Computer Networks 197 (2021) 108288

Contents lists available at ScienceDirect

Computer Networks

journal homepage: www.elsevier.com/locate/comnet

Survey paper

NFV security survey in 5G networks: A three-dimensional threat taxonomy

Taous Madi[1,*], Hyame Assem Alameddine[1], Makan Pourzandi, Amine Boukhtouta

Ericsson Security Research, Montreal, Quebec, Canada

ARTICLE INFO

Keywords:
Security
Network function virtualization
5G networks
Business model
Multi-site deployment
Multi-domain deployment

ABSTRACT

Fifth Generation (5G) networks aim at providing value-added services with advanced performance such as low-latency communications, high reliability, high data rates and capacity to support an increasing number of connected devices. 5G networks are enabled by an automated and flexible provisioning and management of resources and services deployed over a shared infrastructure spanning multiple sites and domains and governed by different business players. This drives towards a complex 5G ecosystem enabled by Network Function Virtualization (NFV) and promoted by multiple business collaborations which draw new threats and vulnerabilities that are yet to be explored. Thus, we explore in this survey the complexity of the 5G ecosystem and derive a 5G telecommunication business model driven by 5G enabling technologies. We use this business model to identify new attack surface and security threats introduced by multiple business collaborations supported by NFV which we overview. Further, we delineate a three dimensional threat taxonomy for NFV-based 5G networks that leverages NFV architecture and deployment use cases in light of different 5G business collaboration scenarios. Finally, we shed light on insightful future research directions towards providing enhanced security in NFV-based 5G networks.

1. Introduction

The evolution towards Fifth Generation (5G) mobile networks is changing current network architecture and management techniques while transforming existing telecommunication business models [3,4]. 5G networks depart from a controlled ownership of its infrastructure for service provisioning to leverage a service-oriented business model supported by a unified management framework control alleviated by virtualization and softwarization [5]. 5G adopts a service-based architecture in which network functions cooperate to provide services to each others in order to achieve a system functionality [6,7]. 5G rethinks end-to-end service design, provisioning and management through enabling new network capabilities to provide multi-tenant, multi-operator, multi-domain services with exceptional Quality of Service (QoS) tailored upon the need of different industry verticals such as those related to automotive, agriculture, city management, government, health care, manufacturing, etc. [5,8]. Network slicing has been introduced to support these new classes of traffic and services by slicing the common network infrastructure into multiple logical ones, each satisfying specific QoS requirements [9]. Fig. 1 depicts a high level overview of a 5G network supporting different vertical industries deployed over multiple network slices.

1.1. 5G networks and their enabling technologies

5G is transforming the way networks operate by re-architecting them to enable flexible, agile and programmable networks supporting (semi-) autonomous deployment and life-cycle management of multiple services over distributed computing environment and network infrastructure spanning different geographical locations and administrative domains [10,11]. 5G supports optimized resource utilization and cost-efficient service provisioning for multiple tenants [3,5].

Network Function Virtualization (NFV) and Software Defined Networks (SDN) are key-enabling technologies of 5G leveraging virtualization and softwarization. While NFV provides a drastic transformation of legacy networks by consolidating software instances of network functions on a range of industry-standard hardware, SDN comes into play to enable programmable networks allowing automated traffic route selection and management [12,13]. 5G will benefit from recent advancements in cloud and edge computing to respond to the ultimate ultra-low latency and high reliability requirements of many Internet of Things (IoT) enabled services such as those related to self-driving cars, virtual and augmented reality, among others [14]. More precisely, Multi-access Edge Computing (MEC) will play a vital role for low-latency services by enabling IoT devices to offload their mission critical

* Corresponding author.
E-mail address: taous.madi@ericsson.com (T. Madi).
[1] The two authors contributed equally to the work.

https://doi.org/10.1016/j.comnet.2021.108288
Received 8 April 2021; Received in revised form 25 June 2021; Accepted 1 July 2021
Available online 8 July 2021

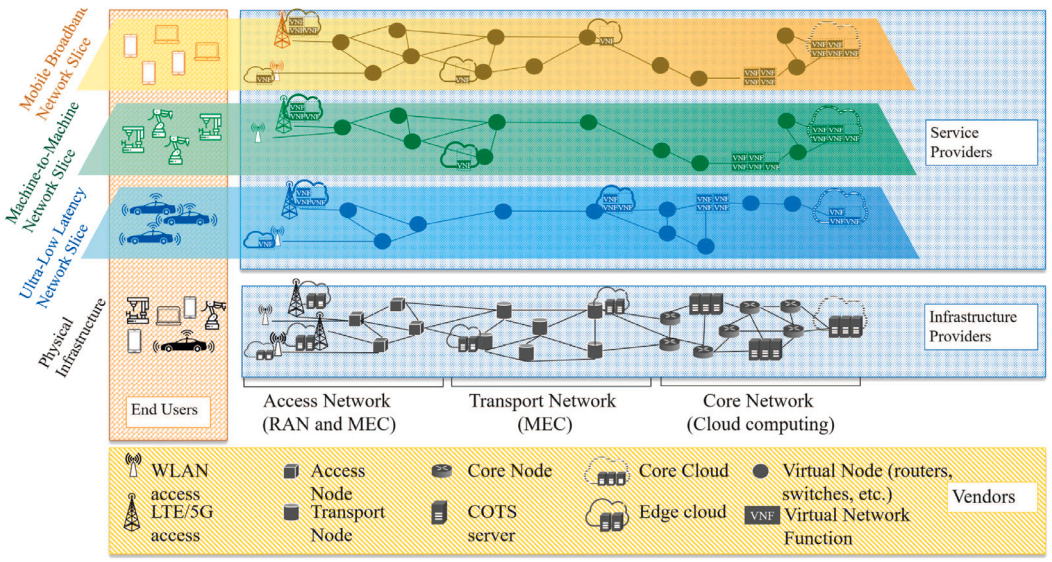


Fig. 1. 5G ecosystem [1,2].

tasks to be processed by computing resources brought to the edge of the network [15–17]. Network slicing encompasses all the aforementioned technologies to enable different classes of services.

From Fig. 1, one can note that 5G spans multiple geographical locations while encompassing different network types such as Radio Access Networks (RANs), transport and core networks supporting edge and cloud computing. These network infrastructures are deployed by infrastructure providers and leased by service providers who offer their services to different vertical industries in terms of network slices.

1.2. Security in NFV-based 5G networks

The 5G ecosystem promotes an open, collaborative, flexible and automated environment encompassing multiple technologies, administrative domains, sites and tenants, which introduces new vulnerabilities and threats in NFV-based 5G networks. These threats can affect the service availability, the reputation of the attacked business players and the privacy of their customers among others. For instance, the worldwide semiannual security spending guide from International Data Corporation reported an annual growth rate of 9.2% over the 2018–2022 forecast period with a total of 133.8 billion in 2022 [18].

The wide adoption of virtualization technologies in 5G networks such as NFV is constrained by the security threats and vulnerabilities it introduces. NFV-based networks not only inherit the security aspects of virtualization but also introduce a new attack surface attributed to the NFV architecture that encompasses different communicating entities spanning the physical infrastructure, the virtual and service layers in addition to the orchestration one [19]. Further, the security of 5G telecommunication networks adopting NFV is affected by the new service-oriented telecommunication business model where resource management and orchestration can be governed by different actors (e.g., infrastructure providers, service providers, etc.). Nonetheless, the automated provisioning and life cycle management of services account for security policies that can be easily violated due to non-trivial service complexity and administrative errors [12]. In addition, the proliferation of IoT devices provide a fertile ground of attacks on the NFV-based 5G networks since they form an integral part of a network slice and require specific QoS and security requirements for their services [9]. IoT devices are characterized by a variety of hardware and software along with insecure design and a lack of firmware update which make them vulnerable to multiple attacks such as Mirai [20,21]. A Mirai botnet can be employed to launch a signaling storm on the RAN, in addition to Distributed Denial of Service (DDoS) attacks on the 5G core which can be further amplified by the centralized management and orchestration provided by NFV [21,22].

Hence, despite the tremendous advantages brought by NFV to 5G networks ranging from flexibility, manageability, reduced time to market among others; a large set of security challenges are yet to be identified and addressed given the large scale deployment of NFV that spans a wide range of data centers and security domains [12]. Many works in academia and industry explored NFV benefits, architecture and its relation with SDN and cloud computing [23–26]. Nonetheless, only few addressed the security concerns brought by NFV [12,27–29]. However, these works overlook the security implications related to the collaborative 5G ecosystem promoting heterogeneous deployment approaches. In addition, they do not discuss the impact of such deployment strategies on the centralized management and orchestration functionality guaranteed by NFV and the new resulting attack surface.

1.3. Contributions

In this paper, we address these gaps by elaborating on the new business model and analyzing its security repercussions on the NFV deployments. More specifically, our contributions can be summarized as follows:

- We investigate the 5G ecosystem and its different enabling technologies with a focus on NFV and its architecture. We then derive a 5G business model that reflects the heterogeneity of the 5G ecosystem in terms of enabling technologies, multi-operators and multi-tenancy.
- We analyze the 5G ecosystem, derive a business model and expose the influence of this service-based environment on the deployment and management of the components of the NFV architecture by different operators. To the best of our knowledge, we are the first to highlight multiple deployment models of the NFV architecture in the complex 5G environment and discuss their impact on network security.
- We present a three Dimensional (3D) threat taxonomy that captures the shared security risks brought by the discussed NFV deployment models as a result of the existing business interactions. Unlike existing works that only discuss threats and vulnerabilities introduced by virtualization and softwarization at each layer of the NFV architecture, we investigate threats at inter-layer, intra-layer and inter-administrative domains dimensions. Our proposed taxonomy provides a holistic threat and attack analysis exposing

non-explored threat boundaries resulting from the 5G business model along with the NFV deployment approaches.
- We highlight different lessons learned inspired by existing advancements on NFV security solutions and our 3D threat taxonomy.
- Finally, we draw insightful future research directions promoting collaborations between different network operators in order to guarantee a secure 5G NFV-based ecosystem.

1.4. Paper organization

Our survey is organized as follows: Section 2 reviews the literature. Section 3 presents NFV and its architecture. Section 4 provides a comprehensive and comparative analysis of the traditional and new telecommunication business model. Section 5 discusses different deployment use cases. Section 6 and Section 7 delineates an in-depth study of a novel NFV 3D threat taxonomy. An overview of different NFV security projects is presented in Section 8. Section 9 summarizes the lessons learned related to NFV threats, vulnerabilities and their associated security solutions. Future research directions are elucidated in Section 10. We conclude in Section 11. Our survey's outline is detailed in Fig. 2 to allow a reading "à la carte". Furthermore, a list of abbreviations is summarized in Table 1.

2. Related works

NFV is closely related to cloud computing and SDN as they complement its purpose in offering services in an agile, cost and resource efficient way. While cloud computing accelerates NFV adoption by providing on demand resource provisioning suitable for virtual network functions deployment; SDN introduces programmability to the network by enabling automated chaining of network functions to provide a service [23]. As virtualization is the main driver of cloud computing and NFV, they both share multiple security threats and vulnerabilities. While SDN security can affect network services provided by NFV, security issues in SDN networks are highly related to the openFlow protocol [30] and the adopted SDN architecture. Thus, we refer the reader to the following works [31–39] for more details on SDN security. In the following sections, we provide a brief review of the literature on security surveys in cloud computing and NFV in order to identify their common attack surface, discuss NFV security and shortcomings of the literature in the latter area. As the present survey discusses the NFV security in 5G networks, we also present a literature review on existing surveys on 5G networks and their security.

2.1. Existing surveys on cloud computing security

Cloud computing accounts for a multi-tenant model leveraging a shared infrastructure between different tenants through the employment of different virtualization technologies. The security issues in cloud computing are classified into five categories comprising: (1) security standards to dictate security policies in the cloud, (2) network security involving network attacks, (3) authentication, privacy and access control, (4) cloud infrastructure attacks such as those related to privileged insiders, and (5) data security issues including data migration, integrity, confidentiality, etc.[40]. Surveys on cloud computing security focus on exploring threats and vulnerabilities related to one or many of the aforementioned categories. Khalila et al. [40] follow the aforementioned categorization, identify and discuss 28 cloud security issues related to misconfigurations, malicious insiders, side channels, among others. Similar attacks and their related solutions are explored in [41]. Bhadauria et al. [42] present cloud computing and its barriers then discuss security threats at the network, data and application levels before suggesting different security enforcement schemes. Other works [43–46] present a list of security threats and vulnerabilities in the cloud, most of which are related to virtualization, network, application and cloud infrastructure. Privacy in the cloud also gained a significant attention. Surveys such as [47–51] discussed trust, authentication and confidentiality in the cloud. Privacy preserving approaches in the cloud are explored in [52]. MEC, which is considered as an extension of cloud computing to the edge network, was surveyed in [53]. The latter work discusses and presents security threats related to edge devices along with access, edge and core networks.

Table 1
List of acronyms.

1G	First Generation Network
4G	Fourth Generation Network
5G	Fifth Generation Network
5G PPP	5G Infrastructure Public Private Partnership
AD	Administrative Domain
AMF	Access and Mobility Management Function
API	Application Programming Interfaces
BSS	Business Support System
CAPEX	Capital Expenditure
CDN	Content Delivery Network
CIDS	Collaborative Intrusion Detection Systems (CIDS)
COTS	Commercial-off-The-Shelf
CRN	Cognitive Radio Network
CTI	Cyber Threat Intelligence
DDOS	Distributed Denial of Service
DoS	Denial of Service
DPI	Deep Packet Inspector
DRAM	Dynamic Random Access Memory
EDoS	Economic Denial of Sustainability
ETSI	European Telecommunication Standards Institute
GRE	Generic Routing Encapsulation
HSS	Home Subscriber Server
IDN	Intrusion Detection Network
IoT	Internet of Things
ISP	Internet Service Provider
MANO	Management and Orchestration
MEC	Multi-Access Edge Computing
MLPOC	Multiple Point of Contact
NAT	Network Address Translation
MNO	Mobile Network Operator
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NFVO	Network Function Virtualization Orchestrator
NS	Network Service
NSD	Network Service Descriptor
NSM	Network security Manager
OPEX	Operational Expenditure
ONAP	Open Network Automation Platform
OSS	Operation Support System
PNF	Physical Network Function
PoP	Point-of-Presence
RAN	Radio Access Network
RoP	Return Oriented Programming
SDN	Software Defined Networking
SLPOC	Single Logical Point of Contact
SMF	Session Management Function
SSL	Secure Socket Layer
TLS	Transport Layer Security
TPM	Trusted Platform Module
vFW	Virtual Firewall
VIM	Virtualised Infrastructure Manager
VLD	Virtual Link Descriptor
VM	Virtual Machine
VNF	Virtual Network Function
VNFC	Virtual Network Function Component
VNFD	Virtual Network Function Descriptor
VNF-FG	Virtual Network Function Forwarding Graph
VNF-FGD	Virtual Network Function Forwarding Graph Descriptor
VNFM	Virtual Network Function Manager
VSF	Virtual Security Function
vTPM	Virtual Trusted Platform Module
QoS	Quality of Service
VLAN	Virtual Local Area Network
VXLAN	Virtual Extensible Local Area Network
WAN	Wide Area Network
WIN	Wide Area Network Infrastructure Manager

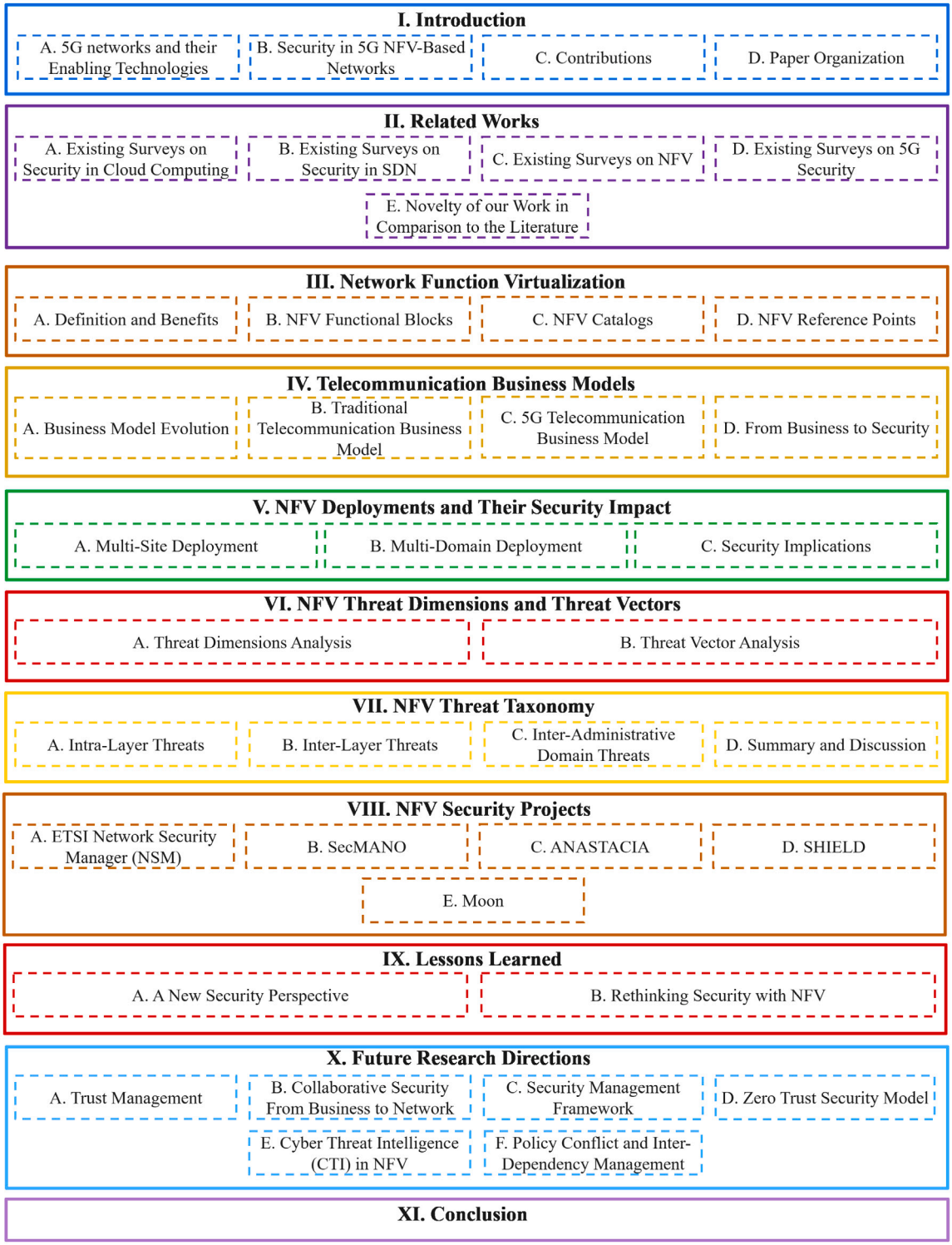


Fig. 2. Survey outline.

Even though security issues identified and studied in the context of cloud computing remain valid in NFV, the latter introduces new threats which need to be explored.

2.2. Existing surveys on NFV

Multiple surveys on NFV aim at providing a clear vision on NFV technology through exploring its architecture, benefits and relationships [23]. Others discuss the state-of-the-art of NFV and its challenges with respect to the software-defined NFV architecture [24]. Mijumbi et al. [26] focus on the management and orchestration challenges in NFV while the authors of [25] explain the implementation aspects of each layer in the NFV architecture. While these works present an in-depth study on NFV challenges, opportunities and future research directions, they overlook the security in NFV.

NFV security is discussed in [12]. The authors of [12] analyze security threats following the different layers of the NFV architecture. The authors present a set of recommendations to secure NFV-based services

and discuss several future research directions. Reynaud et al. [27] survey the attacks that can be performed against SDN and NFV and propose countermeasures to mitigate them. Lal et al. [28] focused on threats targeting the NFV Infrastructure (NFVI) and discuss some security practices to mitigate them. The authors of [29] address threats in an IoT environment and analyze security features brought by NFV and SDN to react to IoT security threats.

2.3. Existing surveys on 5G security

As 5G networks are enabled by NFV, reviewing the work on 5G security is inevitable. Khan et al. [54] discuss security and privacy issues in 5G networks while tackling security issues related to 5G enabling technologies such as MEC, NFV, SDN and network slicing. They focus on physical layer security and analyze ongoing projects on the security of 5G networks. While the authors present threats, vulnerabilities and security challenges in NFV; their work remains brief and limited to threats hindering each layer of the NFV architecture. Security challenges in 5G networks were discussed in [22] and [55] in which the authors overview security issues related to MEC, NFV and SDN along with those related to different parts of the network such as access network and core network. They further present solutions and future research directions to solve these challenges. Security issues in NFV were overlooked in [56] in which the authors focus on security mechanisms, requirements, vulnerabilities, solutions and future research directions related to new features and techniques in 5G networks. Other work on 5G security presents a robust security scheme to secure 5G networks against major security threats such as authentication handover, flow table overloading attack, and DDoS attack in the network [57].

Security of 5G networks involved as well discussions on the security issues in Cognitive Radio Networks (CRNs). CRNs support cognitive radio technology that aims at improving spectrum utilization by allowing the unlicensed secondary users to use the channels that are not currently used by the licensed primary users via spectrum-sensing technology [58]. Hence, this technology enables 5G networks in supporting the tremendous increase of IoT devices and traffic loads [59]. Nonetheless, CRNs suffer from multiple security threats such as primary user emulation attack, falsifying data, DoS attack, eavesdropping and tampering among others that are discussed in [58,60–62]. As CRN security problems are related to the spectrum resource allocation and usage, we leave them out of the scope of this paper which targets security issues related to NFV.

