Computer Communications and Networks

Shao Ying Zhu
Sandra Scott-Hayward
Ludovic Jacquin
Richard Hill *Editors*

# Guide to Security in SDN and NFV

## Challenges, Opportunities, and Applications

Springer

# Computer Communications and Networks

**Series editor**
Prof. A.J. Sammes
Cyber Security Centre
Faculty of Technology
De Montfort University
Leicester, UK

The **Computer Communications and Networks** series is a range of textbooks, monographs and handbooks. It sets out to provide students, researchers, and non-specialists alike with a sure grounding in current knowledge, together with comprehensible access to the latest developments in computer communications and networking.

Emphasis is placed on clear and explanatory styles that support a tutorial approach, so that even the most complex of topics is presented in a lucid and intelligible manner.

More information about this series at http://www.springer.com/series/4198

Shao Ying Zhu • Sandra Scott-Hayward
Ludovic Jacquin • Richard Hill
Editors

# Guide to Security in SDN and NFV

## Challenges, Opportunities, and Applications

Springer

*Editors*
Shao Ying Zhu
University of Derby
Derby, UK

Ludovic Jacquin
Hewlett Packard Labs
Bristol, UK

Sandra Scott-Hayward
Queen's University Belfast
Belfast, UK

Richard Hill
University of Huddersfield
Huddersfield, UK

ISSN 1617-7975 ISSN 2197-8433 (electronic)
Computer Communications and Networks
ISBN 978-3-319-64652-7 ISBN 978-3-319-64653-4 (eBook)
DOI 10.1007/978-3-319-64653-4

Library of Congress Control Number: 2017956124



Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Foreword

When I joined the Open Networking Foundation on its launch day in 2011, I enjoyed nearly a full year of unbridled excitement at how SDN would transform the networking industry (the promise that had (finally) convinced me to return to the networking industry) before the topic of security barged in on my reverie. I had just finished what I thought were some inspiring remarks at a conference in Germany when a reporter confronted me with the assertion that the SDN controller would be a single point of failure and an obvious target for cybercriminals. "Now they can take down the entire network by hacking one box", he contended. That same month I sat in the audience for a seminar at the RSA Conference in San Francisco on the subject of SDN security led by Roy Chua and Matt Palmer of what is now SDxCentral. Every talk related to the topic of SDN's vulnerabilities. A month later I had my first (and only) encounter with Vint Cerf (the so-called Father of the Internet for his invention of TCP/IP and now Chief Internet Advocate at Google). Vint was famous and I wanted to meet him, so I asked ONF's Board Chair Urs Hölzle of Google for an introduction. In my private one-hour meeting with Vint, the only subject he wanted to discuss was whether OpenFlow mandated out-of-band signalling (for the security of control flows). Reverie over.

Not long thereafter, Marc Woolward, then of Goldman Sachs and now with vArmour, spearheaded a working group in ONF on security that moved swiftly to require all ONF working groups to include a statement in their charter on the security impacts of their respective projects. This attempt to build in security rather than adding it on after the fact achieved only marginal success due to the inertia of the groups and the lack of expertise in security matters. We did not really get our arms around what SDN security even meant until I witnessed a presentation at the Ethernet Technology Summit by an academic researcher from Northern Ireland (of all places, I remember thinking) who depicted the landscape – in both theoretical and commercial terms – with such clarity that I believed we could systematically tackle the challenge and the controversy of SDN security. That researcher was this volume's editor Sandra Scott-Hayward, who immediately joined ONF as a research associate and led the project to develop threat models that finally enabled us to quantify the issues defining how to make sure an SDN was itself secure. The working group even built some open-source tools (called Project Delta) that went on to win awards.

I do not remember exactly when I realized that the most interesting aspect of SDN security was its ability to provide unprecedented capabilities to assure the security of networks. Consider the routing provided by OpenFlow versus that of Open Shortest Path First (OSPF). With OSPF, autonomous systems (Internet routers) exchange distributed protocols to choose a route (the shortest path) between two IP addresses. All flows – and there could be many, even between your browser and a website – between those two addresses follow the same route, regardless of their individual characteristics. At any given time it's almost impossible to predict or detect, much less control, that route. With OpenFlow, on the other hand, the SDN controller explicitly instructs the switches in its domain to set up specific, known paths from source to destination. Moreover, these paths apply to individual flows, defined by not just IP addresses but also MAC addresses, application identifiers or even user metadata. Network operators may create control programmes (path-selection algorithms) that reflect technical objectives such as minimizing congestion or latency or business objectives such as maximizing network utilization, minimizing energy consumption or guarding profit or assuring security.

