABLE IV: Relationship among threats, vulnerabilities, and possible countermeasures.

Threat	Vulnerability	Countermeasures
T01	V01, V08, V09	Cloud Trace Back [26], outlier analysis traffic detection mechanism [17], traffic discrimination using probability metrics [27], traffic filtering mechanisms [28], [29], [32], [31], [30].
T02	V06	TPM and trust chains [8], and using MANO trust manager [14].
T03	V04,V07	Using advanced hypervisor scheduler [33].
T04	V02,V09	Using File Allocation Table (FAT) to keep a record of user activities [34], and CloudVal [35].
T05	V02	Use firewalls on service [12], and apply a restricted enterprise administration [36]
T06	V03, V04, V09	Use virtual firewalls on service [34].
T07	V05	Logging accesses within NFV environment to maintain privacy of user information from service operators [38]. Apply security policy and least privilege rule. Use attack tree approach [39].

Since NFV relies on different vendors and each of these vendors uses its own software, this raises two challenges: interoperation integrity and communication between different vendors . There are four main areas to create trust chains between NFV vendors [40], which are: I. Hardware-based roots of trust, II. Software-based roots of trust, III. Certificate-based roots of trust, and IV. Validation guidance for non-repudiation. Some of the stored data in one entity could be private; how one entity could encrypt these data and keep them private, especially if other vendors need access to some of the data, is considered an important issue. Key distribution could challenge trustworthiness between NFV entities considering that several services could be provided to users by different providers. For that reason, a pattern could be created in the future that ensures trustworthiness of hardware and software roots for the NFV.

Further, due to the unique characteristic of the NFV environment, different network functions can be created and terminated dynamically on different and distributed entities that when combined create the network management of different entities. NFV frameworks have to ensure that all entities are up to date with the latest security patchs, especially that a big part of the NFV architecture relies purely on software. In order to achieve automated security management for NFV a new standard has been introduced by ETSI, called NFV Security Lifecycle Management [41]. A major difference between non-virtualized deployment and virtualized deployment of networks is that in the first most of the functional components are standardized while on the later this is not the case. In NFV many different interfaces create the NFVI. Also, not all of them are visible to each other which makes creating security management a challenging task. According to [41], security lifecycle management of NFV runs through three main stages which are: security planning, security enforcement and finally security monitoring (Figure 2); yet, currently there is no complete model that covers security management and there is no model for security monitoring in NFV.

Fig. 2: Security Lifecycle Management in NFV [41]

B. Infrastructure Design

The infrastructure design of NFV creates new challenges because NFV has several characteristics that differ than regular networks. Due to these characteristics, availability and reliability requirements in such environment are very stringent. If one particular part of the network is not available, this will affect the Quality of Service (QoS) for the entire service, and since NFV relies on both hardware and software this makes ensuring reliability of the service even harder.

Moreover, latency is one of the most critical attributes in such services and since several entities may contain different types of virtual machines, this may introduce latency in the integration of different components of the network, which will affect the QoS. This creates a challenge that has to be undertaken during the design process of the infrastructure of NFV.

During the design process, NFV vendors have to define service level agreements, which offer to users the percentage of reliability and availability for the product they are providing, yet unlike other products in NFV the focus is shifted from per network element to end to end service. Generally availability, reliability and quality of service need to be ensured during the design of NFV which creates new challenges that need to be undertaken in order to provide reliable services for the users.

C. NFV Monitoring

Since some users will use a limited number of services, this will introduce the need of additional systems to monitor and analyze end to end infrastructure between the service providers and users. NFV security monitoring is also an open challenge that faces the design and implementation of NFV. A complete new methodology to monitor the security of different components of NFV is required due to the unique aspects of NFV, including multi-tenancy and multi control domains in NFV as well as the distributed and shared infrastructure between the different vendors for NFV. Moreover, since in NFV both legacy and virtualized networks could work together in complex manners to provide the required services, this makes the process of monitoring security risks even more challenging [42]. Having different interfaces in the virtualized

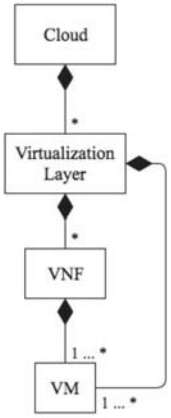

Fig. 3: NFV architecture pattern [43]

network with many of them lacking standardized design makes exploitation of vulnerabilities in the network and tracking separation of malware across the network an even harder task. Therefore, a standardized design for the general infrastructure of NFV is needed. Moreover, in NFV, security monitoring should also include the monitoring of data flow and packet delivery to ensure that all transformations are legal and dont overwhelm the network causing latency in the network.