2.4. Novelty of our work in comparison to the literature

- *With respect to cloud computing surveys:* As NFV is enabled by virtualization and use the cloud computing infrastructure, it inherits many of their security issues. Nonetheless, the layered architecture of NFV (Fig. 3) depicting a service layer and logically centralized management and orchestration layer running on top of the network infrastructure introduces new threats and vulnerabilities.
- *With respect to NFV surveys:* Most of the aforementioned works on NFV security [12,27–29] present the NFV threat taxonomy with respect to the NFV architecture layers proposed by the European Telecommunications Standards Institute (ETSI) [63]. Nonetheless, these surveys fall short in considering the interactions between the layers of the NFV architecture, their point of contacts and their implications on NFV security. Further, they do not account for the different 5G use cases where the physical/virtual networks ownership can be shared between multiple business actors (i.e., infrastructure provider, service provider, etc.). Unlike the works in the literature, we alleviate the business relationship between different operators to provide an FV in-depth study on security challenges in NFV. We do not only focus on threats and vulnerabilities emerging from the virtualized infrastructure but we also adopt a three dimensional threat taxonomy that accounts for both the NFV architecture and the security implications of its possible business based network deployment models. We draw attention on new attacks and vulnerabilities that are highly coupled with the centralized management offered by NFV.
- *With respect to 5G security surveys:* Existing work on 5G security [22,54–56,64] focus on security challenges related to the radio and physical aspects of 5G networks and their recent technologies (e.g., massive MIMO, mmwave, etc.). They briefly discuss security challenges and solutions in NFV, mainly those related to softwarization and virtualization with respect to each layer of the NFV architecture. Hence, they lack an in-depth analysis of threats and vulnerabilities in NFV emanating from the interaction and communication between the different layers of its architecture along with the deployment of the latter in a 5G network. While addressing security challenges in 5G networks related to RAN and its emerging technologies is left out of the scope of this survey, we study in this work the impact of NFV on the security of 5G networks and, the other way around, the impact of the 5G ecosystem on NFV security.

3. Network function virtualization overview

Network and telecommunication operators were looking for new approaches in order to simplify the management and scaling of their network. NFV yields a new technique that responds to their needs.

3.1. Definition and benefits

Service provisioning in the telecommunication industry has traditionally required deploying physical equipment at multiple locations of the network for each function composing the service. These hardware functions are expensive and require trained personnel to be managed [23,26].

NFV allows overcoming this burden by decoupling the software from the hardware. In fact, NFV implements network functions as software called Virtual Network Functions (VNFs), that can run on top of Virtual Machines (VMs) or containers deployed on Commercial-Off-The-Shelf (COTS) servers [23,63]. This decoupling helps in reassigning and sharing the physical infrastructure among different software. The latter can thus be easily instantiated or relocated to different NFV Infrastructure Points-of-Presence (NFVI-PoPs) [63]. An NFVI-PoP consists of computing, storage and networking resources deployed by a network operator and used to run VNFs [63]. This virtualization of network functions allows network and telecommunication operators to automatically instantiate, provision and manage Network Services (NSs), thus, reducing the time to market [63].

3.2. NFV functional blocks

The NFV architecture is defined by ETSI in [63] and is captured in Fig. 3. It is composed of the following functional building blocks:

- *NFV Infrastructure (NFVI):* The NFVI incorporates physical and virtual resources including network, storage and compute resources that build up the environment in which the VNFs are deployed, managed and executed [63]. Physical resources provide processing through COTS, storage and connectivity to VNFs through the virtualization layer (e.g., hypervisor). Virtual resources running on top of the virtualization layer, allow the logical partitioning of physical resources to be allocated to different VNFs while ensuring their isolation. Virtual resources can be VMs managed by a hypervisor or can include containers or any other virtual technology [23,63]. NFVI can span different locations and hence, might have multiple NFVI-PoPs belonging to one or multiple operators.

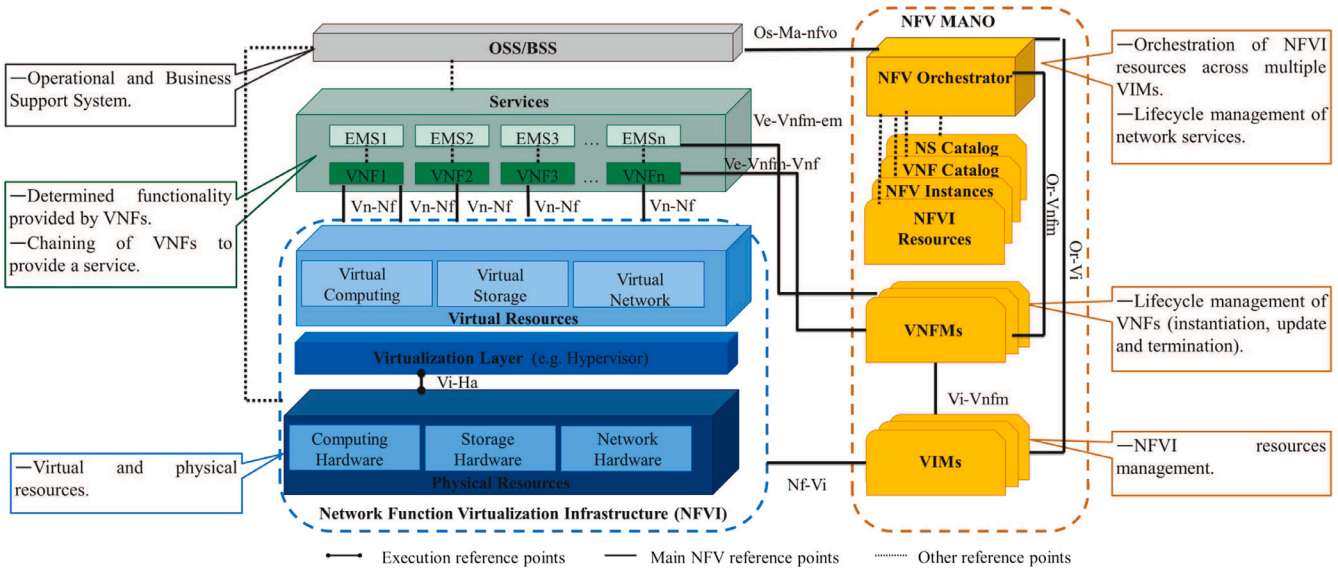


Fig. 3. ETSI NFV architecture [63,65].

- *VNF and Services:* A VNF is a software implementation of a network function with well-defined functionality and external interfaces. A VNF can be composed of multiple components running on the same or on different VM(s) or container(s) [23]. One or multiple VNFs are managed by an Element Management System (EMS) [63] and can be deployed on the same or on different NFVI-PoPs [66]. The chaining of network functions presents a NS which yields an offering of a service provider.
- *NFV Management and Orchestration (MANO):* The NFV MANO aims at enabling the automated management of the NFVI resources, and VNFs and NSs life cycle [23,65]. It is composed of multiple functional blocks that can be summarized as follows:
  - *Virtualised Infrastructure Manager (VIM):* The VIM orchestrates the allocation, upgrade, release and management of the NFVI resources, usually within one operator's infrastructure domain. It assists in the management of VNF-FG by creating and maintaining virtual links, virtual networks and ports [65]. It is also responsible of collecting performance and resource fault information [63]. Multiple VIMs can be deployed under the same NFV MANO framework [63].
  - *VNF Manager (VNFM):* The VNFM is responsible for the life cycle management of VNFs. This includes the instantiation, scaling, update and termination of VNFs [65]. These decisions are done based on the virtualized resource performance measurements and fault information collected from the VIM [67]. VNFM interacts with the EMS to perform some management operations such as configuration, performance and accounting [67]. One or more VNFMs can be used to manage VNF instances in an administrative domain.
  - *NFV Orchestrator (NFVO):* The NFVO is responsible for the NFVI resource orchestration across multiple VIMs. It also handles the life cycle management of NSs including their topology update, scaling, termination and performance measurements collection. The topology of a network service is represented by a virtual network function Forwarding Graph (VNF-FG) expressing the chaining of VNFs and the virtual links connecting them [63]. Further, the NFVO coordinates with the VNFMs in order to manage the VNFs [65].
- *Operation Support System/ Business Support System (OSS/BSS):* OSS/BSS is expected to capture operators' specific functions that may provide management and orchestration of legacy systems and services. It is expected to exchange information with the NFVO.

In the following, we refer to the full deployment of the NFV architecture as an "NFV stack".

3.3. NFV catalogs

In addition to the VIMs, VNFMs and NFVO, the NFV MANO framework incorporates a list of catalogs dedicated to keep track of the deployed VNFs, NSs and their allocated resources. These catalogs can be summarized as follows:

- *NS catalog:* It contains deployed NSs information. This catalog supports the creation and management of NS Descriptor (NSD), Virtual Link Descriptor (VLD) and VNF-FG Descriptor (VNF-FGD) [65,68].
- *VNF catalog:* It contains information related to VNF packages that include VNF Descriptors (VNFDs), software images, manifest files, etc. Note that the VNFD contains all the necessary information for the instantiation and management of a VNF including the resource requirements [65,68].
- *NFV instances repository:* It holds records for each VNF and NS instance that are updated during the life cycle management of the VNF and NS respectively [65,68].
- *NFVI resources repository:* It holds information on the available, reserved, allocated NFVI resources across operator's infrastructure domains [65,68].

3.4. NFV reference points

The NFV architecture functional blocks are interconnected via different reference points. The latter identify the peer to peer relationship between the NFV components, while the interfaces defined on top of them specify how functional blocks' capabilities are exposed to each other and how the flow of information is exchanged in order to enable collaboration. Fig. 4 illustrates the nature of the information exchanged with/within NFV MANO services through the main reference points and their interfaces [65]. Based on the interacting functional blocks, we categorize reference points as follows:

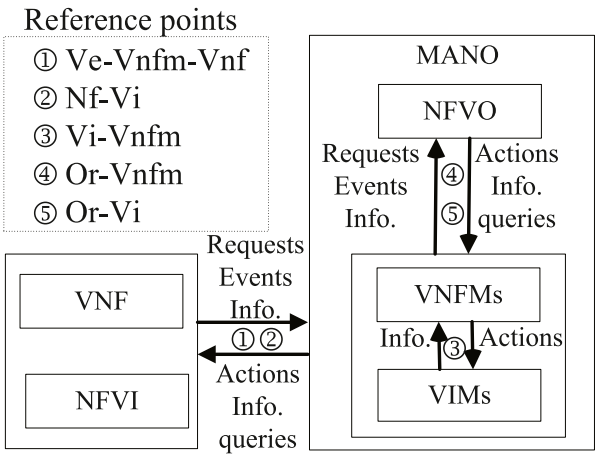


Fig. 4. Interaction between NFV functional blocks through the main ETSI NFV reference points.

- *Management-to-Operational components reference points (Nf-Vi and Ve-Vnfm-Vnf)*: Through *Nf-Vi* and *Ve-Vnfm-Vnf* reference points, the VIM and VNFM use their interfaces to enforce the actions received from the NFVO and query performance measurements information. Specifically, the VNFM forwards configuration actions to the VNF layer such as instance scaling out/in or up/down, instance configuration update, liveliness verification and performance measurements. VNFs use their management interfaces to report VNF status and fault information to the VNFM. Note that similar information is exchanged within the *Em-Vnfm-Vnf* reference point defining the interaction between the VNFM and the EMS. The VIM uses its interface on *Nf-Vi* to allocate virtualized components (VMs/containers) with the indicated amount of resources, update the resource allocation, migrate or terminate virtualized components, create, configure and remove virtual connections between virtual resources. On the other hand, the NFVI uses its interface to forward the configuration information, failure events, performance measurements and resource usage records to the VIM.
- *VIM to VNFM management blocks (Vi-Vnfm):* The VIM uses its interface on *Vi-Vnfm* reference point to forward the information the VNFM has subscribed to such as the resource usage records with respect to the NFVI resources, specific events (resource reservation, allocation and release). It also sends information on virtual infrastructure faults and failures. The VNFM uses its interfaces to submit resource allocation and release actions to the VIM.
- *NFVO to VIM/VNFM management blocks (Or-Vi and Or-Vnfm):* The NFVO issues decisions regarding VNF instantiation, scaling and termination to the VNFM, while the latter issues resource allocation requests and asks for life cycle operations grant (e.g., scale up/out). The VNFM also forwards information about the VNFs which might have an impact on the NSs operation. Using the *Or-Vi*, the NFVO issues resource availability check requests. It instructs the VIM to perform resource reservation, allocation and release. The NFVO further requests the interconnection setup between those resource. The VIM forwards the configuration information, failure events, performance measurements and resources usage records to the NFVO.

3.5. SDN integration within NFV architecture

As defined in [69], SDN is *"a set of techniques that enables to directly program, orchestrate, control and manage network resources"*. In other words, SDN simplifies network management by offering flexible routing through separating the network control logic from the underlying data plane. Within the NFV context, SDN programmability facilitates the interoperability of multi-vendor network resources and leverages the NFV automated management. The integration of the SDN components (i.e., resources, controllers and applications) within the NFV architectural framework is envisioned in different forms [70]:

- Depending on their nature, the SDN resources (e.g., routers and switches) may appear at the NFVI layer as part of the network hardware, as software-based switches running on top of computing hardware, or as virtual switches. They can also appear at the service layer as VNFs [70].
- Classically, the SDN controller is implemented within the NFVI to ensure network connectivity. The latter's functionality can also be implemented as part of the OSS/BSS or as part the VIM. It can also be virtualized and deployed itself as a VNF running on top of the NFVI [70].
- Depending on their functionality, SDN applications might be part of the OSS/BSS logic, they can be defined as EMs or VNFs, they can be part of the VIM and connect to the SDN controller standing in the NFVI, or they can be physical appliances [70].

Overall, SDN solutions can be deployed either at the infrastructure domain, at the tenant domain (e.g., network operator) or both. The details related to possible deployments of SDN within NFV are beyond the scope of this paper.

3.6. Combining NFV and MEC

MEC is another key component of 5G. It provides compute, network and caching resources geographically distributed at the edge of the mobile network (e.g., 5G network) to allow the deployment of various end user applications and RAN/core VNFs close to the end users. This ensures the required QoS and QoE for a plethora of heterogeneous services (e.g., augmented/virtual reality, autonomous vehicles) [16,71]. Both MEC and NFV rely on virtualized platforms to run either Mobile Edge (ME) applications (i.e., end user applications) or VNFs. Thus, in order to maximize the return on investment of their virtualized infrastructure, it is of the best interest of network operators to deploy over it both VNFs and MEC applications [72].

3.7. NFV in 5G networks

In the presented ETSI NFV architecture (Fig. 3), we observe a clear separation of the physical infrastructure from the service layer. In addition, we notice the appearance of a management and orchestration layer that promotes the automation and flexibility of network management, which is at the heart of 5G networks requirements. Furthermore, the integration of NFV with SDN and MEC allows for more flexibility, cost effectiveness and opens up opportunities for the support of a very large variety of services. Thus, considering this architecture and the emerging 5G ecosystem, we derive in the following a comparison between traditional and 5G telecommunication business model.

4. Telecommunication business models

The technological transformation of telecommunication networks entails an ever evolving telecommunication market. The move from legacy, one-size-fits all network architecture towards softwarized and virtualized networks, designed upon the request of a business vertical drives a drastic change in the telecommunication business model. This change is promoted by advancements in NFV, SDN, cloud and edge computing. These technologies allowed the progress of the traditional business model built around infrastructure and product ownership towards a service-oriented one that leverages delegation of responsibilities between different business players. This major transition promotes business agility on one hand and on the other hand introduces new security risks [73]. Thus, it yields interesting exploring the new telecommunication 5G business model in order to dissect the impact of

new technologies on business relationships, identify the security risks it introduces and hence, guide network operators towards highly efficient business decisions to respond to the rapid growth of telecommunication demands [74].

In the following, we highlight the impact of the information technology evolution on the telecommunication business model throughout a literature review of the proposed business models. Then, we identify the traditional telecommunication business model actors and their different interactions. Further, we study, analyze and derive a new telecommunication business model promoted by the 5G ecosystem and the NFV architecture [63].

4.1. Business model evolution

The traditional monopolized telecommunication business architecture evolved around multiple operators and network equipment providers to supply basic telecommunication services that include messaging, calls and data. Al-Debei et al. [74] discuss and analyze the evolution of the telecommunication business model since the first Generation (1G) to the fourth Generation (4G) networks. The rise of virtualization and softwarization trends had a first impact on data centers which were transformed into a pool of shared resources with the cloud computing concept gaining interest in the information technology market [23,75]. Cloud computing revolutionized existing business interactions by decoupling the infrastructure from the services to leverage a service-driven business model that is presented by Zhang et al. [75]. In such a model, hardware and platform resources are provided in an on-demand basis by infrastructure providers [75]. Cisco [73] highlights the distribution of tasks and ownership to the specialized providers in the cloud computing business model to optimize the outcomes to the customers. Cloud computing transformed the business trend from infrastructure and products offering to service offering [73]. This transformation introduced new business interactions and partnerships [76] that exploited the telecommunication business towards inaugurating new services leveraging automation and simplified management to other sectors such as health, manufacturing, among others.

Being a technology enabled by virtualization and softwarization, NFV affected the telecommunication business model. In fact, Mijumbi et al. [23] identify the main business players in an NFV environment and present a reference business model based on the cloud computing one. They recognize telecommunication service providers as one of the NFV business model players which lease resources from infrastructure providers in order to run their VNFs, provided by VNF suppliers. They also consider brokers to simplify the interactions between telecommunication service providers and VNF and server providers. Their proposed business model remains limited to NFV and overlooks the business interactions in a 5G ecosystem. In [77], the authors present a list of players in the NFV ecosystem by accounting for the ETSI NFV architecture [63]. ETSI [78] defines several key roles in the NFV ecosystem including NFV cloud service customers, NFVI and MANO cloud service providers, VNF suppliers and Integrators and discusses their responsibilities.

The rise of 5G networks driven by softwarization and virtualization introduces new business players. Ordonez et al. [79] discuss the network slicing concept in 5G networks based on NFV and SDN and identified three key players in a virtualized network, mainly, infrastructure providers, tenant and end user. They present these players in a 5G network based on network slicing. 5G Infrastructure Public Private Partnership (5G PPP) discussed 5G stakeholders in [80].

The aforementioned contributions are limited to identifying business players that arise with a specific concept or technology. We notice that they either propose a cloud computing or NFV business model. The efforts related to 5G are limited to specifying business players as a result of the network slicing concept. Hence, we find that the literature lacks a comprehensive business study that dictates the evolution of the telecommunication business before and after the rise of virtualization and softwarization. Further, we notice that none of the existing works studies the impact of this business transformation on network security in this era of open, flexible and automated network management and orchestration. Hence, in the following, we address the shortcoming of the literature by presenting the traditional telecommunication business model and comparing it against a 5G telecommunication business model that we derive.

4.2. Traditional telecommunication business model

Traditionally, a few operators and network equipment suppliers were part of the telecommunication business model. The traditional business model depicted in Fig. 5(a) can be defined by the following business players:

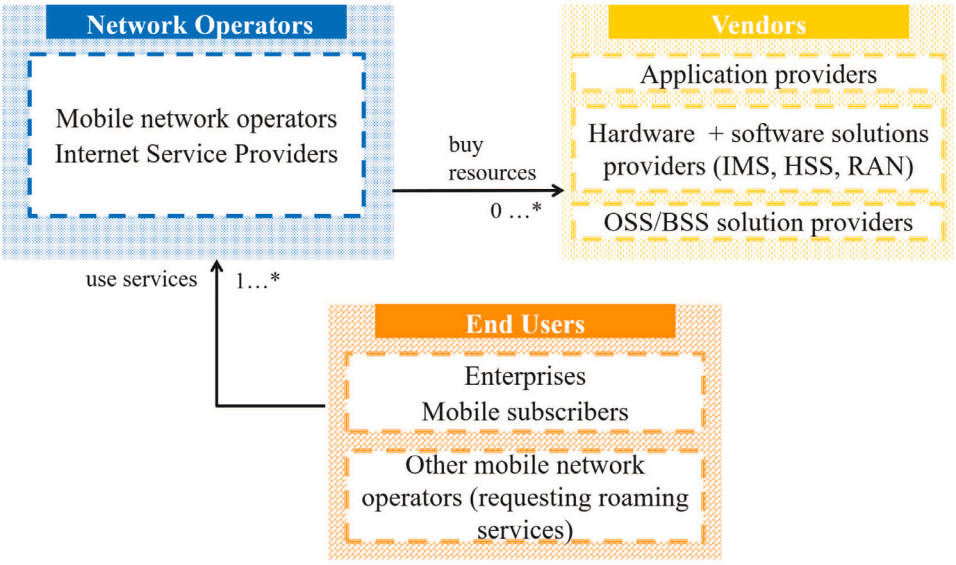
- *Network operators:* In the traditional telecommunication business model, network operators were either Mobile Network Operators (MNOs) or Internet Service Providers (ISPs), which provided cellular and communication services such as calls, messaging and data through a monopolized telecommunication network infrastructure that was built and managed by their own personnel.
- *Network equipment providers:* The network infrastructure built and managed by the network operators relies heavily on different legacy equipment provided by multiple network equipment providers. In fact, those legacy network equipment are hardware appliances that are mounted with software to provide a defined functionality (e.g., Home Subscriber Server (HSS), Radio Access Network (RAN), etc.). The hardware and its software are coupled to form a single entity provided by the same vendor. The network equipment providers also include end user equipment providers who produce mobile phones and user equipment.
- *End users:* Network operators' customers are those interested in the available telecommunication services (e.g., calls, messages, data). They can be classified under different categories. For instance, individual customers, business customers (e.g., small or large enterprises) and other MNOs signing agreements for roaming services [74].

The traditional telecommunication business model encounters different collaborations and business agreements between network operators for extended internet and mobile services such as roaming. These collaborations are limited to providers paying each other for the end-to-end user service and its management. However, business collaborations in 5G are impacted by virtualization. Rather than paying for the service and the whole related management operations, we explain in the following, that business collaborations in 5G involve a delegation of responsibilities and multiple collaborations to devise an end-to-end service for the user. These collaborations entail for example a mobile operator paying for the use of the infrastructure and its management while keeping the end-to-end mobile service deployment and management as part of its responsibility.

