Network Function Virtualization

Subjects: Others

Contributor: Abdulrahman Alnaim, Ahmed Alwakeel, Eduardo Fernandez

Network function virtualization (NFV) is an emerging technology that is becoming increasingly important due to its many advantages. NFV transforms legacy hardware-based network infrastructure into software-based virtualized networks. This transformation increases the flexibility and scalability of networks, at the same time reducing the time for the creation of new networks. However, the attack surface of the network increases, which requires the definition of a clear map of where attacks may happen.

Keywords: network function virtualization ; virtual network function

1. Introduction

To deliver network services to their customers, telecommunication service companies (Telcos) require a wide range of hardware appliances. With the growing demand from users for new network services, Telcos must devote more time and resources to deploying physical hardware and equipment for each network function, in addition to the need for highly skilled network technicians and operators to deal with the complexity of setting up and administering large networks. Furthermore, due to the rapid advancement of hardware, the network life-cycle is becoming shorter [1]. As a result, Telcos' operational expense (OPEX) and capital expense (CAPEX) are expected to rise.

Network function virtualization (NFV) leverages virtualization technology to provision network functions (NFs) such as load balancers, switches, firewalls, domain name server (DNS), etc., which are built in software and offered as services; it allows NFs to be performed in virtual machines (VMs) using cloud infrastructure rather than physical infrastructure [2]. Transforming network appliances into virtual network appliances reduces the need to install, maintain, and acquire special hardware at the customer premises and reduces energy consumption and cost. Also, the agility of NFV encourages network operators to adopt it due to the capability of self-management of network services, and the ability to create a new market that facilitates the development of new businesses. Moreover, NFV promises the following benefits [3]:

- Self-sufficiency: the software is no longer linked to the hardware. As a result, they will evolve independently of one another.
- Flexibility and speed: by decoupling software from hardware, it is possible to reassign and share infrastructure resources, allowing different functions to be performed at different times. As a result, network operations and their connections may be deployed more quickly and with greater flexibility.
- Scalability: in regular legacy network systems, Telcos have to be up to date with new network standards and requirements, which requires time, planning, and money. However, in NFV, decoupling software from hardware allows for dynamically scaling the actual performance of virtualized network functions with finer granularity and minimal effort.
- Reduced energy consumption: with the ability to scale up or down resources, Telcos will be able to reduce the OPEX needed to run network devices. Similarly, energy consumption at the customer end will be reduced significantly due to not having to install dedicated hardware to deliver network functions.
- Speed to set-up the network: the deployment and configuration of network services is much faster in NFV.

In October 2012, network function virtualization was introduced as a new concept by the European Telecommunications Standards Institute (ETSI). The ETSI, with the contribution of telecommunication vendors, presented the first architecture for NFV [3]. Their architecture consists of three main architectural components which are: network function virtualization infrastructure (NFVI), which comprises all the hardware and software components to support the execution of the virtualized network functions; virtual network functions (VNFs), which are software implementations of network functions;

and management and network orchestration (MANO), which covers the VNF lifecycle management and orchestration of physical and software resources.

Despite its advantages, NFV increases system complexity and is susceptible to new threats [4], which makes it important to understand its security issues. Since they rely on software, the network functions in NFV can be configured and controlled by external entities, such as a third-party provider, or a consumer. This makes manipulating the network service easier than in the traditional network infrastructure. In general, the attack surface of NFV is considerably increased compared with the traditional network infrastructure. In addition to the network resources (switches, routers, load balancers, etc.) in the traditional network infrastructure, the whole virtualization environment including live migration and multi-tenant infrastructure could be exposed to more threats than in the traditional networks. The fact that NFV is a fundamental technology of 5G networks indicates that the importance of NFV security will increase significantly. Another important technology, often used to implement NFV, is SDN. Security in 5G and SDN has been studied in several works [5][6][7]; NFV requires the support of cloud computing, and its threats have been studied in many publications. Researchers concentrate here only on modeling some of the security aspects of NFV.

Because security is a global property that requires a holistic approach, researchers strongly believe that architectural models are fundamental to produce secure networks and allow researchers to build networks which are secure by design. Researchers therefore start by finding the possible threats through analysis of NFV use cases. The use cases serve as scenarios where the threats to the architecture can be enumerated. Representing threats as misuse cases that describe the modus operandi of attackers, researchers can find countermeasures to them in the form of security patterns, and researchers can build a security reference architecture (SRA). Security patterns are encapsulated solutions to security problems, while misuse patterns describe attacks from the point of view of the attacker. Until now, only imprecise models of NFV architectures existed; by making them more detailed and precise it is possible to handle not only security but also safety and reliability, although researchers do not explore those aspects. The resulting SRA defines a roadmap to implement secure concrete architectures.