D. Patterns

A future direction is to model the security threats of NFV using patterns. A pattern encapsulates a solution to a recurring problem in a specific context [9]. Patterns can be used to model and design complex systems as well as improve the quality of systems. Further, there are several types of patterns including: analysis patterns, design patterns, architecture patterns, security patterns and misuse patterns, as well as other variety of patterns that help define in a systematic way how to create defenses for the threats mentioned in this paper. Normally, a pattern solution is represented using a UML class diagram, a sequence diagram and maybe a state or activity diagram. Patterns can provide solutions to enhance the security of NFV systems; so far only one pattern that describes the NFV architecture has been published [43]; Figure 3 is the class diagram for the solution of that pattern.

Various patterns could be designed for NFV. For instance, misuse patterns can be used to model and enumerate NFV threats; to do so, a full understanding to NFV component architecture is needed and how attackers compromise these components to fulfill their objectives. Further, security patterns can then be used to control the identified threats. Possible security patterns are a secure hypervisor pattern, and a pattern to secure the communication between different functions that are provided by different vendors. A security reference architecture for NFV could be built by combining several related security patterns.

Several patterns could be designed that will mitigate the severity of threats that may face NFV and provide systematic solutions for NFV security; for instance, a pattern for hypervisor security; such pattern should cover how to secure the connections between different VMs as well as the connections between VMs and hardware resources. Moreover, it should also ensure the security of the applications running in each VM and ensure that it doesnt jeopardize its own VM or other VMs. Another pattern that could be designed to improve the security of NFV is a pattern to secure the MANO of NFV. Such pattern should ensure the secure interaction among the manager of a VNF, the security orchestrator, and the Element Management Systems (EMS) [8]; it would include setting the scaling boundaries in VNF Descriptor (VNFD). Other patterns could be created to ensure the security of virtual volume disks associated with each VNF since they contain sensitive data related to users, and a pattern that ensures a secure network virtualization. Further, several patterns that are already created for cloud systems such as: secure virtual machine image repository, cloud policy management point [44], and virtual machine environments (VME) [45], as well as authorization, authentication, and logging/auditing are necessary security mechanisms that [9] has patterns for them, all of which can be applied to NFV due to the similarities in underlying characteristics of NFV and cloud computing.

VI. Conclusion

NFV is a new technology that has a huge potential and will provide many benefits for Telecommunication Service Providers (TSP) by reducing the cost of setting-up a network, enhance it and allowing dynamically deploy some services to the users. However, this new technology should be secured from insider and outsider attacks, keeping in mind that this service has its own infrastructure with different entities that need to be analyzed critically in order to understand possible threats and vulnerabilities. In this paper, we gave an overview of different security attacks. We also provided countermeasures for common attacks that could mitigate the severity of NFV threats. However, the security of NFV is still a subject under study with many security challenges that need to be considered. The paper also defines some future directions to provide solutions and enhancements to the security of NFV, such as creating new security patterns for different entities and components of NFV to provide reliable and secure service to the users. Moreover, currently NFV lacks experimental implementation to understand its weaknesses and drawbacks.

References

[1] G. ETSI, "Network functions virtualisation (nfv): Architectural framework," *ETsI Gs NFV*, vol. 2, no. 2, p. V1, 2013.

[2] Alcatel-Lucent, "New bell labs application able to measure the impact of technologies like sdn & nfv on network energy consumption," *New Bell Labs*, 2015.

[3] M. Chiosi, "Network functions virtualization: Network operator perspectives on industry progress, 20 p," 2015.

[4] M. D. Firoozjaei, J. P. Jeong, H. Ko, and H. Kim, "Security challenges with network functions virtualization," *Future Generation Computer Systems*, vol. 67, pp. 315–324, 2017.