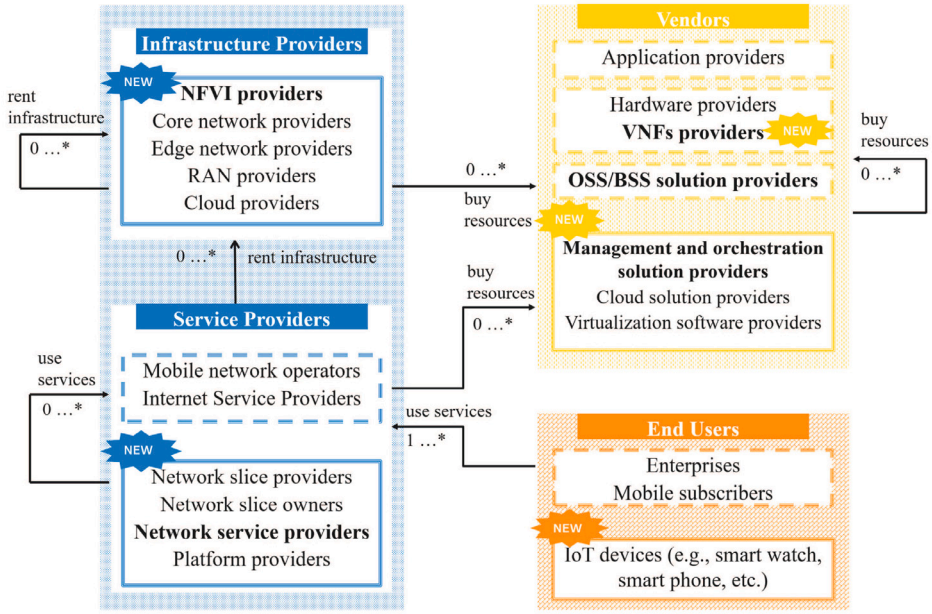
4.3. 5G telecommunication business model

The NFV architecture presented in Section 3.2, which exhibits a clear separation of the network infrastructure from the services, directly impacts the 5G telecommunication business model. Thus, we note that the operators in the traditional business model are split in the new 5G business model into infrastructure providers and service providers. In fact, the 5G telecommunication business model presented in Fig. 5(b) encompasses the following business players:

- *Infrastructure providers:* Infrastructure providers regroup any entity owning and managing a physical network [79]. The latter encompasses any compute (e.g., servers, etc.), storage (e.g., hard drive, etc.) and networking (i.e, routers, switches, physical links, etc.) equipment that can be bought from different vendors. These



(a) Traditional telecommunication business model.



(b) Derived 5G telecommunication business model in which NFV actors are highlighted in bold.

Fig. 5. A comparison between traditional and 5G telecommunication business model.

physical resources can be legacy equipment as well as COTS ones (e.g., standard servers, etc.). RAN, edge network, core network, cloud data center or a combination of two or more of these aforementioned networks are constituted in part of physical equipment. Thus, we consider that infrastructure providers can be RAN, edge, cloud, core providers or a combination of them such as an NFVI provider. Infrastructure providers can lease their network resources to many service providers. Further, upon the need and to respond to their clients, infrastructure providers can collaborate following negotiations and mutual agreements in order to form coalitions to serve their customers [23]. For instance, a cloud provider can collaborate with an edge network provider to serve a Content Delivery Network (CDN) provider.

- *Service providers:* Service providers lease infrastructure resources from one or multiple infrastructure providers to provide one or multiple services [23,79]. In fact, service providers use the leased resources to deploy virtual elements (e.g., VMs, containers, etc.) such as those used in NFV (e.g., VNFs) and SDN (e.g., virtual switch, applications). The interconnection of the virtual elements will form the virtual network of a service provider used to provide one or multiple services. In fact, a service provider decides on the chaining of different VNFs to provide a network service. It is responsible for the deployment and life cycle management of its VNFs and deployed services. Note that the service provider buys its virtual resources (e.g., VMs, containers, VNFs) from different vendors. It can also lease its virtual resources to other service providers [23]. For example, a MNO can lease part of its virtual resources to another MNO representing its child company. In addition, service providers can cooperate to supply an end-to-end network service. In this case, the VNF chain providing the service is decomposed into smaller components that are mapped to virtual resources of multiple service providers collaborating together to enable the network service [81]. Note that a service provider can be a MNO providing telecommunication services or

an ISP. It can also be a network slice owner supplying services for a defined vertical industry (e.g., a manufacturing company owning a network slice to furnish industry 4.0 services, etc.) or a network slice provider which leases network slices to other service providers with specific guarantees on the QoS. The service provider can be a network service provider which supplies a network service composed of a chain of network functions [63], or a platform provider which provides a toolkit of networking and computing resources in addition to VNFs in a form of a platform to the consumer (e.g., an email service provided as a platform with the configuration such as mail domains and user configurations left for the consumer of the platform, etc.) [75,82]. It is worth noting that in some cases, a service provider can be an infrastructure provider as well. For instance, a MNO can be owning and managing its telecommunication network while also providing telecommunication services.

- *End users:* End users are the consumers of the provided services by the service provider [23]. They can be IoT devices such as a smart watch, a smart phone, sensors, among others; which are offloading their tasks to be processed by applications owned by a service provider and deployed at the edge of the network where the edge infrastructure resources are supplied by an infrastructure provider. The end users can also be enterprises using for instance some billing or internet services offered by a service provider. In the simplest case, the end user can be a mobile subscriber. Note that end users can be consumers of multiple services offered by different service providers [23,79].
- *Vendors:* The infrastructure providers and the service providers buy their physical and virtual resources from multiple vendors. Network equipment providers in the traditional telecommunication business model are transformed to vendors where we notice a split of the business actors from hardware and software solutions providers to follow the decoupling of software from the hardware that was introduced with NFV and SDN. Thus, we can observe a split of vendors between software vendors and hardware ones. Hardware providers can be those supplying telecommunication network equipment such as servers, routers, base stations, among others. Software vendors can be VNFs providers or IoT applications vendors. They can also supply management and orchestration solutions for an NFV-based network [77]. OSS and BSS solution providers are examples of software vendors which supply software that help with the billing and renewal services, etc.[77]. Virtualization software providers supply virtual resources, mainly, VMs and containers. Finally, there exists the cloud solution providers which are inherited from the cloud computing business model and that are also part of the software providers.

It is worth noting that the functional layers of the NFV architecture appear as business actors in the new 5G telecommunication business model (Fig. 5(b)). Those actors are highlighted in bold in Fig. 5(b).

4.4. From business to security

The move from the traditional to the new telecommunication 5G business model is enabled by different new concepts and technologies. By comparing Figs. 5(a) and 5(b), one can clearly depict the expansion of information and telecommunication technology business to adopt new business players that act as providers of these new technologies. We notice, for example, the appearance of new NFV actors such as NFVI providers, network service providers, VNF providers, management and orchestration solution providers which reflect the translation of the different parts of the NFV architecture into business players. These business players act as an integral part of bigger categories, mainly infrastructure providers, service providers and vendors that interact together to provide end-to-end services to the end users. This collaboration and interaction between business players reflects the move from the traditional business model built around infrastructure and product ownership towards a service oriented one that leverages delegation of responsibilities between different business players. This major transition promotes on one hand business agility and on the other hand introduces new security risks [73].

In this survey, we aim at exploring and presenting these security risks. Thus, after analyzing the possible collaborations between the business players through the derived 5G telecommunication business model, we study how such collaborations are reflected in the network deployment with respect to the NFV architecture and its suggested approach for management and orchestration of resources. Thus, we present in Section 5 multiple deployment models of the NFV architecture in light of new complex interactions between more divers NFV actors due to the new 5G business model and assess their security implications. Then, we elaborate in Section 6 and Section 7 on our findings related to the NFV architecture, the analysis done on the new 5G telecommunication business model and the discussed deployment models to propose a 3D threat taxonomy. Our proposed 3D threat taxonomy represents a detailed study on the security risks introduced by NFV and inspired by the service oriented business interaction between the divers NFV actors reflected in the derived 5G telecommunication business model.

5. NFV deployments and their security impact

The service-driven telecommunication business model (Section 4.3) supposes new collaborations between the different business players it encompasses. Such collaborations are elaborated by an exchange of resources and/or services. For instance, a service provider can run VNF instances inside an NFVI operated by a different infrastructure provider. Another example would be a service provider offering a network service to another service provider. To make such collaboration possible, ETSI NFV proposed a large number of use cases for the deployment of network services across multiple sites [83] and administrative domains[2] [84]. Thus, in the following, we distinguish between multi-site and multi-administrative domain deployment models [83], exemplify a use case of each, and discuss the implications such deployment models have on the provisioning of the NFV-MANO building blocks. Further, we investigate the resulting security implications introduced by new reference points and interfaces.

5.1. Multi-site deployment

It is anticipated that in the near future, network services will be crossing Wide Area Networks (WAN) as their VNFs and PNFs will be deployed over two or more NFVI-PoPs [83] to support the coverage requirements among others. The connectivity between end points in different NFVI-PoPs is achieved through a specialized VIM, known as WAN Infrastructure Manager (WIM).

For illustration, we consider in Fig. 6 a network service composed of three VNFs deployed over two sites, namely, NFVI-PoP#1 and NFVI-PoP#2, belonging to the same administrative domain. As shown through the labeled arrows in Fig. 6, to establish the multi-site connectivity between the two NFVI PoPs, the NFVO requests the WIM to allocate virtualized resources between NFVI-PoP#1 and NFVI-PoP#2 with a designated bandwidth ①. This request is handled by a new interface on the reference point *Or-Vi* between the NFVO and the WIM. Upon reception, the WIM forwards the request to the network

[2] An administrative domain is a collection of systems and networks operated by a single organization. The latter could correspond to a network operator or a department within a network operator.

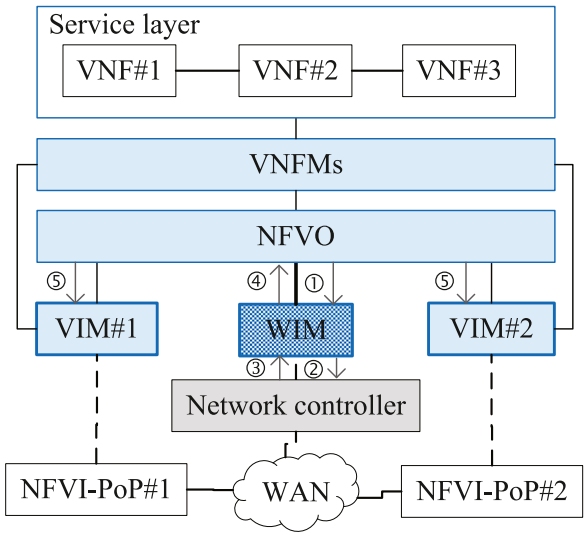


Fig. 6. A multi-site deployment of a network service composed of three VNFs [83]. The labeled gray arrows represent the flow of communications between different components to establish an end-to-end tunnel.

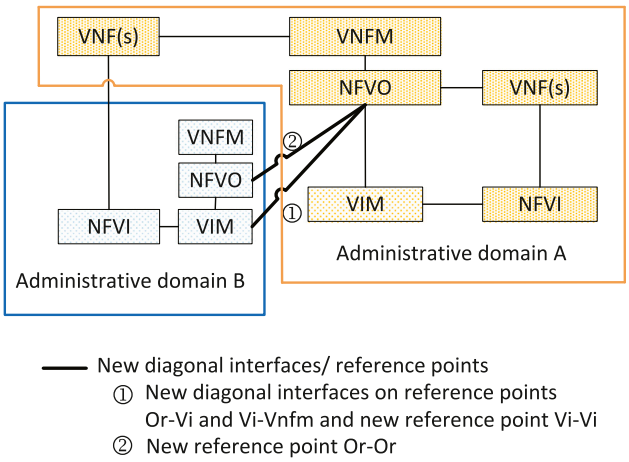


Fig. 7. Administrative domain A (*AD-A*) has VNFs running inside the NFVI of administrative domain B (*AD-B*) [84].

controller[3] to create a network connectivity between the involved sites[4] ②. The network controller creates the needed virtual network resources either using gateways or tunneling protocols [83]. It returns WAN connection information (e.g., IP address, Virtual Extensible Local Area Network (VXLAN) identifier, etc.) as a response to the WIM ③, which in turn returns the response back to the NFVO ④. Afterwards, the NFVO asks the VIMs at site#1 (NFVI-PoP#1) and site#2 (NFVI-PoP#2) to allocate the virtualized resources needed to establish the connection with the WAN for both sites using the provided virtual network resources ⑤. More precisely, VIM#1 and VIM#2 become in charge of creating virtual network connectivity end points to the WAN on their corresponding NFVI PoPs.

A virtual network resource is characterized by various attributes. Examples of such attributes are the virtual network resource type (e.g., Virtual Local Area Network (VLAN), VXLAN, Generic Routing Encapsulation(GRE)), the segment information (e.g., VLAN tag, VXLAN identifier, GRE key, etc.), the bandwidth, the network QoS attributes, etc. Once connectivity is established, the VNFs composing the network service are instantiated and connected to the network connectivity end points using virtual ports.

5.2. Multi-domain deployment

According to the ETSI NFV specification on management and orchestration [65], there will be no single organization maintaining and controlling the whole NFV ecosystem. The collaboration between different business players (i.e., providers) entails an exchange of NFVI resources and services resulting in multiple management and orchestration approaches. This directly reflects on multi-domain deployment options of the NFV stack [84]. ETSI identified multiple deployment strategies to enable efficient management and orchestration of services spanning multiple administrative domains [82]. In our study, we consider the use case where a service provider runs its own VNFs within an NFVI operated by an infrastructure provider. In the following, we will refer to the service provider by tenant as it is leasing the NFVI resources offered by the infrastructure provider. Each of the tenant and the infrastructure provider owns a full NFV stack. For illustration, we briefly discuss the ETSI NFV architecture deployment options for this use case through a concrete example.

Fig. 7 illustrates a tenant's Administrative Domain (AD) *AD-A* and an infrastructure provider's administrative domain *AD-B*. To meet the service coverage and QoS requirements, *AD-A* needs to run some of its VNF instances inside the NFVI of *AD-B*. To achieve this, the NFV MANO blocks from the two administrative domains need to interconnect in order to provide the needed service. This interconnection is achieved either through static configuration of the functional blocks to be interconnected after establishing a business relationship, or through auto-discovery, in which case the functional blocks advertise their own information that need to be used to establish the interconnection with other blocks [84].

Information such as IP addresses, identities and affiliations need to be exchanged between *AD-A* and *AD-B* NFV MANO blocks to establish and maintain live sessions between different parties in order to monitor, detect and fix operational failures.

In the presented example (Fig. 7), *AD-A* uses the NFVI of *AD-B* in addition to its own NFVI. In this situation, the NFVO of *AD-A* is in charge of the network services life cycle management and software images integrity and authenticity verification as well as policies enforcement. Furthermore, the VNFMs of *AD-A* are in charge of the VNFs life cycle management. To express their resource requirements and assure transparency and visibility, the NFVO and the VNFMs of *AD-A* will interact with *AD-B* NFV MANO blocks according to a set of predefined agreements.

In this respect, two main architecture options have been proposed in [84] to ensure information exchange between the NFVI provider (*AD-B*) and the tenant (*AD-A*):

- *Multiple Logical Points of Contact (MLPOC):* In MLPOC deployment model, the tenant has visibility of the provider's VIMs. This architectural option makes use of existing reference points, namely, *Or-Vi* and *Vi-Vnfm*, by introducing new interfaces enabling the interaction between the NFVO and the VNFMs of the tenant and the VIMs of the infrastructure provider.
- *Single Logical Point of Contact (SLPOC):* In SLPOC deployment model, a unified interface is offered to the tenant abstracting the details of internal VIMs of the hosting NFVI. In this case, two architectural options are considered in [84]. Either the SLPOC function is defined at the VIMs, which creates the need for a new reference point between the VIMs (*Vi-Vi*), or the SLPOC function

[3] A network controller is an abstraction layer below the W/VIM responsible for providing programmable network interfaces which enable the establishment of connectivity within a domain [85].

[4] The interface between the network controller and the WIM falls outside the scope of the ETSI NFV reference architecture.

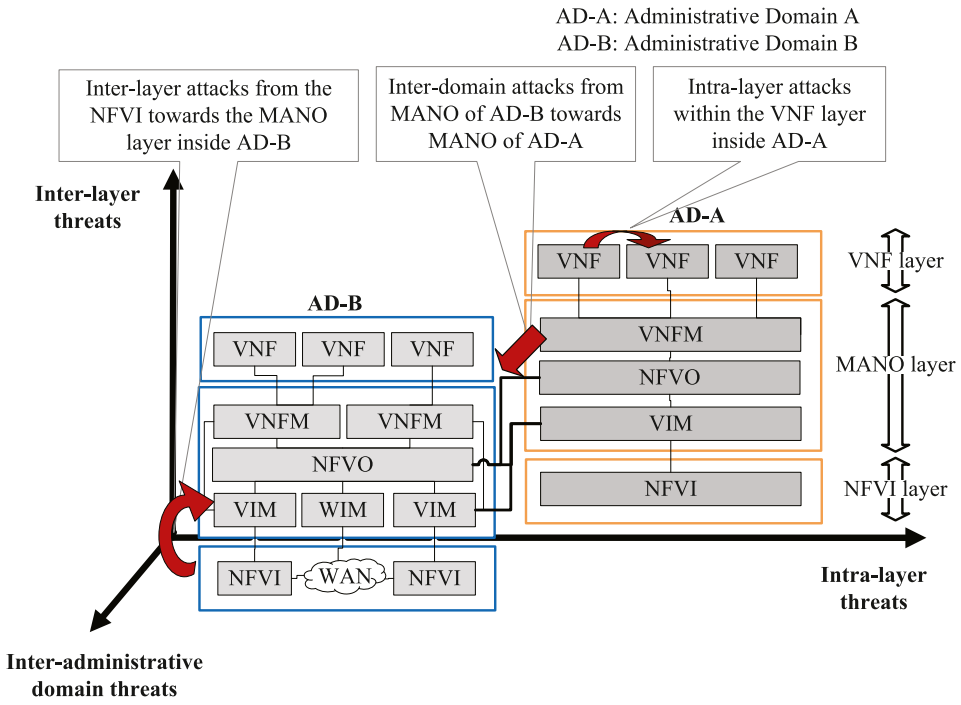


Fig. 8. A three dimensional (3D) NFV threat view spanning the NFV stacks of two administrative domains, AD-A and AD-B.

is defined at the NFVO level, in which case a new reference point is required to define interfaces between the NFVO of the tenant and the NFVO of the provider (*Or-Or*).

More details on the multi-domain deployment architectural options and the supporting reference points and interfaces can be found in [84].

5.3. Security implications

NFV supports the new 5G business model and service requirements by extending the NFV architecture to support the multi-site and multi-domain deployment options. From security point of view, those extensions may be subject to new threats and enlarge the NFV attack surface as they introduce new reference points and configuration operations.

In fact, one can notice that creating network services spanning multiple NFVI-PoPs requires extensive configuration operations to establish network segments crossing the WAN. However, considering the system's complexity and dynamic nature on one side, and the risk of malicious connectivity control through the newly added interfaces on the other side, unintentional or deliberate misconfigurations can be easily introduced, leaving room to network isolation breaches.

Furthermore, the new multi-domain deployment model involving NFV functional blocks owned by different administrative domains creates a need for new reference points and interfaces which will extend the attack surface of the NFV ecosystem. Additionally, the information and entities that need to be exchanged between the tenants and the infrastructure providers such as the VNF software images, etc. result in new threats especially in cases where the trust relationship is not well established between the stakeholders. We expose the security threats related to those deployment models in details in Section 7.

6. NFV threat dimensions and threat vectors

In light of the presented NFV architecture and its deployment model, we present in the following three dimensions along which threats might be manifested inside an NFV, namely, intra-layer, inter-layer and inter-administrative domain threats, then we categorize the NFV threat vectors into four main classes. Those are the virtualization and softwarization, communication links and interfaces, interoperability and service operation, and centralized control and management.

6.1. Threat dimensions analysis

Based on the layered nature of NFV, we introduce the intra-layer and inter-layer threat dimensions. Furthermore, as NFV is used in a multi-tenancy environment where multiple administrative domains can be managed, and different NFV deployment models can take place as explained in Section 5.2, we define a third dimension to capture threats related to such deployment use cases, which we refer to as multi-administrative domain dimension. Fig. 8 illustrates our 3D view of NFV threats. We define the three dimensions as follows.

- *The intra-layer threat dimension* is driven by the NFV layers and it encompasses all the threats instrumenting a unique layer and impacting an asset within the same layer.
- *The inter-layer threat dimension* is concerned with attacks that are initiated at a given layer while their effect is propagated to other layers.
- *The multi-administrative domain threat dimension* encompasses potential attacks which take advantage from NFV deployments spanning multiple administrative domains.

Each of those threat dimensions exploits a set of threat vectors that we detail next.

6.2. Threat vector analysis

By softwarizing and decoupling the network functions from their physical hardware and delegating the management from vendors to centralized entities (i.e., MANO blocks), and by enabling a complex business model, NFV results in an extended attack surface compared to traditional networks relying on proprietary hardware. In the following, we provide a categorization of the main threat vectors [86] resulting from the inherent NFV characteristics (Fig. 9). Concrete examples on how those threat vectors can be exploited to mount attacks are provided in Section 7.

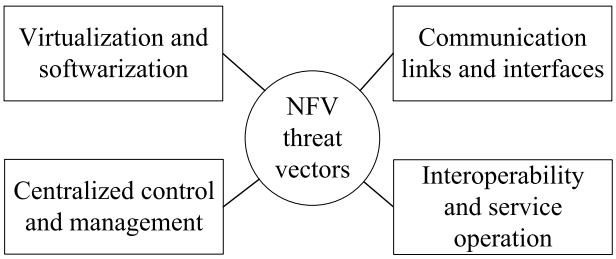


Fig. 9. NFV threat vectors.