2. NFV Architecture

The network function virtualization infrastructure (NFVI) is the NFV's foundation platform, containing both hardware and virtual instantiations that make up the infrastructure on which VNFs are deployed, managed, and executed. The NFVI can be considered as a component of cloud infrastructure-as-a-service (IaaS), which allows cloud providers to establish virtual data centers (VDCs) [8], which comprise all of the virtualized computing, storage, and networking resources required to operate as a physical data center. These VDCs are given to NFV providers, who use them to provide network services to customers. The resources of a VDC offered to a specific NFV provider should be segregated from those of other providers; this isolation allows NFV providers to share the same cloud infrastructure in a secure manner. When it comes to NFV services, the VNFs are deployed over virtual machines (VMs) within a VDC.

The NFVI is made up of three basic components, as depicted in **Figure 1**. First, there are the hardware resources, which include compute facilities, which are typically commercial-off-the-shelf (COTS) appliances, storage hardware, which could be in the form of direct-attached hard disks, external storage area networks (SAN), or network-attached storage (NAS) [9], and network hardware, which could be switches/routers that provide processing and connectivity capabilities to VNFs via the virtualization layer. The virtual machine monitor (VMM) (also known as the hypervisor) is part of the virtualization layer, which sits on top of the hardware resources layer and performs three main functions: decoupling virtual resources from underlying physical resources, providing isolation among VMs, and emulating hardware resources [10]. Third, the virtual infrastructure sits on top of the virtualization layer and incorporates virtualized resources, such as virtual machines, virtual storage, and virtual networking, which are abstractions of hardware resources.

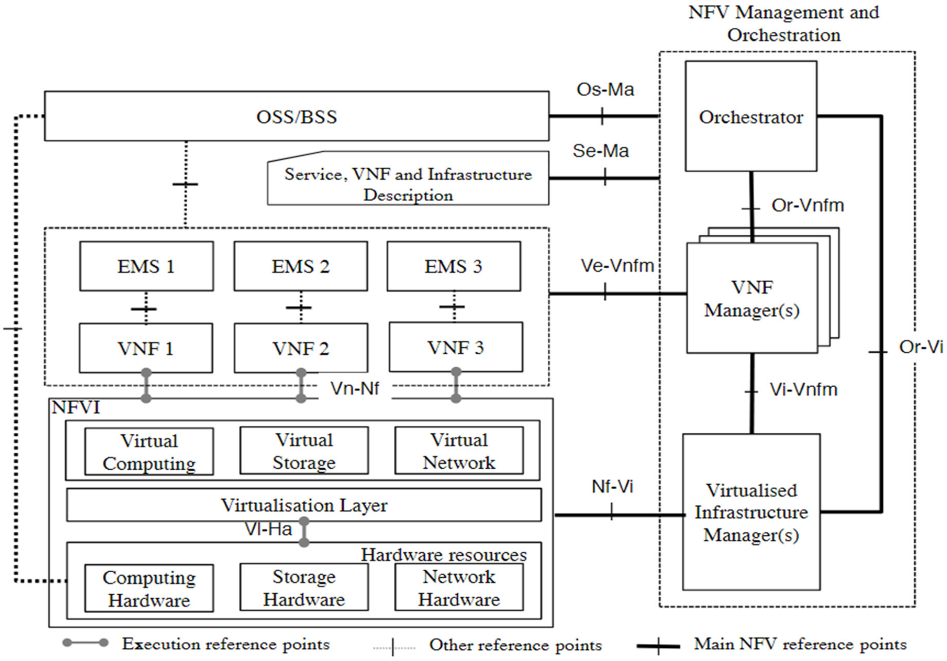

Figure 1. High-level NFV framework [3].

VNFs (virtual network functions): VNFs are software packages that represent the implementation of legacy network functions on the NFVI. Packet data network gateways (PGW), residential gateways, firewalls, and other internal components (VNFCs) could make up a single VNF [3][11]. A VNF, on the other hand, could only have one component, despite the fact that a single VNF might be deployed and dispersed across multiple VMs [3]. Further, a network graph is a collection of VNF services that together give the intended service to the customer, i.e., they might create a virtual network based on the available VNFs. Telcos' virtual network services are typically made up of many VNFs that are tailored to the demands of their customers.

NFV management and orchestration (MANO) is in charge of managing and orchestrating all virtualization-specific operations necessary throughout the VNF's lifespan, from merging several services into a single VNF package to mapping this service to consumers upon request. The MANO also manages any VNF failures that may occur, as well as maintaining state information for each VNF in the service. Furthermore, the MANO is in charge of establishing communications amongst the various VNFs that make up the network graph. The MANO is made up of three main functional blocks:

- Virtual infrastructure manager (VIM): is responsible for managing and controlling the interaction of the VNFs with the NFVI resources. The VIM performs resource management functions, such as keeping an inventory of software as well as management and orchestration of resources. The VIM is also responsible for collecting and logging information to check for faults, as well as collecting information for the purpose of capacity planning, performance monitoring, and performance optimization [3].