When ONF launched, the pesky press in Germany suggested SDN could be a tool for evil network operators to manipulate traffic flows against the public interest. Then at the same conference in Germany I mentioned above, another journalist warned of the emerging regulations for data border control, by which some countries mandated that certain data never flow outside the borders of that country, for reasons of national security and privacy. Here, I seized upon SDN's being the only way to provide data border control. Flows of national interest (or of national residents) follow only those paths that keep them within the borders of the country. Like any tool, SDN can serve noble ends or evil ones, depending on how an operator chooses or a government regulates. Over time we have seen more and more examples of how SDN enhances network security, perhaps most commonly in its rapid isolating of distributed denial of service (DDoS) attacks. As IoT brings the dramatic proliferation of traffic sources on networks of all scales, and mobile edge computing places more computing power near traffic sources, SDN looks to me as the saviour of network security.

This book wisely includes both SDN and NFV; they are not unrelated. Yes, NFV virtualizes network functions (many of them artifacts of hardware-defined networking that will seem archaic in a few years) while SDN separates, both logically and physically, the control and data planes. NFV may operate almost self-contained in a hypervisor environment within a data centre, but in the real world, networks operate with real switching in the network access, aggregation and core sections. Both network operators and their customers (enterprises, governments, small businesses and even consumers) increasingly expect network operation to reflect policies and priorities of their choice. The only way for the control software to convey the desired behaviour to the network elements that implement it is via SDN (whose toolbox contains OpenFlow, Netconf and other communication vehicles).

As the networking industry embraces the advances of modern computing, from distributed systems (such as those that prevent the SDN controller from becoming a single point of failure with any greater likelihood than whatever server gives you

your bank balance the next time you check could also fail and take your money with it) to predictive analysis and other elements of AI, we will see more and better choices on how to build and govern networks. Frameworks for orchestration and policy, based on combinations of open-source and proprietary code, will modularize what today are monolithic programmes that lock operators into rigid, single-vendor solutions with little opportunity for operator uniqueness. High-performance chips with DPI will add new granularity to the definition of what constitutes a flow and how to treat it. Microservices architectures will place appropriate computing, storage and connectivity resources at the behest of individual workloads, in a highly time-dynamic fashion.

None of this computing and networking exists to perform security. It exists to support commerce and the social fabric of life. We need security only because more and more valuable portions of our lives depend on information technologies. These technologies fail from a security standpoint because of errors we make in design or operation and because some people deliberately attack them for either profit or the morbid satisfaction of disruption.

It won't be many years before we look back and wonder how in the world we got along without Software Defined Network Function Virtualization (SDNFV). Because it will be so pervasive, we have an obligation to assure its security. This book offers an excellent purview of the challenges, solutions and remaining opportunities to both secure SDNFV and exploit it as a tool to assure network security, perhaps the best tool we have ever found.

Palo Alto Innovation Advisors, Palo Alto, CA, USA Dan Pitt

# Preface

We have been motivated to produce this book through our research work on security in and of software-defined networking (SDN) and network functions virtualization (NFV). One of the editors of the book has been directly involved with the Open Networking Foundation (ONF), acting as Vice-Chair of the Security Working Group. A second editor has been engaged with the security programme of ETSI NFV and the IRTF SDN Research Group. Our observation through this work and the academic and industry research communities is that there is a necessity to broaden awareness of the importance of security in the design, development and deployment of SDN- and NFV-based systems, as well as to understand how current security mechanisms can be applied, either directly or with modification in the SDNFV context.

Since the beginning of the SDN/NFV security discussion, there has been an obvious split between, on the one hand, consideration of security challenges introduced by the new SDN architecture and the virtualization of network functions and, on the other hand, the potential benefits to securing the network with the technologies of SDN and NFV. Over a number of years, it has become clear that these technologies will be fundamental to the evolution of future networks.

From these aspects of SDNFV security, three sections of the book have naturally emerged. Part I introduces the key concepts of security in SDNFV. Part II presents a series of SDNFV-based network security solutions, and Part III covers the application of SDNFV security in future networks.

In Part I, we begin with Hoang and Farahmandian's introduction to the security challenges of SDN, NFV and cloud computing. In this chapter, they bring together these three interlinked technologies for a survey of the security of the integrated software infrastructure and conclude with a conceptual software-defined security service architecture. In Chap. 2, Faynberg and Goeringer discuss NFV security with a detailed reflection on the work of the ETSI NFV Security Working Group and the industry view it has formulated since its foundation in 2012. This chapter presents a comprehensive, tutorial-style description of NFV security. Much work on SDNFV security targets either SDN or NFV security separately. In Chap. 3, Murillo et al. present a survey of the proposals to secure SDN/NFV platforms and the challenges

for their integration. Chavers et al. present a comprehensive overview of the use of root-of-trust services to secure NFV and Lioy et al. propose a solution to evaluate trust by exploiting remote attestation. Together, the chapters of Part I cover the key concepts in SDNFV security, providing a baseline for exploring the solutions presented in subsequent chapters.