- *Virtualization and softwarization:* NFV and SDN together are creating an increased reliance on additional software layers and components (e.g., infrastructure platform management systems, hypervisors, virtual switches, VNFs, etc.) [87]. On one side, this paradigm shift, where software is the fundamental piece, provides a high degree of agility in network service operation, but on the other side, the unavoidable known and zero day vulnerabilities within each software component constitute a potential entry point for attackers to penetrate and compromise the virtualized infrastructure. Those vulnerabilities are mainly related to the software design, implementation and configuration flaws that could exist at the virtualization software (e.g., hypervisors, container runtime, etc.), at the VNF level, including the NFV MANO components, or at the orchestration and management software level. For example, we mention the vulnerability OSSN-0010 [88] found in OpenStack,[5] which enables a tenant of a virtualized infrastructure to acquire privileges and bypass cross-tenant boundary protection. Another example is the vulnerability CVE-2019-1002101 [89] in Kubernetes,[6] which can be exploited to mount a DoS attack on the Kubernetes API server. Implementation flaws in the MANO software might be manifested as misbehavior and wrong control and management decisions (e.g., wrong deployment of services or modifications of existing ones) [90], which may in turn result in misconfiguration situations that can be exploited for instance to perform privilege escalation. For instance, the vulnerability CVE-2019-12127 [91] in Open Network Automation Platform (ONAP) [92] operator manager (OOM) enables an attacker to gain access to the ONAP services without any authentication by accessing a set of specific ports, and the vulnerability CVE-2019-12318 [93] allows attackers to gain access to the service database by tuning a well crafted user input.
  Furthermore, the heterogeneity of proprietary platforms and software in traditional environments constitutes a natural defense mechanism since vulnerabilities are not repeated. Within NFV however, deploying VNFs using common software platforms (e.g., OpenStack, Kubernetes, Hypervisors) eliminates this heterogeneity [94]. Additionally, VMs and containers are instantiated from a limited pool of images, which increases the opportunity of attackers to mount cascaded attacks with a reduced effort.
  The virtualization technology abstracts the physical infrastructure to provide logically isolated pools of virtualized resources, thus enabling the multi-tenancy model and entailing new threats [95]. In fact, once an attacker manages to breach the isolation enforced by the virtualization layer through a vulnerability exploit, the latter can not only gain access to different tenants' assets sharing the same physical resources, but also to the physical platform, which may affect the entire infrastructure. Additionally, the resource sharing situation naturally gives raise to covert and side channels which could be maliciously used to extract sensitive information for example.
- *Communication links and interfaces:* The NFV paradigm has resulted in a set of new control and management communication interfaces and links, defined over the ETSI NFV reference points, to interconnect management components (NFVO–VNFMs-VIMs) and/or connect management-to-operational components (e.g., VIM–NFVI, NFVO–VNF, NFVO–OSS/BSS) as discussed in Section 3.2. Those new communication links and interfaces are attractive entry points to compromise, especially if they are not/poorly secured in deployments. For instance, if an attack exploiting TLS misconfigurations [96,97] is successfully mounted, spoofing and tampering attacks (i.e., man in the middle) on communication links become feasible [12,98].
  Furthermore, APIs define possible interactions between different components. If not well defined, those interfaces may crash or fail under certain circumstances. For example, if the API does not control the validity of input data, malformed or inappropriate input, such as an invalid file format, an exceed in the file size limit or an erroneous SQL expression injection, this may cause NFV functional components to fail, crash or misbehave in the worst cases. For instance, the vulnerability CVE-2019-12127 [91] in ONAP operator manager (OOM) enables an attacker to gain access to ONAP services without any authentication by accessing a set of specific ports.
- *Interoperability and service operation:* Since the VNF is becoming a niche market attracting an increasing number of industry bodies and open source foundations, network service composition and operation may fail under interoperability issues [28,99]. The latter can be manifested as misbehaviors weakening the security of the network services, or may lead to compliance concerns. The NFV MANO blocks are specifically exposed to the interoperability issue. While ETSI clearly defines the role of the VNFM, the VIM and the NFVO and determines the processes of their interaction [63,65], multi-vendor implementations may exhibit huge divergence with respect to specifications [100]. Additionally, deployment use cases where network services span multiple administrative domains can be also a source of interoperability concerns. At the network service operation level, the chaining of VNFs in a VNF-FG can simplify the attack propagation. Further, faulty or malicious chaining policies can be introduced at the NFVO to be instantiated and deployed as a faulty network service.
- *Logically centralized control and management:* NFV is based on the concept of delegating the management and control to a logically centralized entity, which is the NFV MANO and the NFVO more particularly. The latter maintains a global view on the whole network state and service operation conditions (e.g., resource availability, NS requirements in terms of resources, etc.). In addition, it has to instantly intervene in case of failures based on a set of predefined policies to avoid large scale damage. This logically centralized management style implies that the MANO blocks become a single point of failure and a potential availability bottleneck [90,94], which could be exploited by attackers to cause severe service disruption, over or under utilization of network and computational resources, and even a total failure of the whole ecosystem leading to significant losses.

Based on those threat vectors, we pursue deriving our 3D NFV threat taxonomy next.

7. NFV threat taxonomy

Based on the previously identified threat dimensions and threat vectors (Fig. 10), we define our 3D NFV threat taxonomy. For each one of the threat dimensions, we discuss attacks that exist in the literature. We further forecast potential attacks that may exploit the NFV threat

[5] OpenStack is an open source cloud infrastructure management system.
[6] Kubernetes is an open source orchestration platform for running container-based services.

Table 2
Mapping the threat vectors to NFV threat dimensions.

Threat vectors	Intra-layer			Inter-layer					Inter-administrative domain
	NFVI	VNF	MANO	NFVI–VNF	VNF–NFVI	NFVI/VNF-MANO	MANO-NFVI/VNF	Multi-site	
Virtualization and softwarization	[101–104]	[105,106]	[90]	[107,108]	[108,109]	[101,102,108]	[65]	[103,104,107]	
Communication links and interfaces	[110]	[111,112]	[98]	[110]		[111,112]	[98]	[83,98]	[84,98]
Interoperability and service operation		[113]	[12,113]				[114]		[100,114]
Centralized control and management			[90]			[115,116]	[115,116]	[115,116]	[65]

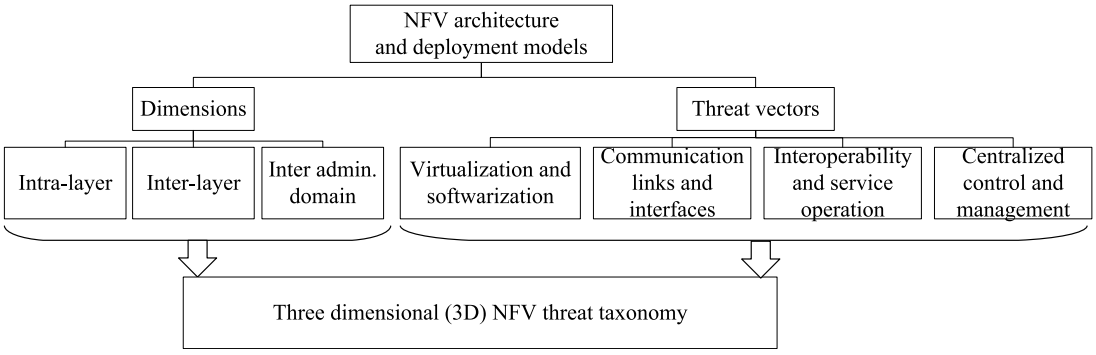


Fig. 10. 3D threat taxonomy elements and organization.

vectors. To the best of our knowledge, this is the first effort exploring potential threats related to the NFV reference points (Section 3.4) as well as the multi-site and multi-administrative domain deployments in the NFV ecosystem. Table 2 summarizes the threat vectors that could be exploited for each NFV threat dimension.

To better structure our taxonomy on potential attacks that could be performed at a given NFV threat dimension, we borrow the STRIDE [117,118] threat classification which categorizes the most common attacks into six types, namely, spoofing, tampering, repudiation, information disclosure, DoS and escalation of privilege. Those attacks respectively affect the authentication, integrity, non repudiation, confidentiality, availability and authorization security properties. As repudiation attacks can happen in any network and may not be NFV specific, we overlook them in our study.

Fig. 11 and Table 3 summarize our 3D taxonomy. Note that the attacks provided in the leaves of the tree taxonomy in the figure are not meant to be exhaustive since the possible attack instances depend on many different factors such as the VNFs and their versions (see Section 7.1.2 for more details), the virtualization software (e.g., Xen [119], VMware [120], Docker [121], etc.), the virtualized infrastructure management platforms (e.g., OpenStack [122], Kubernetes [123], etc.). Furthermore, Table 3 provides references for existing attacks that are already discussed in the literature.

7.1. Intra-layer threats

We discuss the intra-layer threats per NFV layer, namely, NFVI, VNF and MANO as follows.

7.1.1. NFVI threat analysis

Security threats at this level are mainly related to the virtualization and communication link threat vectors. There exist two main virtualization technologies, namely, host virtualization and OS virtualization. In the host virtualization technology, hypervisors enable several VMs to share the same physical host while ensuring the logical isolation. OS virtualization or containerization is a recent technology where the OS kernel is virtualized to be shared among multiple and distinct user space instances known as *containers* [147].

Although the containerization approach provides a certain degree of isolation, it remains less secure than hypervisor-based virtualization, which provides applications with their own operating system [148]. However, different attacks aiming at breaching the logical isolation have been proven effective in both virtualization technologies.

- *Escalation of privilege:* Several attacks can take advantage from hypervisors' vulnerabilities (e.g., CVE-2015-345 [101]). An example of such attacks is hyperjacking or VM escape [107,108], which is a privilege escalation attack, where the malicious VM exploits the hypervisor's vulnerabilities to gain root privilege and then take control over the host and subsequently over all the co-residing VMs [124]. Other attacks taking advantage from network dependencies (i.e., communication links between VMs) could be further mounted to breach the isolation of private virtual networks [110]. Container vulnerabilities are other entry points. For example, a container configured to enable applications running in privilege mode would open opportunities to gain access to the host OS and to other containers running on the same host. Container escape attacks allow the container to escape the container runtime and target the host OS. An example of Docker vulnerabilities enabling container escape is CVE-2016-5195 [102]. More recently, the vulnerability CVE-2019-5736 [149] has been discovered on the `runC` command-line tool, a lightweight universal container runtime which allows spawning and running containers. The latter vulnerability enables a process running as a root inside a container to gain access over the hosting physical machine.
- *Tampering:* A subverted hypervisor can be used to launch a rollback attack [126], which causes recently issued security policies and patches to be bypassed on victim VMs. It can also tamper with the victim VMs' allocated memory which would cause changes in their behavior, or in the worst case, it can stop the victim

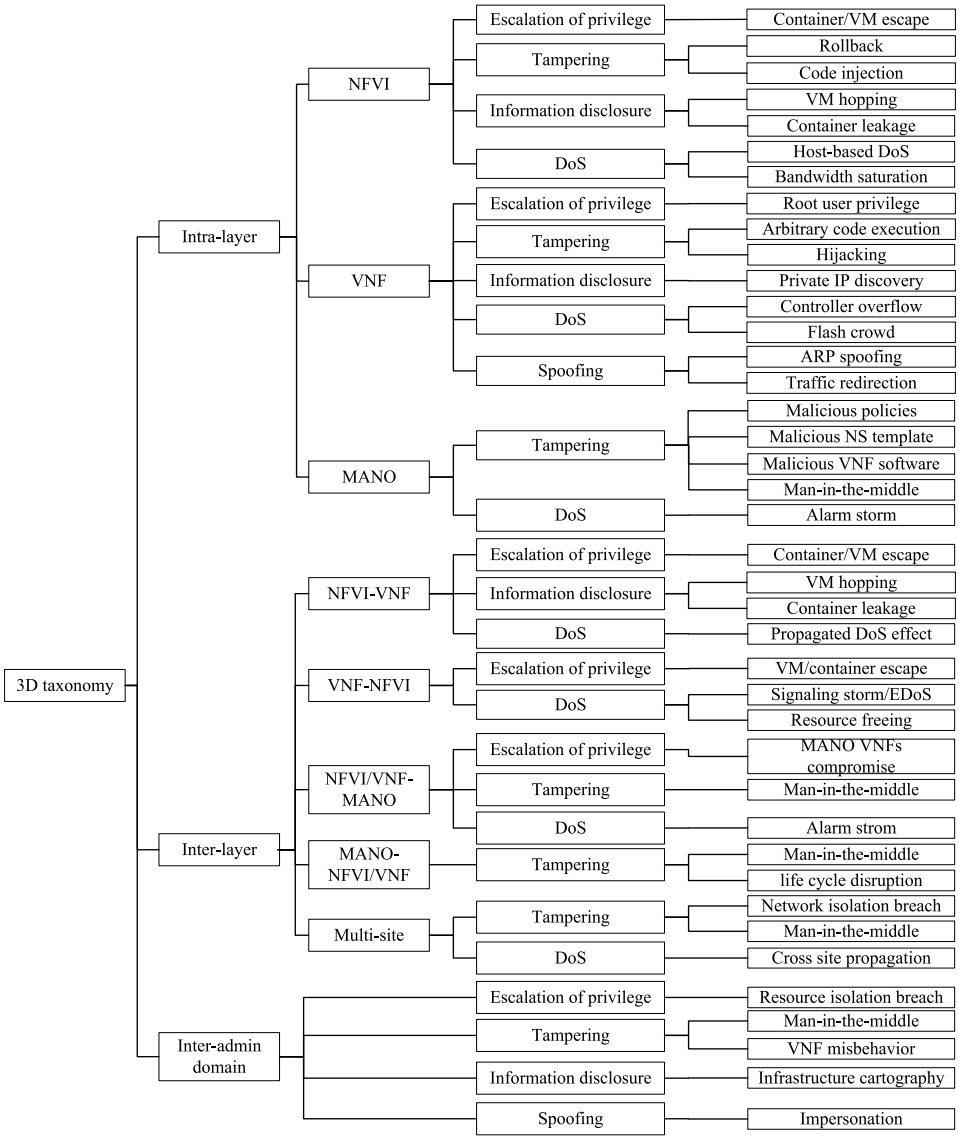


Fig. 11. A 3D NFV threat taxonomy. Threats in the leaves are excerpts of possible attacks that could be performed depending on the existing threat vectors and vulnerabilities.

Table 3
3D NFV threat taxonomy. The symbol *A* means that the category of attacks is likely to happen at the corresponding level of the threat dimension but no references supporting the fact are found in the literature.

Attack categories	Intra-layer			Inter-layer					Inter-administrative domain
	NFVI	VNF	MANO	NFVI–VNF	VNF–NFVI	NFVI/VNF-MANO	MANO-NFVI/VNF	Multi-site	
Escalation of privilege	[107,124]	[125]	A	[107,108]	[108,109]	A	A		A
Tampering	[126–128]	[105,129]	[98]	A	A	[65]	[65,98]	A	[84]
Information disclosure	[130–135]	[136–139]	A	[132]	A	A	A	A	[84]
DoS	[103,104]	[106,140], [141]	[90]	[103,142]	[143,144], [28,104,145]	[90,115,116]	A	A	[114]
Spoofing	A	[111,112, 146]	[98]	A	A	A	A	A	A

VMs which leads to a DoS. Spectre attack [127] is a tampering attack which tricks applications into accessing/altering arbitrary locations in their memory. Process hollowing [128] or code injection attack is another tampering attack which could be launched through containers' processes. In this attack, a legitimate process is launched in a suspended state, then its memory is injected with a malicious code at runtime. A comprehensive analysis of container security can be found in [150].

- *Information disclosure:* In VM hopping attacks, a malicious VM uses side and/or covert channels to recover secret information such as cryptographic keys or to establish illicit communication channels with respect to victim VMs. Examples of VM hopping attacks

are last-level cache attack [130], layer two cache attack [131], timing attack [151] which exploit the caching system of CPUs to leak secret keys, and hammer attack [132], where malicious programs may issue well crafted memory access patterns, such as repeated and rapid activation of the same dynamic random access memory rows, to cause disturbances in neighboring rows. Furthermore, in container-based deployments, the host OS vulnerabilities (e.g., CVE-2017-5123, the Linux kernel vulnerability in the `waitid()` system call [88]) can be exploited by malicious containers or applications to leak sensitive information [134,135,152]. For example, in the MeltDown attack [133], a container leaks information from the host OS and all other containers running on the same system.

- *DoS:* One kind of DoS attacks that can be performed in a virtualized environment is the host-based DoS attack [103,104,153]. The latter consists of placing a well tuned malicious VM within target hosts to drain the shared CPU, memory and bandwidth resource usage, which results in a resource starvation situation of the VMs sharing the same hosts. Bandwidth saturation attack [142] is another DoS attack which exploits the bandwidth over-subscription. This attack may cause edge or aggregate routers/switches to become a bottleneck. In fact, if the attacker manages to build a cartography of the targeted cloud data center, then (s)he can place a set of VMs inside the same rack and synchronize those VMs to simultaneously send packets at maximum rate, this would cause a saturation of the upper link bandwidth at the edge switch leading to packet loss and finally service degradation or unavailability.

7.1.2. VNF and service threat analysis

Three categories of threat vectors can be exploited at the VNF level, virtualization and softwarization, communication link and interfaces, interoperability and service operation (Table 2).

Given the fact that NFV revolves around the use of VNFs for developing and deploying both service operation, control and management functions, VNF software is becoming a large threat vector [154,155] due to the abundance of known and zero day vulnerabilities that may be exploited. Following are few examples of VNF software vulnerabilities and the corresponding attacks. For more comprehensive sets of known/exploitable vulnerabilities and their risks, we refer the reader to the common vulnerabilities and exposures database (CVE) [155] and the national vulnerability database (NVD) [154].

- *Escalation of privilege:* The vulnerability CVE-2017-6710 [125] in the Cisco VNF element manager could allow a remotely authenticated attacker to run commands as a root user on the hosting machine, which enables arbitrary commands to run in the context of root users due to the configuration settings.
- *Tampering:* CVE-2016-1417 [105] is a vulnerability found in Snort [156], a known intrusion detection system, which allows remote attackers to conduct tampering attacks such as arbitrary code execution and spoofing attacks like DLL hijacking using remote file share, which in turn may cause information disclosure. The vulnerability CVE-2018-7218 [129] found in Citrix NetScaler Application Delivery Controller allows remote attackers to execute arbitrary code.
- *Information disclosure:* Many information disclosure vulnerabilities have been found in different network appliances. For example, the vulnerability CVE-2018-13365 [136] discovered in Fortinet operating system [138] versions 6.0.1, 5.6.5 and below, allows attackers to discover the host name and the private IP of FortiGate firewall. CVE-2019-18679 [137] is another vulnerability found in Squid proxy [139] causing information disclosure.
- *DoS:* Several vulnerabilities can be exploited to cause unavailability of the service layer. For instance, the vulnerability CVE-2019-15225 [141] found in Envoy proxy [157] may cause excessive memory consumption when the remote attacker sends requests with very long URIs. If exploited, the vulnerability CVE-2019-3635 [140] on McAfee web gateway prevents legitimate users from accessing inline frames. Exploiting the Apache HTTP server vulnerability CVE-2019-10097 [158] causes a stack buffer overflow. According to [70], the SDN controller can be implemented as a VNF sitting at the service layer. Many vulnerabilities have been discovered on OpenDayLight SDN controller [159]. As an example, the vulnerability CVE-2017-1000411 [106] can be exploited to mount the controller overflow attack, which enables to massively exhaust the SDN controller's resources causing a DoS. Some VNFs, such as virtual Domain Name Systems (DNS), may have publicly exposed Application Programming Interfaces (APIs) to interact with end users. Those interfaces could be exploited either to cause the VNF to crash upon receiving bogus packets, or to cause a flash crowd attack by sending an excessive number of service requests simultaneously.
- *Spoofing:* Zingbox [160] is an IoT inspection and life cycle management functionality. The vulnerability CVE-2019-15022 [146] renders Zingbox inspector to be susceptible to ARP spoofing attacks. The vulnerability CVE-2019-18677 [112] found on Squid 3.x and 4.x web proxy causes inappropriate traffic redirection to false destinations. This is mainly due to the fact that user requests are not verified to be well-formed [111].

In a different context, VNFs are meant to coordinate within a VNF-FG towards delivering a network service. This coordination raises two kinds of threats. First, VNFs may be originating from different vendors and therefore may result in interoperability concerns causing either VNF misbehavior or failure [113]. For instance, assume two SDN controller VNFs, SDN-ctl1 and SDN-ctl2 are running two different OpenFlow versions (OF-v1 and OF-v2 respectively) which do not support backward compatibility. If SDN-ctl1 running OF-v1 sends a signaling packet to SDN-ctl2 with a packet header value which is not supported by OF-v2, this may cause the OpenFlow agent running on top of SDN-ctl2 to crash, which may lead to packet loss and temporary unavailability of the network controlled by SDN-ctl2. Second, the network dependencies within a VNF-FG ease the attacks propagation. Using network dependencies, i.e., the legitimate routes established between different VNF components to enable communication, a rogue VNF can be used to compromise all network services it is part of. In a similar note, if a VNF is under a DoS attack, there is a high probability that the VNFs within the VNF-FGs it belongs to will be affected, which amplifies the losses in terms of resource consumption due to the effect of service sustainability (i.e., scale out/up operations to handle the increased workloads) [114].

7.1.3. MANO threat analysis

MANO is considered as the brain of the NFV ecosystem, therefore, clearly defining all possible threats at this level constitutes a primordial step towards proposing techniques and approaches to secure it. As depicted in the MANO column of Table 2, all the threat vectors can be exploited at this level.

To take advantage from the inherent system's elasticity and to avoid the single point of failure, the NFV MANO functional blocks could themselves be virtualized [65,90,161]. Such a design choice provides the required reliability to sustain MANO services, however, it exposes the MANO blocks to the virtualization threat vector. Indeed, all the threats discussed at the VNF layer will remain valid for the MANO components, except that the impact of such threats may take enormous proportions since MANO is the NFV component where management information is maintained and where decisions are centrally taken. Although we did not find many references in the literature on attacks at the MANO layer due to the juvenility of the field, we believe all the considered categories of attacks are likely to happen. In the following, we forecast and discuss instances of potential threats that are specific to the inherent characteristics of the NFV MANO layer and to its capabilities.