[5] M. Pattaranantakul, R. He, A. Meddahi, and Z. Zhang, "Secmano: Towards network functions virtualization (nfv) based security management and orchestration," in *Trustcom/BigDataSE/I SPA, 2016 IEEE*. IEEE, 2016, pp. 598–605.

[6] F. Reynaud, F.-X. Aguessy, O. Bettan, M. Bouet, and V. Conan, "Attacks against network functions virtualization and software-defined networking: state-of-the-art," in *NetSoft Conference and Workshops (NetSoft), 2016 IEEE*. IEEE, 2016, pp. 471–476.

[7] W. Yang and C. Fung, "A survey on security in network functions virtualization," in *NetSoft Conference and Workshops (NetSoft), 2016 IEEE*. IEEE, 2016, pp. 15–19.

[8] S. Lal, T. Taleb, and A. Dutta, "Nfv: Security threats and best practices," *IEEE Communications Magazine*, vol. 55, no. 8, pp. 211–217, 2017.

[9] E.B.Fernandez, "security patterns in practice: Building secure architectures using software patterns, wiley series on software design patterns," 2013.

[10] Radware, *DDoS Warriors: The Ultimate Resource For Everything You Need to Know about DDoS Attacks Today and Cyber Security*, https://security.radware.com/, version 1.

[11] Romo, Van, Dijkhuizen *et al.*, "Practical security analysis of openflow," *University of Amsterdam, Amsterdam*, 2013.

[12] W. Han, Y. He, and L. Ding, "Verifying the safety of xen security modules," in *Secure Software Integration & Reliability Improvement Companion (SSIRI-C), 2011 5th International Conference on*. IEEE, 2011, pp. 30–34.

[13] ETSI, *Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments, 2017*.

[14] D. B. Marco and L. Antonio, "On the establishment of trust in the cloud-based etsi nfv framework," 2017.

[15] V. Varadarajan, T. Kooburat, B. Farley, T. Ristenpart, and M. M. Swift, "Resource-freeing attacks: improve your cloud performance (at your neighbor's expense)," in *Proceedings of the 2012 ACM conference on Computer and communications security*. ACM, 2012, pp. 281–292.

[16] K. Zunnurhain and S. V. Vrbsky, "Security attacks and solutions in clouds," in *Proceedings of the 1st international conference on cloud computing*, 2010, pp. 145–156.

[17] E. P. Krishna, E. Sandhya, and M. G. Karthik, "Managing ddos attacks on virtual machines by segregated policy management," *Global Journal of Computer Science and Technology*, vol. 14, no. 6-E, p. 19, 2014.

[18] B. Ding, Y. He, Y. Wu, and J. Yu, "Systemic threats to hypervisor non-control data," *IET information security*, vol. 7, no. 4, pp. 349–354, 2013.

[19] F. Z. M. G. P. Desnoyers and R. Sundaram, "Scheduler vulnerabilities and coordinated attacks in cloud computing."

[20] D. Catteddu, "Cloud computing: benefits, risks and recommendations for information security," in *Web application security*. Springer, 2010, pp. 17–17.

[21] B. Han, V. Gopalakrishnan, L. Ji, and S. Lee, "Network function virtualization: Challenges and opportunities for innovations," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 90–97, 2015.

[22] R. Chandramouli, "Security recommendations for hypervisor deployment on servers," *NIST Special Publication*, vol. 800, p. 125A, 2018.

[23] D. Hubbard, M. Sutton *et al.*, "Top threats to cloud computing v1. 0," *Cloud Security Alliance*, pp. 1–14, 2010.

[24] F. Rocha and M. Correia, "Lucy in the sky without diamonds: Stealing confidential data in the cloud," in *Dependable Systems and Networks Workshops (DSN-W), 2011 IEEE/IFIP 41st International Conference on*. IEEE, 2011, pp. 129–134.

[25] N. ISG, "Network function virtualisation (nfv)-resiliency requirements,," *ETSI GS NFV-REL*, vol. 1, p. v1, 2014.