The focus of Part II is to present some specific SDNFV security solutions. In Chap. 5, Pastor and Folgueira describe the process of implementing a virtual home gateway with real residential broadband customers and the practical experience of the security design requirements to do this. Cox et al. present a security policy transition framework for SDN tackling the real issue of revoking or updating policy enforcements following a client resolution of the network policy violation. In Chap. 7, Ali et al. demonstrate the potential for the combined power of SDN and NFV to offer network-wide security in virtualized ICT environments. Their solution is an SDNFV-based DDoS detection and remediation framework. In the final chapter of Part II, Attak et al. present the work of the EU-funded SHIELD project, securing against intruders and other threats through a NFV-enabled environment. SHIELD aims at combining flexible and dynamic security monitoring with big-data analytics to detect threats at the network-wide level.

With Part III, the security implications of SDNFV in evolving and future networks are considered. The section begins with a look at Industry 4.0. Khondoker et al. investigate the use of SDN tools and technologies to protect Industry 4.0 machines and components from network-based threats. The ability to fulfil the requirements of 5G is recognized to be dependent on SDNFV technologies. In Chap. 11, Santos et al. study the security requirements for multi-operator virtualized network and service orchestration for 5G. The security perspectives of the standards organizations (ITU-T and ETSI) are described and a threat analysis is presented. The improvement of security in coalition tactical environments is the subject of Chap. 12. Mishra et al. present the Observe, Orient, Decide and Act (OODA) paradigm and how the security of OODA can be enhanced with SDN. Finally, in Chap. 13, Combe et al. propose a monitoring solution for a Named Data Networking (NDN) architecture that builds on the capabilities of SDN and NFV for more efficient security monitoring.

As previously identified, one of the main objectives of publishing this compilation is for this to be an educational tool focussing on this important aspect of network technologies. In support of this, each author has included a number of questions at the end of their chapter to test the reader's understanding of the key concepts introduced in the chapter. The layout of the book is designed with this in mind, beginning with some survey style introductions to security in SDN and NFV and leading on to future network concepts.

We believe that the reader of this book will grasp the large scope of the security challenges and potential in relation to SDNFV systems. In addition, with his/her awareness raised, the reader will be able to develop new security-related

mechanisms for SDNFV systems or to design next-generation communication networks more securely, thanks to SDNFV.

Derby, UK — Shao Ying Zhu
Belfast, UK — Sandra Scott-Hayward
Bristol, UK — Ludovic Jacquin
Queensgate, UK — Richard Hill

# Acknowledgement

The editors acknowledge the support of the following colleagues during the review and editing phases of this book:

Colin Allison (University of St Andrews)
Marco Anisetti (Università degli Studi di Milano)
Marta Beltran (Universidad Rey Juan Carlos)
Stéphane Betgé-Brezetz (Nokia Bell Labs)
Gergely Biczók (Univ. of Technology and Economics)
Carolina Canales-Valenzuela (Ericsson)
Augusto Ciuffoletti (Università di Pisa)
Emmanuel Dotaro (Thales)
Jordi Ferrer Riera (i2CAT)
Olivier Festor (Inria)
Georgios Gardikis (Space Hellas S.A.)
Bernat Gaston (Fundació Privada I2CAT)
Dimitrios Gkounis (NEC Laboratories Europe)
Doan Hoang (University of Technology, Sydney)
Michail Alexandros Kourtis (NCSR Demokritos)
Bryan Larish (Verizon)
Kahina Lazri (Orange Labs)
Jianxin Li (Beihang University)
Antonio Lioy (Politecnico di Torino)
Diego Lopez (Telefonica I + D)
Linas Maknavicius (NOKIA Bell Labs)
Evangelos Markakis (Technological Education Institute of Crete)
Marie-Paule Odini (Hewlett Packard Enterprise)
Abdelkader Outtagarts (Alcatel-Lucent Bell Labs)
Nicolae Paladi (RISE SICS)
Antonio Pastor (Telefonica I + D)
Dimitrios Pezaros (University of Glasgow)
Fernando Ramos (University of Lisbon)
Sachin Sharma (NEC Laboratories Europe)

Seungwon Shin (Korea Advanced Institute of Science and Technology)
Muhammad-Shuaib Siddiqui (i2CAT)
Eleni Trouva (NCSR Demokritos)
Ziming Zhao (Arizona State University)
Thomas Zinner (University of Wuerzburg)

The editors acknowledge the effort of the authors of the individual chapters without whose work this book would not have been possible.

Shao Ying Zhu, University of Derby, UK
Sandra Scott-Hayward, Queen's University Belfast, UK
Ludovic Jacquin, Hewlett Packard Labs, UK
Richard Hill, University of Huddersfield, UK