- *Tampering:* Assume an internal attacker managed to have access to the NFVO functional block [161]. In this case, the attacker can tamper with the competitor network operators' policies within the NFVO databases, or increase the quota of resources for his own VNFs while reducing it for other tenants' VNFs. The attacker can also inject malicious network service templates and non verified VNF software images, which would be further exploited at the runtime stage. The attacker can also tamper with the life cycle management of network services and VNFs. For instance, he can stop a virtual firewall which exposes the network service to illicit traffic. Furthermore, communication links within the MANO functional blocks are subject to tampering through man in the middle attacks [98]. An attacker can eavesdrop the communications within the reference points between the NFVO and the VIMs (*Or-Vi*), the NFVO and the VNFMs (*Or-Vnfm*), or between the VIM and the VNFM (*Vi-Vnfm*) to tamper with the exchanged information flows (Fig. 4) in order to inject malicious management activities. For instance, the attacker can intercept the communications at *Or-Vi* to tamper with the performance records or VNF components resource usage sent by the VIM to the NFVO. As a consequence, the NFVO will build a wrong view on the global network state (e.g., the amount of resources allocated to VNF instances, NFVI available resources, QoS, etc.) and hence prevent it from taking the right decisions such as granting permission for a legitimate resource increase VNF request. As another example, the attacker may tamper with the information about the location of a sensitive VNF, which would cause non-compliance with the affinity/anti-affinity policies or with the geo-location regulatory requirements of the network operator. Potential software vulnerabilities in MANO blocks can also be exploited by attackers to gain access to the available services and databases. For instance, the vulnerabilities CVE-2019-12115 and CVE-2019-12119 enable unauthenticated attackers already having access to a pod-to-pod communication to execute arbitrary code on specific pods.
- *DoS:* The NFVO block is a logically centralized control point with respect to the multiple VNFM/VIMs it has under its control, which makes it vulnerable to management level volumetric attacks. For instance, in the alarm storm [90], compromised VIMs (respectively VNFMs) can keep sending updates at high rates on resource availability performance metrics (respectively resource requests) causing a bottleneck at the NFVO, which may not be able then to respond promptly to the received requests. The cascaded effect of such attacks taking advantage of the logically centralized control and management is further detailed in Section 7.2.

In addition, since MANO blocks can be supplied by different vendors, interoperability issues may arise as vendors' implementations may deviate from the ETSI specifications [90]. This would raise challenges in enforcing network level security policies and ensuring secure collaboration between the interacting MANO components [12], which can be manifested as disruptions in service life cycle management and orchestration causing severe failures of the whole system [12,162].

7.2. Inter-layer threats

The logically centralized MANO layer provides an automated deployment and management of service requests to support the required flexibility of the underlying network. However, this remote and programmable service life cycle management and virtualized resource control, in addition to the resource sharing fashion and the run-time coordination between the NFV functional blocks enables a new set of cross-layer attacks that we identify in our taxonomy as inter-layer threats. The latter threats could be originating (1) from the NFVI affecting the VNF/service layer, (2) from the VNF/service affecting the NFVI layer, (3) from the NFVI/service cascaded to the MANO layer, (4) from the MANO expanded towards the NFVI/service layers, or (5) across sites when the deployment models spans multiple NFVI-PoPs.

7.2.1. NFVI towards VNF

The NFVI and the VNF/service functional blocks are tightly related in terms of security, since VNFs are running on top of the resources made available by the virtualization layer at the NFVI. It follows that all the intra-layer threats described at the NFVI level, and which exploit the virtualization and softwarization vulnerabilities, have direct impact on the VNF/service layer. Following are examples on how NFVI threats are propagated to the VNF layer.

- *Escalation of privilege:* A malicious VM which managed to perform a privilege escalation to bypass the logical isolation through exploiting a vulnerability at the hypervisor of its hosting machine, can take control over all the VMs running on top of the same host. Once the privilege is escalated, the malicious VM can perform all types of attacks on the VNFs sharing the same host (i.e., tampering, spoofing, repudiation, information disclosure and DoS) [107,108], and probably on VNFs located on other services through exploiting network dependencies [110]. For illustration, assume a virtual firewall (vFW) filtering access to a database server. The vFW is co-residing with a malicious VM, namely, M, as shown in Fig. 12. If the malicious VM, M, could breach the virtualization layer, then it can take control over the vFW. For instance, it can alter the established access control lists to enable illicit ingress traffic to reach the database server, which can be further used for sensitive data ex-filtration. Similar impact could be caused by attacks such as process hollowing and container escape, which may cause legitimate VNFs to deviate from their expected behavior (i.e., tampering).
  Since SDN controllers and applications can themselves be VNFs running on virtualized platforms [70], virtualization bypass threats and VNF vulnerabilities may lead to SDN components compromise. Taking control over the SDN controller through a software vulnerability would enable a malicious tenant to discover and steal, change or alter the network service logic of market competitors sharing the same NFVI [163]. For instance, an attacker can change the routing logic to forward the traffic towards a rogue VNF component, where packet headers can be tampered with before being released to the next VNF in the VNF-FG.
- *Information disclosure:* Side/covert channel attacks would result in secrete cryptographic key leakage, illicit communication links establishment, or functioning disturbance. For instance, in the Hammer attack [132], the malicious tenant can access and potentially alter arbitrary physical memory regions on which he has no legitimate access by repeatedly and rapidly accessing the Dynamic Random Access Memory (DRAM). This would potentially disturb the proper operation of VNFs running on the host under attack.
- *DoS:* Host-based DoS [103] attack is launched by malicious VMs which aim at draining the hosting machine's resources (i.e., CPU, memory, disk I/O and bandwidth) causing the co-residing VMs to starve, which would affect the performance of the VNF components. For example, exploiting the hypervisor's vulnerabilities, a unique malicious VM can increase the CPU cycles usage on a host from the legitimate limit (40%) up to 85%. This would cause the VMs sharing the same host and their running VNFs to suffer from erratic or restricted performance. Similarly, bandwidth saturation attack [142] may cause service unavailability or QoS degradation, which might be particularly problematic to network slices with ultra-low latency requirements.
  To further explore the cascaded effect of a DoS attack starting from the NFVI level and ending at the service level, we consider in Fig. 13 a hypervisor managing two VMs. One VM is hosting a firewall which is a shared VNF between two different services; one service composed of a firewall, an Intrusion Detection System (IDS) and a proxy server, and the other service is formed of a

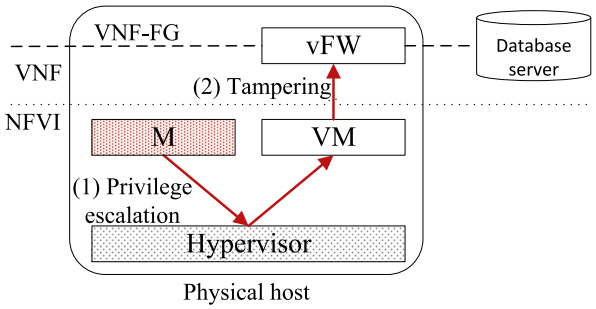


Fig. 12. Inter-layer attack originating from the malicious VM, M, within the NFVI and targeting vFW at the VNF layer.

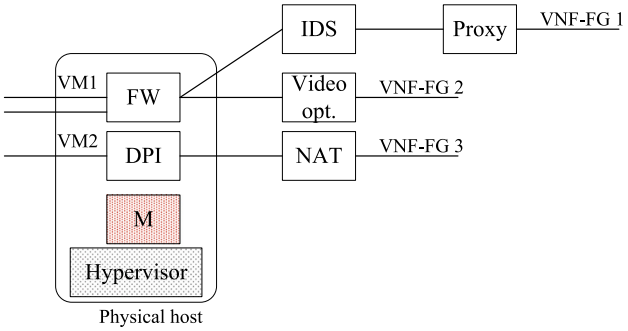


Fig. 13. A malicious VM, namely M, launches a Host-based DoS attack on the hosting machine. The performance of the VNFs running on the co-residing VMs is affected due to resource contention. The effect of the attack is cascaded to the network services of those VNFs.

firewall and a video optimizer function. The second VM managed by the same hypervisor is hosting a Deep Packet Inspector (DPI) as part of a VNF-FG composed of a DPI and a Network Address Translation (NAT). We consider that an attacker exploited one of the hypervisor's vulnerabilities and performed a host-based DoS attack on the hypervisor using a controlled VM named *M* in Fig. 13. Such attack has a direct impact on the VMs managed by the hypervisor. In fact, it will create a resource contention situation leading FW and the DPI running on the VMs hosted by the compromised hypervisor to suffer from starvation, which directly affects the performance of the three services provided by VNF-FG 1, VNF-FG 2 and VNF-FG 3, leading to a service degradation with an extended scope.

7.2.2. VNF towards NFVI

Attacks originating from the VNF/service and propagating to the NFVI layer mainly exploit the virtualization and softwarization threat vector.

- *Escalation of privilege:* A VNF running a malicious application can exploit vulnerabilities in the virtualization layer to gain access to the infrastructure and to other VNFs sharing the same infrastructure. For instance, a compromised/infected application can issue a malicious resource request which is translated by the VM to a malicious hypercall. Once the hypervisor consumes the call, the malicious application gains access to the hypervisor's address space and launches a Return Oriented Programming (RoP) attack [108,109]. This will escalate the privilege of the VM to the highest level, which would enable the VM to gain access to the hosting machine and to manipulate the VNFs sharing the same machine by reading or modifying the memory, copying the VNF to reverse engineer it, or completely stop it. Note that similar attacks can be mounted in container-based applications. We can see here the cascading effect of the attacks. Indeed, a privilege escalation attack is initiated at the VNF layer towards the NFVI layer as a first step, the objective being to mount further attacks on the VNF layer (i.e., spoofing, tampering, information disclosure and DoS on co-residing VNFs).
- *DoS:* In the telecommunication context, application level DDoS attacks could be initiated by end users (e.g., IoT devices) and they target either the control plane or the data plane saturation [145]. Signaling storm [28] is one of those attacks which is initiated by a remote reboot malware infecting a large group of IoT devices. Upon simultaneous reboot operations, each of the infected devices launches an attach request. The large number of service requests launched simultaneously creates a signaling DoS attack on the RAN. If the RAN is running as a VNF within a resource constrained environment (e.g., at the edge cloud), this attack may rapidly exhaust the NFVI resources leading to complete unavailability for legitimated users. The effect of this attack is further propagated to the VNFs that are involved in the attach procedure and which are running at the core network. However, at the core network, where virtualized resources are abundant, these attacks will lead to Economic Denial of Sustainability (EDoS) [143,144] as VNFs are scaled out/up as a response to the "maliciously" increased workloads, which in turn causes massive resource usage to the infrastructure and important financial losses to the operators. In addition, the drastically increased workload may cause resource starvation to neighboring VNFs. It may also trigger a massive number of migration events, which would result into performance degradation at the NFVI as a whole.
  Resource freeing attack and noisy neighbors are attacks which aim at breaching performance isolation among applications running inside the same host. As described in [104], resource freeing attack takes advantage from a vulnerability in Xen resource scheduling modes in order to prevent a victim VNF from using shared resources. For instance, if the malicious VNF manages to increase the network bandwidth usage of the victim VNF in a way to reach a bottleneck, the latter cannot anymore be scheduled to receive other resources such as CPU cycles, which makes more resources available to the malicious VNF.
  For example, assume we have three VNFs, namely, VNF1, VNF2 and VNF3 running on top of the same host and competing on the disk resource. To reduce the resource contention caused by VNF1 and consequently, make more disk resource available, VNF3 maliciously cooperates with VNF2. To do so, VNF3 generates a very large workload of traffic which needs to be handled and forwarded by VNF1 to the next VNF in the chain, which causes VNF1 to reach a bottleneck situation with respect to network bandwidth. Because of a vulnerability in the hypervisor, VNF1 will not be able anymore to receive other resources including the disk usage, which would make more resources available for VNF2.

7.2.3. NFVI/VNF towards MANO

Threats at this level mainly exploit the virtualization and the communication links and interfaces, and the logically centralized control and management threat vectors as described below.

- *Escalation of privilege:* Since MANO blocks might be VNFs [65,90,161] running at the virtualized layer in the NFVI, breaching the virtualization layer through a privilege escalation [101,102,108] would enable attackers to tamper with the MANO VNFs, which would have a large scale damaging effect on the whole network. For instance, if the attacker manages to get access to the VNF descriptors at the NFVO, then he can build an idea about the operational behavior of the VNF as well as its attributes and requirements (e.g., the type of virtualization resources, the hypervisor type the VNF is portable to), which makes it easy to fingerprint and potentially compromise the victim VNF at runtime with a well tuned attack strategy.

- *Tampering:* Although we did not find references in the literature discussing possible tampering threats initiated from the NFVI/VNF layers towards the MANO layer, we believe there exist several tampering threats which can affect the MANO management blocks in different ways. For instance, compromised VNFs and NFVI components can forge fake events to make the MANO execute non-necessary actions or take wrongful management decisions. For instance, a compromised VNF may continue issuing requests for more resources and as a response, the NFVO will continue triggering scale out/up actions. If there exists no policy limiting the amount of resources that should be allocated to the compromised VNF, an over-consumption of the NFVI resources will be caused leading to unnecessary increase of the operational costs of the tenant owning the compromised VNF in addition to the performance degradation with respect to the VNFs hosted at the NFVI under attack. A rogue NFVI may also feed the VIM with fake configuration information which would poison the network view built at the NFVO level. Tampering attacks can also take advantage from the management communication links with the VNFM (*Ve-Vnfm-Vnf*) and modify the information sent to the VNFM (e.g., performance measurement metrics, resources requests, etc.). Similarly, the reference point between the NFVI and the VIM (*Nf-Vi*) may be exploited by a man in the middle attack to tamper with the configuration information sent to the VIM such as the existing connections between VMs, i,e., virtual topology, failure events, performance measurement metrics, and resource usage records to the VIM [65] (Fig. 4).
- *DoS:* Upon the detection of a faulty/abnormal behavior of VNFs or services, a degradation of the performance or complete failure of the latter, a monitoring system usually notifies the NFVO to start a recovery process. However, this centralized fault management feature might be maliciously exploited to cause an alarm storm on the NFVO [90]. If the MANO blocks are not designed to be distributed and scaled at runtime, such threat has a direct impact on the overall network managed by the compromised NFVO. In fact, the time to clear the alarm storm may be so long resulting in a delay in the execution of the NFVO actions, which might be no more valid given the highly dynamic nature of the network. Thus, an alarm storm can translate into a timing failure in the NFVO resulting into inconsistencies in the network. Additionally, the potential NFVO failure resulting from this DoS attack will have a severe effect with network-wide outage situations as significant delays will be instantly cascaded to all the other NFV system components, which creates the risk of lessened robustness and reliability compared to traditional networks [90,115,116].

7.2.4. MANO towards NFVI/VNF

At the MANO layer, all threat vectors can be exploited in many different ways. Indeed, an attacker who manages to tamper with or spoof the NFVO, the VNFM or the VIM, either through a communication interface breach, a virtualization layer breach or a privilege escalation, will be able to abuse all the capabilities available at the compromised/spoofed MANO block. In the following, we forecast and discuss instances of the most prominent tampering threats which could be initiated at the MANO layer and propagated to the NFVI/VNF. Note that, once the MANO blocks are compromised, all other attack categories (e.g., information disclosure, escalation of privilege, etc.) become feasible.

Based on the MANO components' capabilities defined in [65], the NFVO is in charge of onboarding new network services and VNF deployment templates. Therefore, a compromised NFVO may allow non-compliant NSs or VNFs to bypass the integrity, authenticity and consistency validation process. Once instantiated, those NSs and VNFs will lower the security level of the system. For instance, a non validated VNF software image may contain backdoor traps that could be exploited at the operation level to maliciously manipulate the virtualization layer and access other VNFs. The NFVO also controls the network services life cycle management. As such, a compromised NFVO may for instance temporarily suspend a security network service (e.g., a VNF-FG composed of a firewall and a DPI) to prevent malicious network activities from being detected, which would affect the security level of the whole network slice. It can also maliciously modify the topology of the VNF-FG. For instance, introducing a loop in a VNF-FG can be used as a means for amplifying a (D)DoS attack.

Similarly, according to the capabilities attributed to the VNFM [65], a compromised VNFM instance is able to modify the initial configuration requirements mandated in the deployment template at the instantiation phase of the VNF, skip the upgrade/patching operations to keep known vulnerabilities on the VNF, or skip the scale up/out operations to cause VNFs starvation.

A rogue VIM can inject malicious layer 2 and/or layer 3 connectivity components to modify the topology of the VNF-FGs. It can also modify the security group policies to create illicit network reachabilities, which would cause performance and network isolation breaches at the service level. While reporting VNF resource usage records of NFVI resources, a rogue VIM can claim a reduced resource usage for a given victim VNF components, which would cause the NFVO to issue a scale down/in action. As a consequence, the victim VNF's components will suffer from overload because of the depleted amount of resources.

As for the communication links [98], a man in the middle attack at the *Ve-Vnfm-Vnf* may affect the VNF configuration integrity. Upon the communication of a configuration object by the VNFM to the VNF for configuration update, an attacker can intercept the VNF configuration change request and modify the configuration object, hence resulting in a behavior deviation of the compromised VNF [65]. At the *Nf-Vi*, such attack may cause topology inconsistencies with respect to the view maintained at the NFVO level. For instance, the attacker may inject illicit paths between VNFs belonging to different operators, which will be exploited later on to establish unauthorized communications. At *Or-Vnfm* and *Or-Vi*, man in the middle attacks may also cause the VNFM and VIM to forward wrongful actions to be executed at the VNF/server level or at the NFVI level. For instance, the information flowing on the reference point *Or-Vi* (Fig. 4) can be tampered with to scale out a set of VNFs under DDoS attack inside a low resource NFVI, which causes the disruption or the degradation of all the network services having parts of their VNFs running at the victim NFVI.

7.2.5. Multi-sites threats

As discussed in Section 5.1, the multi-site deployment use case creates a new specific VIM, namely, the WIM functional block, as well as a new interface on the reference point *Or-Vi* connecting the NFVO to the WIM. This extends the scope of the virtualization, communication link and interfaces threat vectors. Additionally, the centralized management of multiple NFVI-PoPs may also be exploited to propagate attacks among different points presence.

- *Tampering:* The proper operation of network services spanning different NFVI-PoPs over the WAN largely relies on the correct configuration of virtual tunnel end points and gateways [83]. If a compromised/rogue VIM intentionally changes the mapping of a VNF's virtual port to the wrong end point, then the network service may fail at the operation level and isolation breaches may occur. For instance, if a virtual port is mapped to the VLAN belonging to a different tenant, this may result in an isolation breach leading to information disclosure or to illicit communications to be allowed. A rogue or compromised WIM can mount similar attacks to breach isolation between network services which are supposed to be isolated from each other.

  A man in the middle attack targeting the reference point *Or-Vi* between the WIM and the NFVO may be exploited by an attacker to tamper with the virtual network resources sent to

the NFVO. For instance, the attacker may modify the VXLAN identifier transferred to the NFVO to his own VXLAN identifier for further attacks on the network service.

- *DoS:* An attacker may take advantage from the disparate locations of NFVI-PoPs to mount larger scale DDoS attacks. He can also leverage the centralized management through the NFVO in order to propagate the attack initiated at one location to others. For instance, if the NFVO scales out a VNF, which is already under DDoS attack in one site, into another site then the latter will suffer from the same attack and the economical loss of the attack will be amplified since more resources are available for service sustainability.

7.3. Inter-administrative domain threats

The inter-administrative domain threats involve the communication link and interfaces, the interoperability and centralized management threat vectors. As discussed in 5.2, the multi-administrative domain deployments require the creation of new reference points (e.g., *Or-Or*) and/or interfaces depending on the architecture options. It also requires establishing and maintaining live sessions between the NFV MANO services belonging to different administrative boundaries in order to monitor, detect and fix operational failures. This obviously engenders new threats by creating interactions between organizations among which the trust relationship is not well established, and by extending the contact points between the MANO services from different boundaries. We summarize those potential threats as follows:

- *Escalation of privilege:* Depending on the implemented architectural option [84], the VIM/NFVO of the infrastructure provider should limit the scope of possible operations of the tenant's NFVO/VNFMs to the set of infrastructure resource groups assigned to him (e.g., request the quota, reserve virtual resources). However, a malicious tenant may exploit potential vulnerabilities in the interfaces exposed by the provider to escalate those privileges and then perform harmful management operations on the infrastructure resource groups assigned to other tenants such as virtual resource reservation, release or quota changing.
- *Tampering:* The cross-domain use cases create new reference points and interfaces between the NFV MANO components of different administrative domains [84] (Section 5.2). As a consequence, the communication link and interface threat vector is extended through the MANO services of different NFV trust domains. For instance, a man in the middle attack can be performed at the new reference point *Or-Or* or at the new interfaces defined at the reference point *Vi-Vnfm* for illegal interception (i.e., information disclosure), to tamper with the resource requirements expressed by the tenant or to compromise the integrity of the resource consumption information delivered by the VIMs/NFVO of the provider to the tenant.
  On a different note, in the multi-domain use case a tenant has to distribute the software images of his VNFs to the infrastructure provider. Hence, a malicious provider can tamper with the integrity and the authenticity of those software images, which may cause VNF misbehavior at the operation level [84]. The provider may also make unauthorized usage of the distributed images [84]. A malicious provider's MANO may also provide the tenant's VNFMs and NFVO with wrongful information as for the resource consumption and their mapping to VNF components. For instance, it may claim more resource consumption than what is really consumed, in order to increase the victim's expenses, or forge an excessive number of alarm events to cause a bottleneck at the tenant's NFVO.
- *Information disclosure:* Malicious tenants may exploit the visibility provided to them regarding the provider's NFV MANO service to perform data leakage or infer some information of the hosting infrastructure. For instance, a tenant may use the provided IP addresses and information on the VIMs in order to partly infer the infrastructure topology and possible management strategies (e.g., the VM placement policy in use) [164].
  A tenant's NFVO can distribute malicious VNF software images to the NFVI provider. Once instantiated on the target VIM, those VNFs may be used to breach the virtualization layer and perform malicious activities such as abusing the available resources or ex-filtrating sensitive information about other VNFs belonging to business competitors. They can also be used for unauthorized or hidden use of infrastructure resources or for resource exhaustion through excessive use. Potential attacks at this level are described in Section 7.1.
- *Spoofing:* If no authentication mechanisms are implemented, impersonation attacks can be mounted across different domains, causing illegitimate tenants to run their resources on the provider's NFVI, or legitimate tenants to run their resources on a rogue NFVIs [114].