- VNF manager (VNFM): is responsible for managing and monitoring the VNF through the element management system (EMS), which includes scaling, changing operations, and adding new resources to the VNF, as well as communicating the states of VNFs to the other functional blocks that create the NFV architecture.

- Orchestrator: provides the necessary resources and networks needed to set up cloud-based services and applications, including the use of different virtualization software as well as hardware [9].

3. Patterns and Reference Architectures

A pattern is a solution to a recurrent problem in a specific context [12]. Patterns differ based on their purpose and the issue they solve. Security patterns are used to build secure systems by describing ways to control threats, patch vulnerabilities, and provide security attributes [13]. Design and architecture patterns are used to build flexible and extendible systems. Misuse patterns are used to describe how attacks are carried out from the attacker's perspective [14]. They also define the environment in which the attack is carried out, what security mechanisms are required as countermeasures to stop it, and where forensic information can be found to trace the attack once it has occurred.

A reference architecture (RA) is a generic abstract software architecture for analyzing, designing, and understanding complex systems. An RA includes a set of stakeholders, use cases, and a diagram that outlines system components, their functionalities, and their interdependencies but does not include implementation details [15]. Security mechanisms can be incorporated in appropriate places within the RA to manage identified threats, thus defining a security reference architecture.

Patterns are abstractions of best practices; they do not propose new solutions. Because of this, pattern papers do not include implementations or experiments, the originality of patterns and reference architectures is in the completeness and fidelity of the models with relation to existing systems; the idea is to reuse this knowledge and experience for new designs and to evaluate existing designs. SRAs are similar in intent and use and are similarly validated.

References

1. Chiosi, M.; Clarke, D.; Willis, P.; Reid, A.; Feger, J.; Bugenhagen, M.; Khan, W.; Cui, C.; Deng, H.; Chen, C. Network Functions Virtualisation (NFV): Network Operator Perspectives on Industry Progress. In Proceedings of the SDN & OpenFlow World Congress, Düsseldorf, Germany, 14–17 October 2013.
2. ETSI. Network Functions Virtualisation (NFV); Infrastructure Overview; ETSI: Sophia Antipolis, France, 2015.
3. ETSI. Network Functions Virtualisation (NFV); Architectural Framework; ETSI: Sophia Antipolis, France, 2014.
4. Milenkoski, A.; Jaeger, B.; Raina, K.; Harris, M.; Chaudhry, S.; Chasiri, S.; David, V.; Liu, W. Security Position Paper: Network Function Virtualization; Cloud Security Alliance-Virtualization Working Group, 2016; Available online: https://cloudsecurityalliance.org/artifacts/security-position-paper-network-function-virtualization/ (accessed on 30 April 2022).
5. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. Overview of 5G Security Challenges and Solutions. IEEE Commun. Stand. Mag. 2018, 2, 36–43.
6. Correa Chica, J.C.; Imbachi, J.C.; Botero Vega, J.F. Security in SDN: A Comprehensive Survey. J. Netw. Comput. Appl. 2020, 159, 102595.
7. Madi, T.; Alameddine, H.A.; Pourzandi, M.; Boukhtouta, A. NFV Security Survey in 5G Networks: A Three-Dimensional Threat Taxonomy. Comput. Netw. 2021, 197, 108288.
8. Basilier, H.; Darula, M.; Wilke, J. Virtualizing network services—The telecom cloud. Ericsson Rev. 2014, 91, 1–9.
9. SdxCentral. 2017 NFV Report Series Part I Foundations of NFV: NFV Infrastructure and VIM; SdxCentral: Santa Clara, CA, USA, 2017.
10. ETSI. Network Functions Virtualisation (NFV); Infrastructure; Hypervisor Domain; ETSI: Sophia Antipolis, France, 2015.
11. ETSI. Network Functions Virtualisation (NFV); Virtual Network Functions Architecture; ETSI: Sophia Antipolis, France, 2014.
12. Buschmann, F.; Meunier, R.; Rohnert, H.; Sommerland, P.; Stal, M. Pattern-Oriented Software Architecture Volume 1: A System of Patterns; Wiley: New York, NY, USA, 1996.
13. Fernandez, E.B. Security Patterns in Practice: Designing Secure Architectures Using Software Patterns; John Wiley & Sons: Hobokon, NJ, USA, 2013.
14. Fernandez, E.; Pelaez, J.; Larrondo-Petrie, M. Attack Patterns: A New Forensic and Design Tool. In Advances in Digital Forensics III; Springer: New York, NY, USA, 2007; pp. 345–357.
15. Avgeriou, P. Describing, Instantiating and Evaluating a Reference Architecture: A Case Study. Default J. 2003, 342, 1–24.