# Contents

# Contributors

**Abeer Ali** School of Computing Science, University of Glasgow, Glasgow, Scotland, UK

**Hamza Attak** Hewlett Packard Labs, Bristol, UK

**Kpatcha Bayarou** Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT), Darmstadt, Germany

**Gergely Biczók** CrySyS Lab, Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, Hungary

**Álvaro A. Cárdenas** Department of Computer Science, UT Dallas, Richardson, TX, USA

**Marco Casassa-Mont** Hewlett Packard Labs, Bristol, UK

**Jesús Folgueira** Telefonica I+D, Madrid, Spain

**Thibault Cholez** INRIA, Rocquencourt, France

**Russell J. Clark** College of Computing, Georgia Institute of Technology, Atlanta, GA, USA

**Théo Combe** Thales Services, La Défense, France

**Jacob H. Cox Jr** School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA

**Richard Cziva** School of Computing Science, University of Glasgow, Glasgow, Scotland, UK

**Cristian Dávila** Fundació I2CAT, Barcelona, Spain

**Eleni-Constantina Davri** Orion Innovations P.C., Athens, Greece

**Edgardo Montes de Oca** Montimage, Paris, France

**Guillaume Doyen** UTT, Troyes, France

**Sarah Farahmandian** University of Technology Sydney, Ultimo, NSW, Australia

**Igor Faynberg** Cable Labs, Louisville, CO, USA

**Carolina Fernandez** Fundació I2CAT, Barcelona, Spain

**Georgios Gardikis** Space Hellas S.A., Athina, Greece

**Bernat Gaston** Fundació I2CAT, Barcelona, Spain

**Steve Goeringer** Cable Labs, Louisville, CO, USA

**Doan B. Hoang** University of Technology Sydney, Ultimo, NSW, Australia

**Ludovic Jacquin** Hewlett Packard Labs, Bristol, UK

**Simon Jouët** School of Computing Science, University of Glasgow, Glasgow, Scotland, UK

**Rahamatullah Khondoker** Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT), Darmstadt, Germany

**Pedro Larbig** Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT), Darmstadt, Germany

**Antonio Lioy** Dipartimento di Automatica e Informatica, Politecnico di Torino, Torino, Italy

**Antonis Litke** Infili Technologies PC, Athens, Greece

**Diego R. Lopez** Telefonica I+D, Seville, Spain

**Wissam Mallouli** Montimage, Paris, France

**Barbara Martini** Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT), Pisa, Italy

**Bertrand Mathieu** Orange, Paris, France

**Vinod K. Mishra** U.S. Army Research Labs, Aberdeen, MD, USA

**Laura Victoria Morales** Systems and Computing Engineering Department, Universidad de los Andes, Colombia

**Jerónimo Núñez** Telefónica I+D, Madrid, Spain

**Henry L. Owen III** School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA

**Francesco Paolucci** Scuola Superiore Sant'Anna, Pisa, Italy

**Nikolaos K. Papadakis** Infili Technologies PC, Athens, Greece

**Dimitris Papadopoulos** Infili Technologies PC, Athens, Greece

**Antonio Pastor** Telefonica I+D, Madrid, Spain

**Dimitrios P. Pezaros** School of Computing Science, University of Glasgow, Glasgow, Scotland, UK

**Andrés Felipe Murillo Piedrahita** Systems and Computing Engineering Department, Universidad de los Andes, Bogotá, Colombia

**Alireza Ranjbar** Ericsson Research, Finland, Finland

**Sandra Julieta Rueda** Systems and Computing Engineering Department, Universidad de los Andes, Bogotá, Colombia

**Mateus Augusto Silva Santos** Ericsson Telecomunicações S/A, Indaiatuba, Brazil

**Dirk Scheuermann** Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT), Darmstadt, Germany

**Adrian L. Shaw** Hewlett Packard Enterprise, Bristol, UK

**Tao Su** Dipartimento di Automatica e Informatica, Politecnico di Torino, Torino, Italy

**Eleni Trouva** Institute of Informatics and Telecommunications NCSR "Demokritos", Agia Paraskevi, Greece

**Dinesh C. Verma** IBM T J Watson Research Center, Yorktown Heights, NY, USA

**Frank Weber** Fraunhofer Institute for Secure Information Technology (Fraunhofer SIT), Darmstadt, Germany

**Christopher Williams** Defence Science and Technology Laboratories, Salisbury, Wiltshire, UK

# About the Editors

**Dr. Shao Ying Zhu** is a Senior Lecturer in Computing at the University of Derby, UK. She is the programme leader for M.Sc. Advanced Computer Networks and B.Sc. Computer Networks and Security. She has published many peer-reviewed conference and journal papers on a wide range of topics such as image processing, e-learning, computer networks and cloud security. She has edited a number of books for Springer's Computer Communications and Networks series and organised many IEEE workshops on network security subject areas. She has also served as programme committee member for many conferences and reviewer for several international journals.
Email: s.y.zhu@derby.ac.uk

**Dr. Sandra Scott-Hayward**, CEng, is a Lecturer (Assistant Professor) at Queen's University Belfast. She has experience in both research and industry, having worked as a Systems Engineer and Engineering Group Leader with Airbus before returning to complete her Ph.D. at Queen's University Belfast. In the Centre for Secure Information Technologies at QUB, Sandra leads research and development of network security architectures and security functions for software-defined networks (SDN). She has presented her research globally and has published a series of IEEE papers on performance and security designs for SDN. Sandra is Vice-Chair of the Open Networking Foundation (ONF) Security Working Group and has received Outstanding Technical Contributor and Outstanding Leadership awards from the ONF in 2015 and 2016, respectively.
Email: s.scott-hayward@qub.ac.uk