In addition to those attacks, the multi-domain deployment use cases pave the way for interoperability issues if the applied security and communication protocol stacks are different, which leads to potential security breaches at the network service level.

7.4. Summary and discussion

In this section, we provided a taxonomy synthesizing the NFV threat landscape while accounting for the new deployment options ETSI NFV proposed. From our analysis, we realized that threats related to the virtualization threat vectors are well covered in the literature. Indeed, the literature is abundant with works studying the feasibility, the impact and the possible mitigation approaches for attacks targeting the cloud virtualized infrastructure (e.g., [103,104,124,126,130–132,165]). Software vulnerabilities, related threats and security risks are also well known [154,155]. However, when it comes to virtualizing network functions and centralizing their control and management, although there exist some surveys forecasting potential attacks (e.g., [28,108]), the literature still lacks efforts on prototyping, analyzing and assessing the severity of those threats as a first step towards devising detection, mitigation and prevention solutions. For example, the cross-layer attacks involving multiple NFV components and exploiting the centralized control and management for propagating their effects are discussed in [28,114], however, no implementation or experiments have been conducted to evaluate the feasibility and severity of those attacks with respect to different technologies and deployment options. To the best of our knowledge, our work constitutes the first effort providing a taxonomy which elaborates on the multi-site and multi-administrative domain threats based on use cases provided by ETSI NFV in [83,84]. Although, the deployment options proposed by ETSI NFV are still under study, we believe the security analysis we performed in the inter-layer and multi-administrative domain dimensions of our threat taxonomy constitute valuable findings towards evaluating the risks related to possible deployment models adoption.

8. NFV security projects

In order to secure NFV-based networks, multiple projects have been developed by academia, industry and standardization bodies. This section provides a technical review on most relevant projects and their contributions to the security of NFV.

8.1. ETSI network security manager (NSM)

ETSI complements the NFV architecture with a NSM [166] as a new logical NFV functional block interacting with the existing NFV MANO blocks to enable security as a service. NSM aims at automatically enforcing security policies defined at the design stage throughout the whole life cycle of the network services. To enforce security policies, NSM triggers the instantiation of Virtual Security Functions (VSFs) (e.g. vFWs, virtual security gateways, etc.) through the VNFM according to the defined policies and updates the network topology accordingly.

8.2. SecMANO

The NFV-based Security Management and Orchestration project known as SecMANO [162] represents a conceptual security framework designed to work in parallel with NFV MANO in order to defend against massive attacks that can propagate from the Internet or those introduced by NFV. SecMANO extends the scope of the NFV MANO framework by introducing a security orchestration functionality through an architecture that provides a security by design and a security as a service. The security by design accounts for a security trust model and validates the security characteristics of resources and services. The security as a service module consists of a set of security functions such as intrusion detection and prevention systems, identity and access management, in addition to network isolation and data protection solutions. A dynamic set of these functions is used by a security orchestrator, based on the need, to prevent attacks and ensure the compliance of network services and resources with the user required security characteristics.

8.3. ANASTACIA

The Advanced Networked Agents for Security and Trust Assessment in Cyber–physical system based on IoT Architectures named ANASTACIA is a European project aiming at developing new methodologies and tools to provide security and trust in cyber–physical systems [54,167]. A security management architecture is developed as part of ANASTACIA project [167,168] to provide security and privacy for cyber–physical systems and IoT-enabled critical infrastructures. The security framework combines advancement in NFV and SDN to provide self-healing and self-protection for cyber–physical systems. Its architecture consists of a set of modules that enable proactive policy deployment, automatic monitoring, attack detection using machine learning techniques and reaction mechanisms by inferring possible countermeasures to attacks in order to mitigate them through enforcing new security policies. Security policy enforcement is performed through a coordination between a security orchestrator, the NFV MANO framework along with an SDN and IoT controllers [167].

8.4. SHIELD

SHIELD [169] is a European funded project aiming at developing a novel cyber-security framework to provide security as a Service in a telecommunication environment. The SHIELD security framework leverages SDN and NFV in order to dynamically deploy and manage VSFs destined to monitor, prevent and mitigate attacks. Monitoring VSFs collect data and logs that are aggregated and provided to an information-driven Intrusion Detection and Prevention System platform called Data Analysis and Remediation Engine (DARE). Real-time big data analytic is supported by DARE which analyses the monitoring information to predict and detect attacks that cannot be detected by individual VSFs. DARE provides automatic mitigation approaches through implementing remediation activities by recommending remediation actions or triggering countermeasures. The SHIELD security framework provides a trusted environment through a trust monitor that ensures the authentication and integrity of VSFs.

8.5. Moon

Moon [170] is a security management system developed as part of the OPNFV project. It is considered as a management layer over the NFV/OpenStack infrastructure. It proposes creating security managers assigned to protect VNF instances grouped into tenants. Different protection mechanisms can be supported for each tenant such as authorization, logging of operations and interactions between VNFs, security policies enforcement and storage protection. Moon uses Congress [171] as its policy engine and will be integrating ONFV/Copper [172] as other engines in the future.

The above discussed projects add a layer of security to the NFV architecture either by considering a full security framework collaborating with the NFV MANO or by adding VSFs, or through deploying security managers. These projects reflect the most widely used security approaches to secure the NFV framework. Nonetheless, other projects focusing on 5G security while accounting in part for NFV security were also presented in the literature. For a more exhaustive review of the existing projects, we refer the reader to [54].

9. Lessons learned

NFV provides great benefits to telecommunication service providers and network operators in terms of flexibility, agility and automated management allowing dynamic service deployability and cost effectiveness. Those benefits come with a set of new security challenges and opportunities. The security of NFV-based networks is sensitive to the new service-driven telecommunication business model that lead to new complex interactions between new NFV actors. In addition, the deployment models of the NFV architecture which respond to these new business interactions impact as well the security of NFV-based networks. In the following we summarize the lessons learned from our study related to the diverse aspects of 5G/NFV.

9.1. NFV in 5G networks: A new security perspective

From our study, we learned that the new NFV threat-landscape is governed by threat vectors manifested along our 3D taxonomy dimensions which are: (1) Intra-layer threats targeting NFVI, VNF/service and MANO layers of the NFV architecture; (2) Inter-layer threats exploiting the interaction between the aforementioned layers of the NFV architecture through different reference points and interfaces along with those added in a multi-site deployment; (3) Inter-administrative domain threats caused by the new interfaces and reference points added between multiple MANO components belonging to different administrative domains and business partners.

All the three dimensions are subject to threats and vulnerabilities related to virtualization and softwarization technologies, mainly, the use of virtualized components (virtual machines and containers), in addition to the replacement of hardware network functions by software. While softwarization and virtualization-related threats have been widely studied in the literature, we note that they introduce a new level of security issues in NFV, as they can be used as a stepping stone to stage more harmful attacks. This can be achieved by taking advantage from the service chaining at the operational level in order to propagate towards other layers, sites and administrative domains, causing very large scale damages. Interoperability issues between the components of the NFV MANO services and VNFs from multi-vendor implementations may cause failure to comply with the predefined security requirements causing security breaches, which can be exploited by attackers. Communication links and interfaces defined within and between the components of different layers of the NFV architecture, in addition to those added between different NFV stacks with respect to the multi-site and multi-domain deployments, represent a new threat vector to NFV-based networks. They can be exploited by attackers to

perform man in the middle attacks, eavesdrop or even tamper with the exchanged data.

Above all the aforementioned security threats brought by NFV, the major ones lie in the centralized control and management. The MANO framework constitutes a single point of failure hindering the availability of the whole network. Attacks targeting the MANO framework exploit its role in instantiating, updating, scaling and terminating VNFs and services. Compromising any component of this framework can cause over or under provisioning of resources, DoS and escalation of the attacks to other sites and domains, hence, affecting the virtual networks of other tenants and business partners, resulting in serious financial losses. Security threats at any dimension of the presented 3D taxonomy can take multiple forms such as spoofing, escalation of privilege, tampering, information disclosure and DoS.

9.2. Rethinking security with NFV

Addressing the above security concerns brought by NFV is intrinsic for its successful adoption and deployment in 5G networks. In the following, we propose some main security solutions and directives in order to secure NFV-based networks.

9.2.1. Security by design and security as a service

Security of NFV-based networks should be by design and not an after thought. Security by design consists of defining a security trust model and ensuring confidentiality of all access to the underlying infrastructure resources and services by designing and enforcing security policies along with a zero-trust model [12,162,173]. This allows overcoming the complexity and the threats associated with the configuration of security technologies such as firewalls, IPsec, etc. [12]. Security by design should be followed by a security as a service. Security as a service can be offered by a provider to a tenant through a set of VSFs chained to form a security service offering identity and access management, data protection, etc. Security as a service addresses trust, privacy and security issues emanating from the shared network ownership and management between different business players, each offering a service to the other and controlling part of the network [12,162]. Security by design and security as a service include offering and implementing a fully fledged security solution comprising different security measures and techniques to address the threats and vulnerabilities presented by our 3D threat taxonomy.

9.2.2. From threat vectors to security solutions

Since the virtualization threat vector is a common entry point to a large variety of attacks affecting all the three dimensions, securing the network at the virtualized layer constitutes the most urgent and elementary activity that needs to be brought forward both at the security design level and at the continuous security enforcement stage. For instance, security risks associated with virtualization and softwarization (e.g., hyperjacking, VM escape, VM hopping, DoS, etc.) can be reduced and mitigated through regular software updates and patches. Behavioral analysis can also be applied to detect components deviating from their baseline (i.e., anomaly detection). For example, in [174,175], Machine Learning (ML)-based approaches are proposed to detect the preliminary symptoms of SLA violation and to identify the anomalous VNFs which are at the origin of the SLA violation. Note that, SLAs could also be impacted by having the NFVI provider deploying security agents different from those delivered by the VNF providers. Further, hypervisor introspection which consists of deploying intrusion detection systems on the host operating system to defend against attacks in VMs through monitoring and intercepting VMs-related events yields an important security solution to be applied [28]. Runtime monitoring of VMs and containers, like the approach presented in [176], also constitute an important aspect to implement especially in multi-tenant environments. Interoperability issues between NFV elements (e.g., VNFs, VIM, VNFM, NFVO, etc.) require standardization efforts such as those ongoing by OpenStack [122] and OPNFV [177] to avoid service lock-in and incompatibility complications [12].

Securing interfaces and communication links is a necessity to defend against their related threats and vulnerabilities. Specifically, well-crafted APIs reduce the risks related to malformed or malicious requests aiming at ex-filtrating data. Moreover, end-to-end data encryption prevents illegitimate users from accessing the network and protect data integrity and confidentiality [12,178]. However, even when APIs are only accessed through robust security protocols [179], the concern related to man in the middle attacks remain valid, therefore, there is a need for considering advanced state of the art detection capabilities (e.g., [180,181]) from the state of the art, in addition to the adoption of best practices such as dropping connections requiring protocol downgrade.

Furthermore, guaranteeing the availability of the NFVO in particular and the NFV MANO blocks in general helps in overcoming security issues related to the centralized control and management [12].

9.2.3. Security opportunities brought by NFV

Despite the security risks introduced by NFV and the aforementioned security measures that need to be considered, we would like to shed light on the fact that NFV provides new security opportunities while supporting the security by design and the security as service. In fact, NFV offers increased flexibility and programmability when it is complemented by SDN, which provides a centralized view of the network state, facilitates customized traffic steering and supports customized security logging ad monitoring mechanisms. For example, if a network function is detected to be compromised, the NFVO enables to put it into quarantine for security analysis, and replace it with a new instance, while SDN allows rerouting traffic towards the new VNF instance. This is of course supported by the network automation advantage brought by NFV which promotes automated instantiation and life cycle management of virtual resources and services through the NFV MANO framework. Network automation enables security automation through automated provisioning and management of VSFs at different parts of the network, hence, providing a highly distributed and customized security functionality at the virtualized infrastructure at the edge, at the core or at the operator's data center based on the required quality of protection. Finally, it is worth noting that a well-designed implementation of security controls ensuring continuous monitoring, prevention, detection and mitigation of attacks within the NFV architecture is a must for a secure NFV environment [12,182].

10. Future research directions

5G networks will make extensive use of virtualization through employing NFV in order to create logically isolated networks or slices running on a common infrastructure and designated to serve multiple tenants [3]. The creation, management and orchestration of these logical networks involve a collaboration between multiple business players which adds a new level of complexity in ensuring the security of these networks. To alleviate the threats resulting from such collaborations in addition to those resulting from the logically centralized management in NFV-based networks, security needs to be thought of early at the design stage and continuously and autonomously enforced and assessed at run-time with appropriate security controls. In the following, we discuss potential open research questions that are worth the attention in order to provide secure and self-healing 5G NFV-based networks.

10.1. Trust management

5G is identified by the complexity of the collaborations existing between different business actors in order to provide a service [64]. The new 5G telecommunication business model enables new collaborations, opening up for new capabilities to create and evolve new services. Trust between different stakeholders within the 5G business model becomes

an important security challenge [64]. Hence, given that security and QoS are main requirements in 5G networks, it yields necessary to identify and evaluate the possible resulting risks before initiating any collaborations between business actors. This calls for the need of an efficient standardized trust model that captures the business actors' trustworthiness as well as the trustworthiness of their provided network systems or entities [183].

More precisely, we envision that agreements between different 5G business actors will be augmented with standardization efforts to depict a clear stakeholders trust model definition that can act as a legal agreement which helps in devising a security enforcement mechanism aligned with the responsibilities attributed to each business actor taking part in the collaboration. Defining such a model in 5G yields intrinsic in order to help with the identification of clear security boundaries and security enforcement policies [184]. From another perspective, the long chain of trust given the multi-vendor context and the heterogeneous deployments existing in an NFV environment [185–187] calls for the need of automated trust establishment and continuous evaluation and validation mechanisms [115].

10.2. Collaborative security from business to network

In the 5G telecommunication business model (Section 4.2), we notice business collaborations between players belonging to the same business category (e.g., infrastructure providers, service providers, etc.) and between those of different ones (e.g., collaboration between an infrastructure provider and a service provider, etc.). Those collaborations are coupled with new security threats matching the three dimensions of the discussed taxonomy (Section 7). Thus, we envision that 5G NFV-based networks will benefit from advancements in collaborative security to expand the idea of collaborative detection to other security controls (e.g., preventive and defensive capabilities) in order to overcome the security management complexity. Further, we picture a wider adoption of collaborative security in 5G networks that will be extended to collaboration between business players belonging to different business categories. As cross-layer attacks can cascade, for example, from the infrastructure to service and management layer, we believe that early threat detection at any of those layers which may belong to different business players can be communicated to others in order to prevent the escalation of the attack and enforce security controls at early stages. For instance, an attack can be detected at the NFVI layer by an infrastructure provider before affecting the service provider services. In this case, and following a collaborative security agreement between both parties, the infrastructure provider can initiate a mitigation strategy to mitigate the attack before it cascades to the service layer. Meanwhile, the infrastructure provider can advise the service provider to implement some prevention mechanisms. Note that such security collaborations suppose trustworthiness between business players and their network domains.

10.3. Security management framework

The automated life cycle management of network services, their distribution across multiple points of presence, in addition to the changes in the user-defined security policies, necessitate an automatic alignment of security configurations with the continuous network service changes in a timely manner to avoid inconsistencies and policy violations. The latter contribute to a privilege escalation and can be a result of deploying VNFs in a rogue NFVI (Section 7.2.3). Thus, there is an intrinsic need for a security orchestration approach compliant with the flexibility and automated life cycle management of VNFs and services offered by NFV [4].

Towards this objective, ETSI defined a policy driven NSM [166] to enable a security as a service model. Nonetheless, we notice that existing works fall short in solving many security challenges attributed to the logically centralized management and orchestration provided by NFV. We note from these challenges continuous monitoring and real-time compliance verification that translates into autonomous security enforcement measures accounting for QoS and Quality of Experience (QoE) of the provisioned 5G services. As dynamic VNF and service provisioning, scaling, migration and termination can be accompanied with security breaches related to malicious NS and VNF templates, policies or possible man in the middle attacks (Section 7.1.3), it yields challenging to orchestrate security while the aforementioned actions are performed. In this context, dynamic deployment of VSFs to secure the provisioned services while also accounting for physical security functions already existing in the network is to be considered in a complex multi-domain and multi-site deployment [188] that should be empowered with automated and intelligent detection, prevention and mitigation approaches that work hand in hand with NFV MANO.

Thus, one of the interesting research directions is the design of a fully featured security framework to provide security orchestration in accordance with NFV MANO. Such a framework is expected to make efficient use of Cyber Threat Intelligence (CTI) combined with ML to learn the best security practices and enforcement mechanisms based on real-time network state and available resources while accounting for QoS and QoE of the provisioned services.

10.3.1. Security monitoring

As we already discussed in Section 7, once the virtualization layer is breached, attackers may tamper with the VNFs and alter their proper functionality. In this context and as part of the workload integrity monitoring, there exists a need for assets discovery and profiling at different levels of granularity to enable the identification of the baseline behavior of legitimate instances in addition to the detection of unusual activities (e.g., unknown processes listening on known ports and unusual communication patterns), rogue or compromised entities. Security monitoring should support security events logging and monitoring at different levels (e.g., network counters, traces, system calls, etc.), with respect to multiple tenants' administrative boundaries to build a ground truth on VNF and service profiles. However, with the heterogeneity of VNF implementations and platforms along with the multi-tenancy model, devising effective monitoring techniques is still an open issue that requires a lot of attention.

10.3.2. ML-based attack detection

Attack detection is primordial in a security management framework. Security monitoring including VNF and service profiling in addition to learning of VNF requests patterns can be used to empower the NFVO with recognition capabilities to detect sequences of requests emanating from malicious manipulation of resources. Cognitive intelligence may also be used at the NFV MANO level to proactively forecast the upcoming threats and react adequately to prevent large scale damage. Considering the huge amount of streams of data produced by the NFV ecosystem, and which needs to be processed and analyzed instantly to support run-time verification and detection capabilities, data analytics artifacts such as data mining, ML and AI are seen as a key enablers for the design of effective systems to harden NFV security. This direction started receiving researchers' attention recently (e.g., [13,189–192]). However, there is sill a lot of effort is still to be invested in order to take full advantage of ML techniques. For example, distributed and federated learning algorithms seem to be promising ML approaches to achieve online detection of compromised components, probing activities and DDoS attacks in virtualized environments.

10.3.3. Cross-layer attacks root cause analysis

Root cause analysis is highly valuable in a security framework for efficient prevention and mitigation. In fact, the logically centralized MANO framework in NFV simplifies the management and orchestration of VNFs and services, however, it introduces new types of cascaded attacks (Section 7.2) that can have a severe impact on the whole network. Thus, there is a need for empowering NFV MANO with

security controls not only to prevent such attacks but also to efficiently detect and mitigate them [64]. This requires dynamic knowledge-based models detailing the dependencies existing between resources at different layers in real-time. Such models should be augmented with different key performance indicators along with network metrics that can help in anticipating possible attacks, detecting and mitigating them, and most importantly, identifying their root cause. Building such a model is expected to make efficient use of the NFV catalogs, alarms and performance metrics collected by the VIMs and any other monitoring tools deployed within NFV. AI and ML techniques such as reinforcement learning yield promising tools to explore for achieving cross-layer attacks root cause analysis.

10.4. Zero trust security model

The castle and moat traditional security approaches focusing on securing the network perimeter and preventing the outsider threats from penetrating the infrastructure do not fit the NFV-based 5G environments [193]. This is mainly due to the highly dynamic nature of the workloads within the cloud virtualized environments (e.g., workload creation, deletion, auto-scaling and migration operations), the reduced visibility because of the increased complexity, the lack of appropriate monitoring approaches and the multi-tenancy model where the underlying infrastructure is shared among potentially distrusted entities. Those factors create a plethora of insider threats which did not exist in the traditional corporate data centers (Section 7.1) and emphasize the need for a more distributed and adaptive security model known as the zero trust model [193]. Zero trust model suggests that all network traffic is distrusted and resources should be accessed securely at anytime [194].

In this perspective, an interesting research direction would be to leverage new security monitoring approaches and ML techniques to capture the dynamic changes in workloads, their behavior and communication patterns, and customize/enforce fine-grained security policies accordingly. This would enable to reduce the risk related to insider threats, enhance the visibility and support the zero trust security model.

10.5. Cyber threat intelligence (CTI) in NFV

Given the large scale of the NFV-based 5G environment spanning multiple domains and sites, the latter is expected to produce vast amounts of data (e.g., log files at different levels, notifications, etc.), which may include different types of abnormalities either related to malicious activities or misconfiguration issues. An interesting future research direction would be to leverage data mining techniques to extract this data and feed it to the CTI [195,196] knowledge bases in order to help in detecting suspicious activities that might threaten the NFV-based 5G environment. As an example, we can envision augmenting CTI with performance and resource fault information collected by VIMs, and suspicious event patterns observed at the NFVOs and the VNFMs, such as fake events injected by man in the middle attacks as discussed in Section 7. The augmented CTI will leverage the NFV attack detection mechanisms and predict eminent failures.

Furthermore, since virtualization and softwarization constitute an important threat vector to NFV as elaborated in Section 6.2, we believe that recovering existing information from CTI databases, such as malicious system calls, memory dumps and suspicious run-time file changes, can be used to help in profiling malicious activities, detecting them at run-time and adjusting the security policies at the management level accordingly

10.6. Policy conflict and inter-dependency management

To fit in with the flexibility and automation requirements in NFV-based 5G environments, NFV MANO highly relies on the concept of policy management. In fact, decision making at the NFV MANO functional blocks is governed and assisted by a set of policies (i.e., rules). Those policies are specified and created by multiple sources [197], which could be internal to NFV (e.g., EM or NFVO) or external (e.g., OSS/BSS) [65], and enforced by NFV MANO building blocks. This distributed authorship of policies in NFV MANO may give rise to conflicting situations where some policies are potentially defined by different sources and determine conflicting actions for the same preconditions. Policy conflicts can also be intentionally initiated by malicious actors. An example of such situation is described in Section 7.3, where the NFVO provider activates an auto-scale policy which restricts the granting of resources to the VNF types of a victim tenant.