[26] B. Joshi, A. S. Vijayan, and B. K. Joshi, "Securing cloud computing environment against ddos attacks," in *Computer Communication and Informatics (ICCCI), 2012 International Conference on*. IEEE, 2012, pp. 1–5.

[27] K. Li, W. Zhou, P. Li, J. Hai, and J. Liu, "Distinguishing ddos attacks from flash crowds using probability metrics," in *Network and System Security, 2009. NSS'09. Third International Conference on*. IEEE, 2009, pp. 9–17.

[28] T. Alharbi, A. Aljuhani, and H. Liu, "Holistic ddos mitigation using nfv," in *Computing and Communication Workshop and Conference (CCWC), 2017 IEEE 7th Annual*. IEEE, 2017, pp. 1–4.

[29] A. Jakaria, W. Yang, B. Rashidi, C. Fung, and M. A. Rahman, "Vfence: A defense against distributed denial of service attacks using network function virtualization," in *Computer Software and Applications Conference (COMPSAC), 2016 IEEE 40th Annual*, vol. 2. IEEE, 2016, pp. 431–436.

[30] S. K. Fayaz, Y. Tobioka, V. Sekar, and M. Bailey, "Bohatei: Flexible and elastic ddos defense." in *USENIX Security Symposium*, 2015, pp. 817–832.

[31] C. J. Fung and B. McCormick, "Vguard: A distributed denial of service attack mitigation method using network function virtualization," in *Network and Service Management (CNSM), 2015 11th International Conference on*. IEEE, 2015, pp. 64–70.

[32] B. Rashidi and C. Fung, "Cofence: a collaborative ddos defence using network function virtualization," in *Network and Service Management (CNSM), 2016 12th International Conference on*. IEEE, 2016, pp. 160–166.

[33] Z. Mahmood, *Cloud Computing: Challenges, Limitations and R&D Solutions*. Springer, 2014.

[34] P. Kumar, "Cloud computing: Threats, attacks and solutions," *International Journal of Emerging Technologies in Engineering Research (IJETER)*, vol. 4, 2016.

[35] C. Pham, D. Chen, Z. Kalbarczyk, and R. K. Iyer, "Cloudval: A framework for validation of virtualization environment in cloud infrastructure," in *Dependable Systems & Networks (DSN), 2011 IEEE/IFIP 41st International Conference on*. IEEE, 2011, pp. 189–196.

[36] ETSI, *Network Functions Virtualisation (NFV); Infrastructure; Hypervisor Domain , 2015*.

[37] L. S. Indrusiak, J. Harbin, and M. J. Sepulveda, "Side-channel attack resilience through route randomisation in secure real-time networks-on-chip," in *Reconfigurable Communication-centric Systems-on-Chip (ReCoSoC), 2017 12th International Symposium on*. IEEE, 2017, pp. 1–8.

[38] B. Ruppert and R. Wanner, "Protecting against insider attacks," *SANS Institute InfoSec Reading Room*, 2009.

[39] I. Ray and N. Poolsapassit, "Using attack trees to identify malicious attacks from authorized insiders," in *European Symposium on Research in Computer Security*. Springer, 2005, pp. 231–246.

[40] N. F. Virtualisation, "Nfv security; security and trust guidance," 2017.

[41] ETSI, *Network Functions Virtualisation (NFV) Release 3; Security; Security Management and Monitoring specification, 2017,ETSI GS NFV-SEC 013 V3.1.1 (2017-02)*.

[42] Intel, *security Considerations for Network Functions Virtualization for Communications Service Providers*.

[43] E. B.Fernandez and B. Hamid, "A pattern for network functions virtualization," in *A pattern for Network Functions Virtualization, 21st European Conf. on Pattern Languages of Programs (EuroPLoP 2015, ACM 2015*.

[44] E. B. Fernandez, R. Monge, and K. Hashizume, "Two patterns for cloud computing: Secure virtual machine image repository and cloud policy management point," in *Proceedings of the 20th Conference on Pattern Languages of Programs*. The Hillside Group, 2013, p. 15.

[45] M. H. Syed and E. B. Fernandez, "A pattern for a virtual machine environment," in *Proceedings of the 23rd Conference on Pattern Languages of Programs*. The Hillside Group, 2016.