**Dr. Ludovic Jacquin** is a Senior Researcher at Hewlett Packard Labs – the research organisation of Hewlett Packard Enterprise – in Bristol, UK. He holds an M.Sc. in Applied Mathematics and Computer Science from ENSIMAG (Grenoble, France) and received his Ph.D. in Computer Science from Grenoble University (France) in 2013. His broader research interest is to develop security mechanisms for computer and network infrastructure, both at the hardware and operating system level. He joined the Security Lab of Hewlett Packard Enterprise in 2014 with a focus on trust and attestation of the network infrastructure in the new paradigm of SDN and

their application to related environments such as NFV. During his Ph.D., he mainly worked on the impact of network signalling protocols on security protocols such as IPsec.
Email: ludo@hpe.com

**Professor Richard Hill** is Head of the Department of Informatics and Director of the Centre for Industrial Analytics and Design Innovation at the University of Huddersfield. Richard has published widely in the areas of Big Data, predictive analytics, the Internet of Things, and Industry 4.0, and has specific interests in the use of digital technologies to create new value-creation opportunities.
Email: r.hill@hud.ac.uk

# Part I

# Introduction to Security in SDNFV – Key Concepts

# Security of Software-Defined Infrastructures with SDN, NFV, and Cloud Computing Technologies

1

Doan B. Hoang and Sarah Farahmandian

## 1.1 Introduction

Software-defined networking separates the control plane from the underlying network data plane for both efficient data transport and fine-grained control of network management and services. SDN allows network virtualization and provision of virtual networks on demand. Network functions virtualization is a network architecture concept in which network functions are virtualized, implemented in software, and deployed strategically with the support of a dynamic virtual/physical infrastructure/platform to provide network services.

Cloud computing relies on its aggregation and centralization of virtual resources and their flexible provision and orchestration to provide services to its customers.

Software-defined networks, network functions virtualization platforms, and clouds have established themselves as modern IT service infrastructures. They all rely on the virtualization technology to virtualize and aggregate physical resources into pools of virtual resources (virtual machines, virtual networks, virtual storage, virtual functions, and virtual services) and provision them to users on demand. Security has been recognized as an essential and integral part in the design of systems, infrastructures, organizations, and services; yet, the current state of security research and practice is at best fragmented, local, or case specific. With modern infrastructures that support ever-increasing complex and pervasive applications, such as social networks, Internet of everything, mobile applications, cloud services, new security models, and innovative security, technologies must be invented to match the complexity of emerging applications and the sophistication of their attackers.

D.B. Hoang (✉) • S. Farahmandian
University of Technology Sydney, Ultimo, NSW, Australia
e-mail: Doan.Hoang@uts.edu.au; sarah.farahmandian@student.uts.edu.au



S.Y. Zhu et al. (eds.), *Guide to Security in SDN and NFV*, Computer Communications and Networks, DOI 10.1007/978-3-319-64653-4_1

This chapter discusses the security of those software-defined infrastructures using their paradigms and their underlying technologies: virtualization of network infrastructures, virtualization of virtual machines, network functions, and security functions and services. In particular, it explores security architectures, virtual security elements, and virtual connectivity infrastructures for supporting security goals and services. The chapter is organized as follows. Section 1.2 summarizes the defining characteristics and the common virtualization technology of SDN, NFV, and cloud computing. Section 1.3 provides a summary of major security challenges specific to SDN, NFV, and cloud. Section 1.4 discusses key security challenges and solutions to SDN, NFV, and cloud including virtualization, isolation, and security of identity and access management. Section 1.5 discusses the security of OpenStack, a widely deployed platform for implementing cloud-SDN-NFV infrastructure. Section 1.6 reviews and discusses the development of the new software-defined security approach. Section 1.7 concludes the chapter with some remaining challenges.

## 1.2 Defining Characteristics of Software-Defined Networking, Network Functions Virtualization, and Cloud Computing

This section provides a brief description of SDN, NFV, and cloud computing and their defining characteristics. Virtualization is described as the common underlying technology, and its security is one of the key security challenges in SDI.

### 1.2.1 Software-Defined Networking

Software-defined networking has emerged as a networking paradigm that separates the data forwarding plane from the control plane by centralizing the network state and the decision-making capability in the control plane (SDN controller), leaving simple forwarding operation at the data plane (SDN network devices), and abstracting the underlying network infrastructure to the application plane. The separation of the control plane and the data forwarding plane is through a programming interface between the SDN network devices and the SDN controller.

The Open Networking Foundation (ONF) defines a high-level architecture for SDN [3], with three main layers as shown in Fig. 1.1: the application layer for expressing and orchestrating application and network service requirements; the control layer for network control, services provisioning, and management; and the infrastructure layer for abstraction of physical network resources. The infrastructure layer can be expanded into two planes: the physical plane and the virtual plane. The physical resources plane consists of the underlying physical infrastructure, and the virtual resources plane represents the virtual resources abstracted from the physical resources through virtualization.