Thus, automated, collaborative and transparent conflict resolution approaches are needed to assist the NFV MANO building blocks in enforcing valid policies and help it in taking the right actions on one side, and to boost the trust between tenants and providers on the other side. ML techniques such as reinforcement learning constitute good candidates for the systematic conciliation of conflicting policies. Those approaches could be further leveraged to learn optimized management policies, for instance, for network service self-healing after the detection of faulty components (e.g., virtual links detection).

From a different angle, policies defined at different levels (i.e., network service life cycle at the NFVO level, VNF life cycle at the VNFM level, resource and placement management at the VIM level) are inter-dependent. For instance, a network service scaling policy at the NFVO is translated to a set of VNF scaling policies at the VNFM with respect to the VNFs composing it. It may also translate into a set of affinity/anti-affinity placement requirement policies at the VIM level. Mechanisms guaranteeing the proper mapping between those inter-dependent policies and their enforcement is another research direction [197].

10.7. MEC security implications analysis

MEC plays a key role in fostering the development of myriads of real-time and mission critical 5G and beyond applications with stringent requirements [198]. For example, in vehicle-to-vehicle (V2V) and vehicle-to-everything (V2X) services, MEC facilitates provisioning VNFs at the edge to ensure the very high reliability and ultra low latency requirements. Another example is the Unmanned Aerial Vehicles (UAVs) services in public safety and smart agriculture, where the MEC allows offloading the application data from the UAVs for resource constraints accommodation and to ensure high performance and scalability [199]. To this end, MEC networks are meant to provision billions of communication devices, interconnect multiple infrastructure providers and heterogeneous access networks. This makes MEC at the intersect of diverse threat vectors emanating from different technologies. The first and potentially the most important threat vector the MEC faces lies in UEs and IoT devices which are not necessarily designed with security considerations in mind. Access networks between UEs and the base stations are constituted of radio channels which are exposed to attacks such as MitM, eavesdropping and DoS. With the expected convergence between MEC and NFV orchestration [200], MEC will also inherit all the above discussed NFV threats. Therefore, studying the security implications of the MEC NFV frameworks integration on the 5G ecosystem constitute and important topic to be addressed.

11. Conclusion

Supported by NFV, 5G networks promote multiple business collaborations between existing and emerging business players to provide

end-to-end services served by multi-site and multi-domain deployments over a shared infrastructure.

This survey was dedicated to explore the security implications of this new 5G ecosystem empowered by an NFV-based infrastructure. Thus, we first provided a high level overview of 5G network design and enabling technologies. We then shed light on NFV, one of the enabling technologies of 5G, and presented a comprehensive study on its benefits, design requirements and architecture. In light of the presented NFV-enabled 5G ecosystem, we studied the new 5G business model and compared it against the old telecommunication business model where softwarization and virtualization were absent. This new business model derives new multi-domain and multi-site deployments whose management is supported by the NFV MANO framework. Thus, we discussed the latter and then presented a 3D NFV threat taxonomy, where we analyzed the security implications of the inherent characteristics of NFV paired with the new deployment models it enables.

Finally, we presented interesting future research directions that are worth exploring from industry and academia alike, in order to enable more automated and robust NFV environments.

We believe that this survey provides insights for promoting an open 5G ecosystem driven by secure and trustworthy collaborations between different business players. We also hope that the basis of such collaborations will be promoted by holistic and intelligent NFV-based security framework benefiting from the flexibility, automation and scalability offered by NFV for efficient design and enforcement of security controls.

CRediT authorship contribution statement

Taous Madi: Conceptualization, Methodology, Writing - original draft, Writing - review & editing, Visualization. **Hyame Assem Alameddine:** Conceptualization, Methodology, Writing - original draft, Writing - review & editing, Visualization. **Makan Pourzandi:** Conceptualization, Methodology, Writing review & editing. **Amine Boukhtouta:** Validation, Writing - review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] W. Guan, X. Wen, L. Wang, Z. Lu, Y. Shen, A service-oriented deployment policy of end-to-end network slicing based on complex network theory, IEEE Access 6 (2018) 19691–19701.

[2] J.-M. Fernandez, I. Vidal, F. Valera, Enabling the orchestration of IoT slices through edge and cloud microservice platforms, Sensors 19 (13) (2019) 2980.

[3] K. Sienkiewicz, W. Latoszek, P. Krawiec, Services orchestration within 5G networks—Challenges and solutions, in: 2018 Baltic URSI Symposium, URSI, IEEE, 2018, pp. 265–268.

[4] G. Arfaoui, P. Bisson, R. Blom, R. Borgaonkar, H. Englund, E. Félix, F. Klaedtke, P.K. Nakarmi, M. Näslund, P. O'Hanlon, et al., A security architecture for 5G networks, IEEE Access 6 (2018) 22466–22479.

[5] 5G Infrastructure Association, et al., The 5G infrastructure public private partnership: The next generation of communication networks and services, 2015.

[6] 3GPP TS 23.501 V16.3.0, 3rd generation partnership project; technical specification group services and system aspects; system architecture for the 5G system (5GS); stage 2 (release 16) , 2019, https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144.

[7] N. Alliance, Service-based architecture in 5G, 2018.

[8] T. Taleb, A. Ksentini, R. Jantti, "Anything as a service" for 5G mobile systems, IEEE Netw. 30 (6) (2016) 84–91.

[9] J. Ni, X. Lin, X.S. Shen, Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT, IEEE J. Sel. Areas Commun. 36 (3) (2018) 644–657.

[10] S. Covaci, M. Repetto, F. Risso, Towards autonomous security assurance in 5G infrastructures, IEICE Trans. Commun. (2018).

[11] C.J. Bernardos, O. Dugeon, A. Galis, D. Morris, C. Simon, R. Szabó, 5G exchange (5GEx)-multi-domain orchestration for software defined infrastructures, Focus 4 (5) (2015) 2.

[12] M. Pattaranantakul, R. He, Q. Song, Z. Zhang, A. Meddahi, NFV security survey: From use case driven threat analysis to state-of-the-art countermeasures, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3330–3368.

[13] I. Farris, J.B. Bernabé, N. Toumi, D. Garcia-Carrillo, T. Taleb, A. Skarmeta, B. Sahlin, Towards provisioning of SDN/NFV-based security enablers for integrated protection of IoT systems, in: 2017 IEEE Conference on Standards for Communications and Networking, CSCN, IEEE, 2017, pp. 169–174.

[14] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, T. Taleb, Survey on multi-access edge computing for internet of things realization, IEEE Commun. Surv. Tutor. 20 (4) (2018) 2961–2991.

[15] H.A. Alameddine, S. Sharafeddine, S. Sebbah, S. Ayoubi, C. Assi, Dynamic task offloading and scheduling for low-latency IoT services in multi-access edge computing, IEEE J. Sel. Areas Commun. 37 (3) (2019) 668–682.

[16] S. Kekki, W. Featherstone, Y. Fang, P. Kuure, A. Li, A. Ranjan, D. Purkayastha, F. Jiangping, D. Frydman, G. Verin, et al., MEC in 5G networks, ETSI White Paper 28, 2018, pp. 1–28.

[17] F. Giust, G. Verin, K. Antevski, J. Chou, Y. Fang, W. Featherstone, F. Fontes, D. Frydman, A. Li, A. Manzalini, et al., MEC deployments in 4G and evolution towards 5G, ETSI White Paper 24, 2018, pp. 1–24.

[18] K. Massey, J. Goepfert, M. Shirer, Worldwide spending on security solutions forecast to reach $103.1 billion in 2019, according to a new IDC spending guide, 2019, https://www.idc.com/getdoc.jsp?containerId=prUS44935119.

[19] S.L. Thirunavukkarasu, M. Zhang, A. Oqaily, G.S. Chawla, L. Wang, M. Pourzandi, M. Debbabi, Modeling NFV deployment to identify the cross-level inconsistency vulnerabilities, in: 2019 IEEE International Conference on Cloud Computing Technology and Science, IEEE, 2019, pp. 167–174.

[20] C. Kolias, G. Kambourakis, A. Stavrou, J. Voas, DDoS in the IoT: Mirai and other botnets, Computer 50 (7) (2017) 80–84.

[21] G. Spathoulas, N. Giachoudis, G.-P. Damiris, G. Theodoridis, Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets, Future Internet 11 (11) (2019) 226.

[22] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, 5G security: Analysis of threats and solutions, in: 2017 IEEE Conference on Standards for Communications and Networking, CSCN, IEEE, 2017, pp. 193–199.

[23] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, R. Boutaba, Network function virtualization: State-of-the-art and research challenges, IEEE Commun. Surv. Tutor. 18 (1) (2015) 236–262.

[24] Y. Li, M. Chen, Software-defined network function virtualization: A survey, IEEE Access 3 (2015) 2542–2553.

[25] M. Veeraraghavan, T. Sato, M. Buchanan, R. Rahimi, S. Okamoto, N. Yamanaka, Network function virtualization: A survey, IEICE Trans. Commun. (2017) 2016NNI0001.

[26] R. Mijumbi, J. Serrat, J.-L. Gorricho, S. Latré, M. Charalambides, D. Lopez, Management and orchestration challenges in network functions virtualization, IEEE Commun. Mag. 54 (1) (2016) 98–105.

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

[28] S. Lal, T. Taleb, A. Dutta, NFV: Security threats and best practices, IEEE Commun. Mag. 55 (8) (2017) 211–217.

[29] I. Farris, T. Taleb, Y. Khettab, J. Song, A survey on emerging SDN and NFV security mechanisms for IoT systems, IEEE Commun. Surv. Tutor. 21 (1) (2018) 812–837.

[30] OpenFlow switch specification, version 1.5.1, 2015, https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-switch-v1.5.1.pdf.

[31] I. Ahmad, S. Namal, M. Ylianttila, A. Gurtov, Security in software defined networks: A survey, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2317–2346.

[32] S. Scott-Hayward, S. Natarajan, S. Sezer, A survey of security in software defined networks, IEEE Commun. Surv. Tutor. 18 (1) (2015) 623–654.

[33] D. Kreutz, F. Ramos, P. Verissimo, Towards secure and dependable software-defined networks, in: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, ACM, 2013, pp. 55–60.

[34] S. Hogg, SDN Security attack vectors and SDN hardening, Artikkeli Netw. (2014).

[35] M.C. Dacier, H. König, R. Cwalinski, F. Kargl, S. Dietrich, Security challenges and opportunities of software-defined networking, IEEE Secur. Priv. 15 (2) (2017) 96–100.

[36] T. Dargahi, A. Caponi, M. Ambrosin, G. Bianchi, M. Conti, A survey on the security of stateful SDN data planes, IEEE Commun. Surv. Tutor. 19 (3) (2017) 1701–1725.

[37] S. Scott-Hayward, G. O'Callaghan, S. Sezer, SDN Security: A survey, in: 2013 IEEE SDN for Future Networks and Services, SDN4FNS, IEEE, 2013, pp. 1–7.

[38] R. Klöti, V. Kotronis, P. Smith, OpenFlow: A security analysis, in: ICNP, Vol. 13, 2013, pp. 1–6.

[39] K. Benton, L.J. Camp, C. Small, Openflow vulnerability assessment, in: Proceedings of the Second ACM SIGCOMM Workshop on Hot Topics in Software Defined Networking, ACM, 2013, pp. 151–152.

[40] I. Khalil, A. Khreishah, M. Azeem, Cloud computing security: A survey, Computers 3 (1) (2014) 1–35.

[41] S.V.K. Kumar, S. Padmapriya, A survey on cloud computing security threats and vulnerabilities, Int. J. Innov. Res. Electr. Electron. Instrum. Control Eng. (2014) ISSN (Online)-2321-2004, Print-2321-5526.

[42] R. Bhadauria, R. Chaki, N. Chaki, S. Sanyal, A survey on security issues in cloud computing, 2011, pp. 1–15, arXiv preprint arXiv:1109.5388.

[43] R. Kumar, A. Pandey, A survey on security issues in cloud computing, Int. J. Sci. Res. Sci. Eng. Technol. 2 (3) (2016) 506–517.

[44] E. Worlanyo, A survey of cloud computing security: Issues, challenges and solutions, 2017.

[45] V. Singh, S. Pandey, Cloud computing: Vulnerability and threat indications, in: Performance Management of Integrated Systems and Its Applications in Software Engineering, Springer, 2020, pp. 11–20.

[46] N.H. Hussein, A. Khalid, A survey of cloud computing security challenges and solutions, Int. J. Comput. Sci. Inf. Secur. 14 (1) (2016) 52.

[47] H. Karajeh, M. Maqableh, R. Masa'deh, Privacy and security issues of cloud computing environment, in: Proceedings of the 23rd IBIMA Conference Vision, 2020, pp. 1–15.

[48] M. Zhou, R. Zhang, W. Xie, W. Qian, A. Zhou, Security and privacy in cloud computing: A survey, in: 2010 Sixth International Conference on Semantics, Knowledge and Grids, IEEE, 2010, pp. 105–112.

[49] R. Kanday, A survey on cloud computing security, in: 2012 International Conference on Computing Sciences, IEEE, 2012, pp. 302–311.

[50] S. Chaudhary, F. Suthar, N. Joshi, Comparative study between cryptographic and hybrid techniques for implementation of security in cloud computing, in: Performance Management of Integrated Systems and Its Applications in Software Engineering, Springer, 2020, pp. 127–135.

[51] S. Kumar, R. Goudar, Cloud computing-research issues, challenges, architecture, platforms and applications: a survey, Int. J. Future Comput. Commun. 1 (4) (2012) 356.

[52] T.J. Neela, N. Saravanan, Privacy preserving approaches in cloud: a survey, Indian J. Sci. Technol. 6 (5) (2013) 4531–4535.

[53] B. Ali, M.A. Gregory, S. Li, Multi-access edge computing architecture, data security and privacy: A review, IEEE Access 9 (2021) 18706–18721.

[54] R. Khan, P. Kumar, D.N.K. Jayakody, M. Liyanage, A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions, IEEE Commun. Surv. Tutor. 22 (1) (2019) 196–248.

[55] I. Ahmad, S. Shahabuddin, T. Kumar, J. Okwuibe, A. Gurtov, M. Ylianttila, Security for 5G and beyond, IEEE Commun. Surv. Tutor. 21 (4) (2019) 3682–3722.

[56] J. Cao, M. Ma, H. Li, R. Ma, Y. Sun, P. Yu, L. Xiong, A survey on security aspects for 3GPP 5G networks, IEEE Commun. Surv. Tutor. 22 (1) (2019) 170–195.

[57] I. Abdulqadder, D. Zou, I. Aziz, B. Yuan, W. Dai, Deployment of robust security scheme in SDN based 5G network over NFV enabled cloud environment, IEEE Trans. Emerg. Top. Comput. (2018).

[58] J. Li, Z. Feng, Z. Feng, P. Zhang, A survey of security issues in cognitive radio networks, China Commun. 12 (3) (2015) 132–150.

[59] W.S.H.M.W. Ahmad, N.A.M. Radzi, F. Samidi, A. Ismail, F. Abdullah, M.Z. Jamaludin, M. Zakaria, 5G technology: Towards dynamic spectrum sharing using cognitive radio networks, IEEE Access 8 (2020) 14460–14488.

[60] T.C. Clancy, N. Goergen, Security in cognitive radio networks: Threats and mitigation, in: 2008 3rd International Conference on Cognitive Radio Oriented Wireless Networks and Communications, CrownCom 2008, IEEE, 2008, pp. 1–8.

[61] A. Sumathi, R. Vidhyapriya, Security in cognitive radio networks-a survey, in: 2012 12th International Conference on Intelligent Systems Design and Applications, ISDA, IEEE, 2012, pp. 114–118.

[62] C.W. Tan, Cognitive Radio Networks: Performance, Applications and Technology, Nova Science Publisher Inc., 2018.

[63] I. ETSI, ETSI GS NFV 002 V1.2.1-Network Functions Virtualisation (NFV);Architectural Framework, Technical Report, 2014.

[64] G. Arfaoui, J.M.S. Vilchez, J.-P. Wary, Security and resilience in 5G: Current challenges and future directions, in: 2017 IEEE Trustcom/BigDataSE/ICESS, IEEE, 2017, pp. 1010–1015.

[65] ETSI GS NFV-MAN 001 V1.1.1, Network functions virtualisation (NFV); management and orchestration, 2014.

[66] N.F. Virtualisation, Network operator perspectives on NFV priorities for 5G, ETSI White Paper, 2017.

[67] R. Chayapathi, S.F. Hassan, P. Shah, Network Functions Virtualization (NFV) with a Touch of SDN: Netw Fun Vir (NFV EPub_1, Addison-Wesley Professional, 2016.

[68] G.N.-S.. v.2.7.1, Network functions virtualisation (nfv) release 2; protocols and data models; NFV descriptors based on TOSCA specification, in: ETSI, Group Specification, 2020.

[69] Recommendation ITU-T Y.3300 (06-2014): "Framework of software-defined networking", 2014, Available at: https://www.itu.int/ITU-T/recommendations/rec.aspx?rec=12168. (Accessed 16 June 2021).

[70] ETSI GS NFV-EVE 005 V1.1.1, Network functions virtualisation (NFV); ecosystem; report on SDN usage in NFV architectural framework, 2015.

[71] B. Blanco, J.O. Fajardo, I. Giannoulakis, E. Kafetzakis, S. Peng, J. Pérez-Romero, I. Trajkovska, P.S. Khodashenas, L. Goratti, M. Paolino, E. Sfakianakis, F. Liberal, G. Xilouris, Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN, Comput. Stand. Interfaces 54 (2017) 216–228, http://dx.doi.org/10.1016/j.csi.2016.12.007, SI: Standardization SDN & NFV. URL https://www.sciencedirect.com/science/article/pii/S0920548916302446.

[72] G. Baldoni, P. Cruschelli, M. Paolino, C.C. Meixner, A. Albanese, A. Papageorgiou, H. Khalili, S. Siddiqui, D. Simeonidou, Edge computing enhancements in an NFV-based ecosystem for 5G neutral hosts, in: 2018 IEEE Conference on Network Function Virtualization and Software Defined Networks, NFV-SDN, 2018, pp. 1–5, http://dx.doi.org/10.1109/NFV-SDN.2018.8725644.

[73] Cloud services business model transition, 2014, https://www.cisco.com/c/dam/en/us/td/docs/services/Cloud-Services-Business-Model-Transition.pdf.

[74] M.M. Al-Debei, D. Avison, Business model requirements and challenges in the mobile telecommunication sector, J. Organ. Transform. Soc. Change 8 (2) (2011) 215–235.

[75] Q. Zhang, L. Cheng, R. Boutaba, Cloud computing: state-of-the-art and research challenges, J. Internet Serv. Appl. 1 (1) (2010) 7–18.

[76] Business models in telecommunications, 2008, https://www.comarch.com/files-com/file_33/Technology-Review-2008-2-85684.pdf.

[77] S. Patil, Y. Jog, H. Pall, K.J. Batara, Understanding benefits of network function virtualization to telecom network operators, Int. J. Eng. Sci. Res. 3 (12) (2015).

[78] G.N.-R.. V1.1.1, Network functions virtualisation (NFV); accountability; report on quality accountability framework, in: ETSI, Group Specification, 2016.

[79] J. Ordonez-Lucena, P. Ameigeiras, D. Lopez, J.J. Ramos-Munoz, J. Lorca, J. Folgueira, Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges, IEEE Commun. Mag. 55 (5) (2017) 80–87.

[80] J. Cosmas, N. Jawad, M. Salih, S. Redana, O. Bulakci, 5G PPP architecture working group view on 5G architecture, 2019.

[81] S.Y. Zhu, S. Scott-Hayward, L. Jacquin, R. Hill, Guide to Security in SDN and NFV: Challenges, Opportunities, and Applications, Springer, 2017.

[82] ETSI GS NFV 001, Network function virtualization (NFV): Use cases, 2013.

[83] ETSI GR NFV-IFA 022 V3.1.1, Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on Management and Connectivity for Multi-Site Services, 2018.

[84] ETSI GR NFV-IFA 028 V3.1.1, Network Functions Virtualisation (NFV) Release 3; Management and Orchestration; Report on Architecture Options to Support Multiple Administrative Domains, 2018.

[85] ETSI GS NFV-IFA 010 V2.1.1, Network functions virtualisation (NFV); management and orchestration; functional requirements specification, 2016.

[86] European Union Agency for Network and Information Security (ENISA), Guideline on threats and assets, 2015.

[87] S.Y. Zhu, S. Scott-Hayward, L. Jacquin, R. Hill, Guide to Security in SDN and NFV: Challenges, Opportunities, and Applications, Springer, 2017.

[88] J. Finnigan, OSSN-0010, 2019, https://wiki.openstack.org/wiki/OSSN/OSSN-0010. (Accessed 28 November 2019).

[89] CVE-Details, CVE-2019-1002101, 2019, Available at: https://www.cvedetails.com/cve/CVE-2019-1002101/. (Accessed 28 November 2019).

[90] A.J. Gonzalez, G. Nencioni, A. Kamisiński, B.E. Helvik, P.E. Heegaard, Dependability of the NFV orchestrator: State of the art and research challenges, IEEE Commun. Surv. Tutor. 20 (4) (2018) 3307–3329.

[91] National Vulnerability Database, CVE-2019-12127, 2020, https://nvd.nist.gov/vuln/detail/CVE-2019-12127. (Accessed 21 July 2020).

[92] The Linux Foundation Projects, ONAP-open network automation platform, 2020, https://nvd.nist.gov/vuln/detail/CVE-2019-12127. (Accessed 21 July 2020).

[93] National Vulnerability Database, CVE-2019-12318, 2020, https://nvd.nist.gov/vuln/detail/CVE-2019-12318. (Accessed 21 July 2020).

[94] T.S.G. Services, S. Aspects, Study on security impacts of virtualisation, 2019.

[95] European Union Agency for Cyber-Security, ENISA THREAT LANDSCAPE FOR 5G NETWORKS. Threat assessment for the fifth generation of mobile telecommunications networks (5G), 2019.