SDN network devices are all placed at the infrastructure layer. The SDN network devices make a simple decision of what to do with incoming traffic (frames or packets) according to instructions programmed by their SDN controller. The SDN

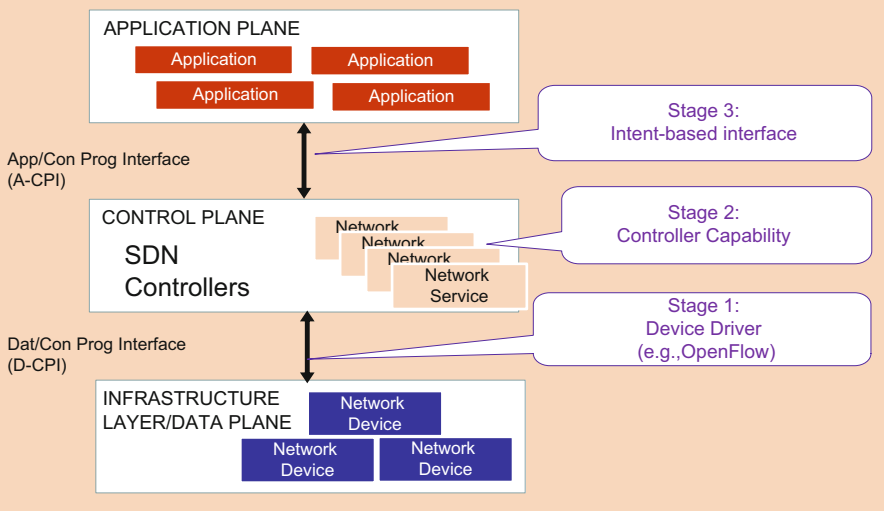


**Fig. 1.1** Software-defined network architecture

controller (or group of controllers) is located in the control layer. It programs and controls the forwarding behavior of the network devices and presents an abstraction of the underlying network infrastructure to the SDN applications. Applications and network services are on the application layer. The controller allows applications to define traffic flows and paths, with the support of a comprehensive information database of all underlying network infrastructure operations, in terms of common characteristics of packets to satisfy the applications' needs and to respond to dynamic requirements by users and traffic/network conditions [11].

The SDN controller uses interfaces for communicating with other layers. To communicate with the data/infrastructure layer, a southbound interface (SBI) is used for programming and configuring network devices. To communicate with the application layer, a northbound interface (NBI) is provided for the interaction between the SDN controller and applications. The NBI is to describe the needs of the application and to pass along the commands to orchestrate the network. East/west interfaces are for information exchange between multiple or federated controllers. The OpenFlow protocol has been developed and widely adopted as one of the SBIs between SDN controllers and SDN switches. OpenFlow uses a secure channel for message transmission over the Transport Layer Security (TLS) connection.

### 1.2.2 Network Functions Virtualization

Network functions virtualization (NFV) is proposed aiming to virtualize an entire class of network component functions using virtualization technologies. The objective is to decouple the network functions from the network equipment. A network

function is now a virtual instance of customized software program called a virtual network function (VNF). This object can be created on demand, launched into operation wherever needed without the need for installation of new equipment (on any virtual or physical servers at data centers, gateways, routers). It can be moved at will and terminated when its function is no longer needed [2]. The NFV enables network functions to be executed as software instances in a virtual machine (VM) on a single or multiple hosts instead of customized hardware equipment. Network functions virtualization can be applied to both data and control planes in fixed or mobile infrastructures. The NFV provides operators the ability to combine numerous different types of network equipment into high-volume switches, servers, and storage inside data centers, network nodes, and end user premises. It offers a new means for creating, deploying, and managing networking services.

Examples of these classless of functions include switching elements; tunnel gateway elements: IPSec/SSL (secure sockets layer), VPN (virtual private network) gateways; security functions: firewalls, virus scanner, and intrusion detection systems; traffic analysis services: load balancers, network monitoring, and deep packet inspection tools; service assurance: SLA (service-level agreement) monitoring, test, and diagnostics; mobile network elements: multifunction home router, set top boxes, base stations, and the evolved packet core (EPC) network [13].

ETSI provides an NFV reference architecture for a virtualized infrastructure and points of reference to interconnect the different components of the architecture. The NFV architecture has three key components for building a practical network service: network functions virtualization infrastructure (NFVI), VNFs, and NFV management and orchestration (MANO) [8]. Figure 1.2 shows an overall view of NFV architecture adapted from ETSI NFV model.

The NFVI includes hardware and a hypervisor that virtualizes and abstracts the underlying resources. The VNF is the software implementation of a network function which runs over the NFVI. The NFV MANO is responsible for configuring, deploying, and managing the life cycle of VNFs. An important key principle of NFV is service chaining: as each VNF provides limited functionality on its own, service chaining allows combining multiple VNFs to create useful new network functions and services.

### 1.2.3 Cloud Computing

Cloud computing has become an alternative IT infrastructure where users, infrastructure providers, and service providers all share and deploy resources for their business processes and applications. Business customers are shifting their services and applications to cloud computing since they do not need to invest in their own costly IT infrastructure but can delegate and deploy their services effectively to cloud vendors and service providers [37].

Cloud computing offers an effective solution for provisioning services at lower costs, on demand over the Internet by virtue of its capability of pooling and virtualizing computing resources dynamically. Clients can leverage a cloud to store

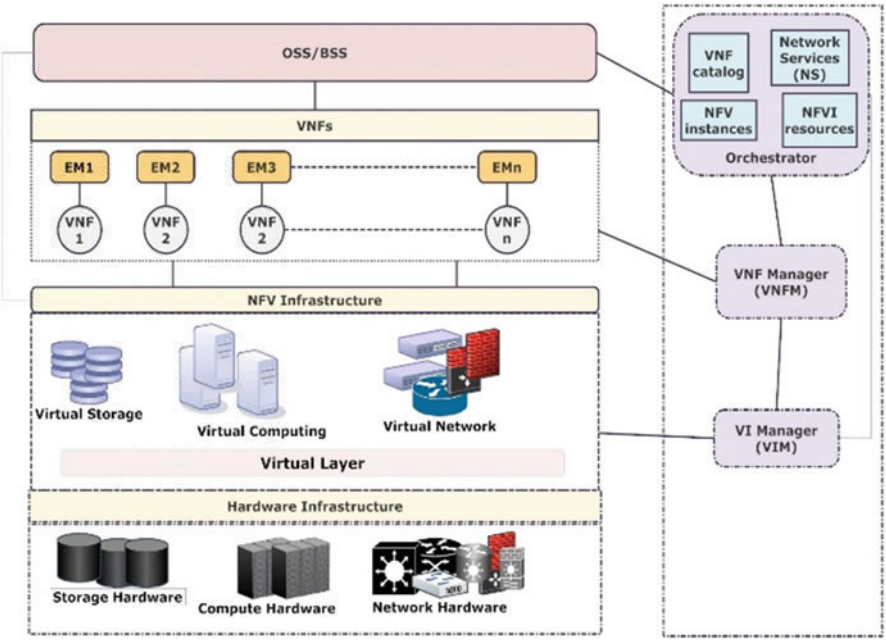


**Fig. 1.2** NFV architecture

their documents online, share their information, and consume or operate their services with simple usage, fast access, and low cost on a remote server rather than physically local resources [26].

The most relevant definition is probably the one provided by the National Institute of Standards and Technology (NIST) [17]: "Cloud computing is a model for enabling ubiquitous, convenient, on-demand, network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." This cloud model is composed of five essential characteristics, three service models, and four deployment models. The five characteristics are on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) constitute the three service models. SaaS directly offers cloud services such as Google Docs, Google Map, Google Health, etc., online to users. With PaaS, developers can order a required development platform, which may consist of SDK (software development kit), documentation, and test environment, to develop their own applications. IaaS is more about packaging and provisioning underlying virtual resources to customers, who then build, orchestrate, provision, and sell tailored infrastructure resources to organizations to support their own businesses.

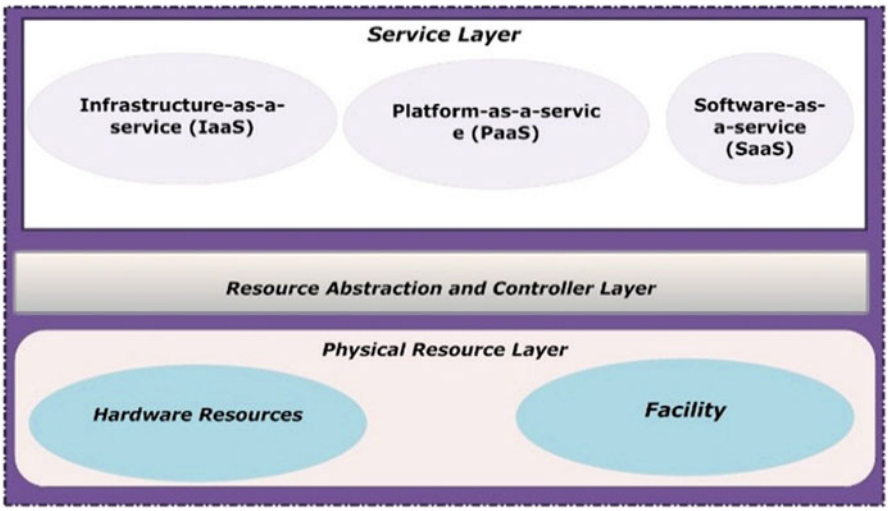


**Fig. 1.3** Cloud provider—three-layer service orchestration model

NIST provides a three-layer service orchestration model as shown in Fig. 1.3. The *physical resource layer* includes all the physical computing resources: computers (CPU and memory), networks (routers, firewalls, switches, network links, and interfaces), storage components (hard disks), and other physical computing infrastructure elements. The *resource abstraction and control layer* contains the system components that cloud providers use to provide and manage access to the physical computing resources through software abstraction (virtualization layer). The resource abstraction components include software elements such as hypervisors, virtual machines, virtual data storage, and other computing resource abstractions. The control aspect of this layer refers to the software components that are responsible for resource allocation, access control, and usage monitoring. The *service layer* contains interfaces for cloud consumers to access the computing services.