[96] C. Meyer, J. Schwenk, Lessons learned from previous SSL/TLS attacks - A brief chronology of attacks and weaknesses, IACR Cryptol. ePrint Arch. 2013 (2013) 49.

[97] C. Meyer, J. Schwenk, SoK: Lessons learned from SSL/TLS attacks, in: Y. Kim, H. Lee, A. Perrig (Eds.), Information Security Applications, Springer International Publishing, Cham, 2014, pp. 189–209.

[98] T. Combe, W. Mallouli, T. Cholez, G. Doyen, B. Mathieu, E.M. De Oca, An SDN and NFV use case: NDN implementation and security monitoring, in: Guide to Security in SDN and NFV, Springer, 2017, pp. 299–321.

[99] W. Yang, C. Fung, A survey on security in network functions virtualization, in: 2016 IEEE NetSoft Conference and Workshops, NetSoft, IEEE, 2016, pp. 15–19.

[100] NFV orchestration with cisco network services orchestrator, 2019, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/solutions-cloud-providers/white-paper-c11-738702.html,

[101] Common Vulnerabilities Exposure, VENOM, CVE-2015-3456, 2015.

[102] National Vulnerability Database (NVD), CVE-2016-5195, 2019, https://nvd.nist.gov/vuln/detail/CVE-2016-5195. (Accessed 29 November 2019).

[103] T. Zhang, R.B. Lee, Host-based dos attacks and defense in the cloud, in: Proceedings of the Hardware and Architectural Support for Security and Privacy, HASP '17, ACM, New York, NY, USA, 2017, pp. 3:1–3:8.

[104] V. Varadarajan, T. Kooburat, B. Farley, T. Ristenpart, 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, CCS '12, ACM, New York, NY, USA, 2012, pp. 281–292, URL http://doi.acm.org/10.1145/2382196.2382228.

[105] CVE-Details, CVE-2016-1417, 2019, https://www.cvedetails.com/vulnerability-list/vendor_id-621/product_id-1068/Snort-Snort.html. (Accessed 27 November 2019).

[106] CVE-Details, CVE-2017-1000411, 2019, https://www.cvedetails.com/vulnerability-list/vendor_id-13628/Opendaylight.html. (Accessed 27 November 2019).

[107] R. Wojtczuk, Poacher turned gamekeeper: Lessons learned from eight years of breaking hypervisors, 2014.

[108] A.R. Riddle, S.M. Chung, 2015. A survey on the security of hypervisors in cloud computing, in: 2015 IEEE 35th International Conference on Distributed Computing Systems Workshops, 2015, pp. 100–104.

[109] E.B.F. Abdulrahman K. Alnaim, Misuse patterns for NFV based on privilege escalation, in: Proceeding of the 8th Asian Conference on Pattern Languages of Programs AsianPLoP2019, 2019.

[110] T. Madi, Y. Jarraya, A. Alimohammadifar, S. Majumdar, Y. Wang, M. Pourzandi, L. Wang, M. Debbabi, ISOTOP: Auditing virtual networks isolation across cloud layers in openstack, ACM Trans. Priv. Secur. 22 (1) (2018) http://dx.doi.org/10.1145/3267339.

[111] Common Weakness Enumeration, CWE-352: Cross-site request forgery (CSRF), 2019, http://cwe.mitre.org/data/definitions/352.html. (Accessed 23 December 2019).

[112] National Vulnerability Database, CVE-2019-18677, 2019, https://nvd.nist.gov/vuln/detail/CVE-2019-18677. (Accessed 23 December 2019).

[113] N.F.S. de Sousa, D.A.L. Perez, R.V. Rosa, M.A. Santos, C.E. Rothenberg, Network service orchestration: A survey, Comput. Commun. (2019).

[114] 5G Americas, The evolution of security in 5G: A slice of mobile threats, 2019.

[115] ETSI GS NFV-SEC 003 V1.1.1, Network functions virtualisation (NFV); NFV security; security and trust guidance, 2015.

[116] ETSI GR NFV-REL 007 V1.1.1, Network Function Virtualisation (NFV); Reliability; Report on the Resilience of NFV-MANO Critical Capabilities, 2017.

[117] R. Klöti, OpenFlow: A security analysis, 2012.

[118] H. Shawn, L. Scott, O. Tomasz, S. Adam, Uncover security design flaws using the STRIDE approach, 2006.

[119] Xen project, 2020, https://xenproject.org/. (Accessed 03 January 2020).

[120] Vmware, 2020, https://www.vmware.com/ca-fr.html. (Accessed 03 January 2020).

[121] Docker, 2020, https://www.docker.com/. (Accessed 03 January 2020).

[122] OpenStack, 2020, https://www.openstack.org/. (Accessed 03 January 2020).

[123] Kubernetes, 2020, https://kubernetes.io/. (Accessed 03 January 2020).

[124] O. AbdElRahem, A.M. Bahaa-Eldin, A. Taha, Virtualization security: A survey, in: 2016 11th International Conference on Computer Engineering Systems, ICCES, 2016, pp. 32–40.

[125] National Vulnerability Database, CVE-2017-6710, 2019, https://nvd.nist.gov/vuln/detail/CVE-2017-6710. (Accessed 23 December 2019).

[126] Yubin Xia, Yutao Liu, H. Chen, B. Zang, Defending against VM rollback attack, in: IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, DSN 2012, 2012, pp. 1–5.

[127] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, Y. Yarom, Spectre attacks: Exploiting speculative execution, 2018, CoRR abs/1801.01203. URL arXiv:1801.01203.

[128] Process hollowing, 2019, https://attack.mitre.org/techniques/T1093/. (Accessed 27 November 2019).

[129] National Vulnerability Database, CVE-2018-7218, 2019, https://nvd.nist.gov/vuln/detail/CVE-2018-7218. (Accessed 23 December 2019).

[130] F. Liu, Y. Yarom, Q. Ge, G. Heiser, R.B. Lee, Last-level cache side-channel attacks are practical, in: 2015 IEEE Symposium on Security and Privacy, 2015, pp. 605–622.

[131] Y. Xu, M. Bailey, F. Jahanian, K. Joshi, M. Hiltunen, R. Schlichting, An exploration of L2 cache covert channels in virtualized environments, in: Proceedings of the 3rd ACM Workshop on Cloud Computing Security Workshop, CCSW '11, ACM, 2011, pp. 29–40, URL http://doi.acm.org/10.1145/2046660.2046670.

[132] Y. Xiao, X. Zhang, Y. Zhang, R. Teodorescu, One bit flips, one cloud flops: Cross-VM row hammer attacks and privilege escalation, in: 25th USENIX Security Symposium, USENIX Security 16, USENIX Association, Austin, TX, 2016, pp. 19–35, URL https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/xiao.

[133] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, A. Fogh, J. Horn, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, M. Hamburg, Meltdown: Reading kernel memory from user space, in: 27th USENIX Security Symposium (USENIX Security 18), USENIX Association, Baltimore, MD, 2018, pp. 973–990, URL https://www.usenix.org/conference/usenixsecurity18/presentation/lipp.

[134] X. Gao, Z. Gu, M. Kayaalp, D. Pendarakis, H. Wang, Containerleaks: Emerging security threats of information leakages in container clouds, in: 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN, IEEE, 2017, pp. 237–248.

[135] X. Gao, B. Steenkamer, Z. Gu, M. Kayaalp, D. Pendarakis, H. Wang, A study on the security implications of information leakages in container clouds, IEEE Trans. Dependable Secure Comput. PP (2018) 1.

[136] National Vulnerability Database, CVE-2018-13365, 2019, https://nvd.nist.gov/vuln/detail/CVE-2018-13365. (Accessed 23 December 2019).

[137] NVD, CVE-2019-18679, 2019, https://nvd.nist.gov/vuln/detail/CVE-2019-18679. (Accessed 23 December 2019).

[138] Fortinet FortiOS, 2020, https://www.fortinet.com/products/fortigate/fortios.html. (Accessed 04 January 2020).

[139] Squid: Optimizing web delivery, 2020, http://www.squid-cache.org/. (Accessed 04 January 2020).

[140] NVD, CVE-2019-3635, 2019, https://nvd.nist.gov/vuln/detail/CVE-2019-3635. (Accessed 23 December 2019).

[141] NVD, CVE-2019-15225, 2019, https://nvd.nist.gov/vuln/detail/CVE-2019-15225. (Accessed 23 December 2019).

[142] H. Liu, A new form of DOS attack in a cloud and its avoidance mechanism, in: Proceedings of the 2010 ACM Workshop on Cloud Computing Security Workshop, CCSW '10, ACM, 2010, pp. 65–76, URL http://doi.acm.org/10.1145/1866835.1866849.

[143] G. Somani, M.S. Gaur, D. Sanghi, DDoS/EDoS attack in cloud: affecting everyone out there! in: SIN, 2015, pp. 169–176.

[144] W. Alosaimi, M. Zák, K. Al-Begain, R. Alroobaea, M. Masud, Economic denial of sustainability attacks mitigation in the cloud, IJCNIS 9 (2017).

[145] E. Gelenbe, O.H. Abdelrahman, Countering mobile signaling storms with counters, in: International Internet of Things Summit, Springer, 2015, pp. 199–209.

[146] CVE-Details, CVE-2019-15022, 2019, https://nvd.nist.gov/vuln/detail/CVE-2019-15022. (Accessed 23 December 2019).

[147] M.F. Kacamarga, B. Pardamean, H. Wijaya, Lightweight virtualization in cloud computing for research, in: R. Intan, C.-H. Chi, H.N. Palit, L.W. Santoso (Eds.), Intelligence in the Era of Big Data, Springer Berlin Heidelberg, 2015, pp. 439–445.

[148] R.D. Pietro, F. Lombardi, Virtualization technologies and cloud security: advantages, issues, and perspectives, 2018, CoRR abs/1807.11016.

[149] National Vulnerability Database, CVE-2019-5736, 2019, https://nvd.nist.gov/vuln/detail/CVE-2019-5736. (Accessed 21 December 2019).

[150] A. Martin, S. Raponi, T. Combe, R.D. Pietro, Docker ecosystem – Vulnerability analysis, Comput. Commun. 122 (2018) 30–43.

[151] Z. Wu, Z. Xu, H. Wang, Whispers in the hyper-space: High-speed covert channel attacks in the cloud, in: Presented As Part of the 21st USENIX Security Symposium, USENIX Security 12, USENIX, Bellevue, WA, 2012, pp. 159–173.

[152] L. Catuogno, C. Galdi, N. Pasquino, An effective methodology for measuring software resource usage, IEEE Trans. Instrum. Meas. 67 (10) (2018) 2487–2494, http://dx.doi.org/10.1109/TIM.2018.2815431.

[153] T. Zhang, Y. Zhang, R.B. Lee, Memory dos attacks in multi-tenant clouds: Severity and mitigation, 2016, ArXiv abs/1603.03404.

[154] National Iinstitute of Standards and Technologies, National vulnerability database, 2019, https://nvd.nist.gov/ (Accessed 21 December 2019).

[155] Common vulnerabilities exposures, 2019, https://cve.mitre.org/. (Accessed 21 December 2019).

[156] SNORT, 2020, https://www.snort.org/. (Accessed 04 January 2020).

[157] Envoy: Open source edge and service proxy, 2020, https://www.envoyproxy.io/. (Accessed 04 January 2020).
[158] National Vulnerability Database, CVE-2019-10097, 2019, https://nvd.nist.gov/vuln/detail/CVE-2019-3635. (Accessed 23 December 2019).
[159] The Linux Foundation Projects, OpenDaylight, 2020, https://www.opendaylight.org/. (Accessed 04 January 2020).
[160] Zingbox, 2020, https://www.zingbox.com/company/. (Accessed 04 January 2020).
[161] ETSI GS NFV-SEC 014 V3.1.1, Network functions virtualisation (NFV) release 3; NFV security; security specification for MANO components and reference points, 2018.
[162] M. Pattaranantakul, R. He, A. Meddahi, Z. Zhang, SecMANO: Towards network functions virtualization (NFV) based security management and orchestration, in: 2016 IEEE Trustcom/BigDataSE/ISPA, IEEE, 2016, pp. 598–605.
[163] M. Dhawan, R. Poddar, K. Mahajan, V. Mann, SPHINX: Detecting security attacks in software-defined networks, in: NDSS, 2015, pp. 1–15.
[164] V. Varadarajan, Y. Zhang, T. Ristenpart, M. Swift, A placement vulnerability study in multi-tenant public clouds, in: 24th USENIX Security Symposium, USENIX Security 15, USENIX Association, Washington, D.C., 2015, pp. 913–928, URL https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/varadarajan.
[165] T. Ristenpart, E. Tromer, H. Shacham, S. Savage, Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds, in: Proceedings of the 16th ACM Conference on Computer and Communications Security, CCS '09, Association for Computing Machinery, New York, NY, USA, 2009, pp. 199–212, http://dx.doi.org/10.1145/1653662.1653687.
[166] ETSI GS NFV-SEC 013 V3.1.1, Network functions virtualisation (NFV) release 3; security; security management and monitoring specification, 2017.
[167] A.M. Zarca, J.B. Bernabe, R. Trapero, D. Rivera, J. Villalobos, A. Skarmeta, S. Bianchi, A. Zafeiropoulos, P. Gouvas, Security management architecture for NFV/SDN-aware IoT systems, IEEE Internet Things J. (2019).
[168] A.E.-d. Mady, R. Trapero, A. Skarmeta, S. Bianchi, Towards secure building management system based on Internet of Things, in: Proc. CENICS, 2017, pp. 61–644.
[169] G. Gardikis, K. Tzoulas, K. Tripolitis, A. Bartzas, S. Costicoglou, A. Lioy, B. Gaston, C. Fernandez, C. Davila, A. Litke, et al., SHIELD: A novel NFV-based cybersecurity framework, in: 2017 IEEE Conference on Network Softwarization, NetSoft, IEEE, 2017, pp. 1–6.
[170] OPENFV, Moon, 2019, https://wiki.opnfv.org/display/moon/Moon. (Accessed 6 December 2019).
[171] Policy as a service ("Congress"), 2020, https://wiki.openstack.org/wiki/Congress. (Accessed 18 September 2020).
[172] OPNFV copper project, 2016, https://artifacts.opnfv.org/copper/brahmaputra/docs/design/design.pdf.
[173] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, A. Gurtov, Overview of 5G security challenges and solutions, IEEE Commun. Stand. Mag. 2 (1) (2018) 36–43.
[174] C. Sauvanaud, K. Lazri, M. Kaâniche, K. Kanoun, Anomaly detection and root cause localization in virtual network functions, in: 2016 IEEE 27th International Symposium on Software Reliability Engineering, ISSRE, 2016, pp. 196–206.
[175] C. Sauvanaud, K. Lazri, M. Kaâniche, K. Kanoun, Towards black-box anomaly detection in virtual network functions, in: 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshop, DSN-W, 2016, pp. 254–257.
[176] V.V. Sarkale, P. Rad, W. Lee, Secure cloud container: Runtime behavior monitoring using most privileged container (MPC), in: 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing, CSCloud, 2017, pp. 351–356.
[177] The Linux Foundation Project, OPNFV, 2019, https://www.opnfv.org/. (Accessed 6 December 2019).
[178] Security considerations for network functions virtualization for communications service providers, 2016, Available at: https://builders.intel.com/docs/networkbuilders/security_considerations_for_network_functions_virtualization_for_communications_service_providers.pdf,
[179] ETSI, ETSI GS NFV-SOL 013 V2.6.1- Protocols and Data Models; Specification of common aspects for RESTful NFV MANO APIs , Tech. Rep., Technical Report, 2019.
[180] Y. Wang, X. Liu, W. Mao, W. Wang, DCDroid: Automated Detection of SSL/TLS certificate verification vulnerabilities in android apps, in: Proceedings of the ACM Turing Celebration Conference - China, ACM TURC '19, 2019, pp. 1–9.
[181] S. Folarin, Improved SSL/TLS Man-In-The-Middle Attack Detection Technique Using Timing Analysis and Other Behavioral Anomalies (Master's thesis), National College of Ireland, Dublin, 2019, URL http://trap.ncirl.ie/3901/.
[182] M. Geller, P. Nair, 5G security innovation with cisco, 2018, Available at: https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/service-provider-security-solutions/5g-security-innovation-with-cisco-wp.pdf,
[183] P. Bisson, J. Waryet, 5G PPP Phase1 Security Landscape, 5G PPP Security Group White Paper, 2017.
[184] Considerations, best practices and requirements for a virtualised mobile network, 2017, Available at: https://www.gsma.com/futurenetworks/wp-content/uploads/2017/05/Virtualisation.pdf,
[185] White Paper: Considerations for Securing SDN/NFV, FCC TAC Cybersecurity Working Group, Securing SDN NFV Sub-Working Group, Available at: https://transition.fcc.gov/bureaus/oet/tac/tacdocs/reports/2016/Securing%20-SDN-NFV%20-SWG-WP-Final.pdf.
[186] How to minimize your risk in NFV implementations, 2019, https://www.ixiacom.com/resources/network-function-virtualization-nfv-5-major-risks. (Accessed 28 November 2019).
[187] ETSI GR NFV-SEC 007 V1.1.1, Network Functions Virtualisation (NFV); Trust; Report on Attestation Technologies and Practices for Secure Deployments, 2017.
[188] A.S. Sendi, Y. Jarraya, M. Pourzandi, M. Cheriet, Efficient provisioning of security service function chaining using network security defense patterns, IEEE Trans. Serv. Comput. (2016).
[189] C. Sauvanaud, K. Lazri, M. Kaâniche, K. Kanoun, Anomaly detection and root cause localization in virtual network functions, in: 2016 IEEE 27th International Symposium on Software Reliability Engineering, ISSRE, IEEE, 2016, pp. 196–206.
[190] M. Wallschläger, A. Gulenko, F. Schmidt, O. Kao, F. Liu, Automated anomaly detection in virtualized services using deep packet inspection, Procedia Comput. Sci. 110 (2017) 510–515, 14th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2017) / 12th International Conference on Future Networks and Communications (FNC 2017) / Affiliated Workshops.
[191] M. De Benedictis, A. Lioy, P. Smiraglia, Container-based design of a Virtual Network Security Function, in: 2018 4th IEEE Conference on Network Softwarization and Workshops, NetSoft, 2018, pp. 55–63.
[192] A. Molina Zarca, J. Bernal Bernabe, I. Farris, Y. Khettab, T. Taleb, A. Skarmeta, Enhancing IoT security through network softwarization and virtual security appliances, Int. J. Netw. Manag. 28 (5) (2018).
[193] D. Klein, Micro-segmentation: securing complex cloud environments, Netw. Secur. 2019 (3) (2019) 6–10.
[194] J. Kindervag, Forrester Research, Inc., 2016, Dated Mar 23.
[195] V. Mavroeidis, S. Bromander, Cyber threat intelligence model: an evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence, in: 2017 European Intelligence and Security Informatics Conference, EISIC, IEEE, 2017, pp. 91–98.
[196] R. Trifonov, O. Nakov, V. Mladenov, Artificial intelligence in cyber threats intelligence, in: 2018 International Conference on Intelligent and Innovative Computing Applications, ICONIC, IEEE, 2018, pp. 1–4.
[197] ETSI GR NFV-IFA 023 V3.1.1, Network Functions Virtualisation (NFV); Management and Orchestration; Report on Policy Management in MANO; Release 3, 2017.
[198] U. of Oulu, 6G White Paper on Edge Intelligence - 6G Research Visions, No. 8, Tech. Rep., 2020.
[199] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, T. Taleb, Survey on multi-access edge computing for internet of things realization, 20, 2018, pp. 2961–2991,
[200] ETSI, Mobile Edge Computing (MEC); Deployment of Mobile Edge Computing in an NFV environment, Tech. Rep., Technical Report, 2018.

Taous Madi is currently an Experienced Researcher at Ericsson Canada. She holds a Ph.D. in Information Systems Engineering from Concordia University, Montreal. Her research interests include network function virtualization security, software-defined networks security, internet of things security, security metrics, machine learning and formal verification. She has co-authored a book and several conference and journal articles at reputable cybersecurity venues.

Hyame Assem Alameddine is an experienced researcher at Ericsson, Montreal, Canada. She received her Ph.D. degree from the Concordia Institute of Information Systems Engineering, Concordia University, Montreal, Canada. She is the Co-Founder of the Montreal Operations Research Student Chapter, where she also held the positions of Vice President and Academic Events Director. She was the recipient of several awards, including the MITACS Elevate Postdoctoral Fellowship in 2019 and the NSERC PERSWADE award in 2018. Her research interests are in the areas of cloud computing, network function virtualization, software

defined networks, edge computing, Internet of Things, 5G, and network optimization and security.

Dr. Makan Pourzandi is a research leader at Ericsson, Canada. He received his Ph.D. degree in Computer Science from University of Lyon I Claude Bernard, France and M.Sc. in parallel computing from École Normale Supérieure de Lyon, France. He has more than 20 years of experience in the fields of cyber security, Telecom and distributed systems. He co-authored two books on cyber security published by Springer and is also the co-inventor of 21 granted US patents. He has published more than 70 research papers in peer-reviewed scientific journals and conferences. His current research interests include security, cloud computing, software security engineering.

Dr. Amine Boukhtouta is an Experienced Researcher at Ericsson Security Research Group. He received the computer science engineering degree from USTHB University, Algiers, Algeria, in 2005 and the Master of Applied Science degree in information systems security degree and the Ph.D. degree in electrical and computer engineering from Concordia University, Montreal, Canada, in 2009 and 2016, respectively. He was a Cyber-Threat Researcher within National Cyber-Forensics Training Alliance Canada, doing research on the generation of cyber-threat intelligence based on malware and network traces. He joined a Post-doc industrial program in 2016, where he worked on finding malicious indicators in evolving delivery network by applying big data analytics and machine learning. His current research interests include prevention, detection of cyber-threats by applying machine learning, and artificial intelligence. He published 5 journal papers and 11 conference papers in peer-reviewed venues. He was a recipient of OCTAS Prize in 2009 University Competition, the FQRNT Doctoral Scholarship in 2010–2011, the Best Paper Award, and the MITACS as well as PROMPT Postdoctoral Fellowships in 2016–2017.