### 1.2.4 Virtualization

Virtualization is a key technology for cloud computing, SDN, and NFV. The technology enables network functions virtualization and software-defined network the ability to create a scalable, dynamic, and automated programmable virtual network functions and virtual network infrastructures in integrated cloud platforms such as telecom clouds. Virtualization is the technology that simulates the interface to a physical object by *multiplexing*, *aggregation*, or *emulation*. It is a process that translates hardware into emulated software-based copies. The virtualization simulates the interface to a physical object by several means: with multiplexing,

it creates multiple virtual objects from an instance of a physical object; with aggregation, it creates one virtual object from multiple physical objects; and with emulation, it constructs a virtual object from a different type of physical object [16].

On another level, virtualization can be defined as the logical abstraction of assets, such as the hardware platform, operating system (OS), storage devices, network, services, or programming interfaces. More commonly, virtualization is introduced as a software abstraction layer placed between an operating system and the underlying hardware (computing, network, and storage) in the form of a hypervisor. A hypervisor is a small and specialized operating system that runs on a physical server (host machine), allowing physical resources to be partitioned and provisioned as virtual resources (virtual CPU, virtual memory, virtual storage, and virtual networks). On computing resources, a hypervisor creates and manages virtual machines which are isolated instances of the application software and guest OS that run like separate computers. A virtual machine (VM) encapsulates the virtual hardware, the virtual disks, and the metadata associated with the application. In cloud data centers, since the hypervisor manages the hardware resources, multiple virtual machines each with its own operating system and applications and network services can run in parallel in a single hardware device [25]. Figure 1.4 illustrates the virtualization of virtual machines.

Virtualization allows elastic and scalable resource provisioning and sharing among multiple users. The technology allows multi-tenancy in clouds through isolation mechanism and enables each cloud tenant to perform its own services, applications, operating systems, and even network configuration in a logical environment without concerns over the same underlying physical infrastructure. Virtualization results in better server utilization and server/data center consolidation (multiple VMs run within a physical server) and workload isolation (each application on a physical server has its own separate VM).

Virtualization technology has been deployed by enterprises in data centers storage virtualization (NAS (network-attached storage), SAN (storage area network)),

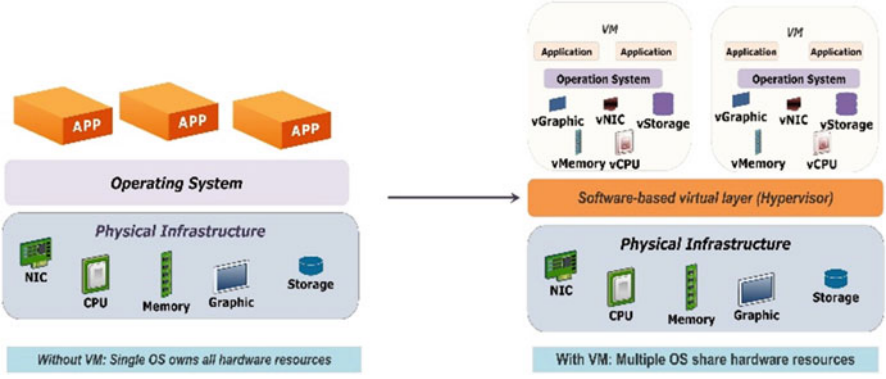


**Fig. 1.4** Virtual machines virtualization

database), OS virtualization (VMware, Xen), software or application virtualization (Apache Tomcat, JBoss, Oracle App Server, Web Sphere), and network virtualization [35].

## 1.3 Security Challenges of NFV, SDN, and Cloud

This section summarizes concepts that are pertinent to our discussion on security issues of SDN, NFV, and cloud. It summarizes their current security challenges.

### 1.3.1 General Security Requirements and Definitions

For securing an entity/system, it is widely accepted that five essential security functions are required: confidentiality, integrity, availability, authenticity, and accountability (CIAAA). Confidentiality ensures that private and confidential information about data or individuals is not disclosed to unauthorized users. Integrity ensures that information and intended system operation are not tampered with inadvertently or deliberately by unauthorized users. Availability ensures that systems and services are not denied to unauthorized users. Authenticity ensures that users can be verified and trusted as who they claim they are and that inputs arriving at the system came from a trusted source. Accountability generates the requirement for actions of an entity to be traced uniquely to that entity [30].

A system, an organization, or a cyberspace consists of three key elements: *real and virtual entities*, an *interconnecting infrastructure*, and *interactions among entities through the infrastructure*. Real and virtual entities include real things of physical devices such as human beings, computers, sensors, mobile phones, electronic devices, and virtual abstraction of entities such as data/information, software, and services. Infrastructure includes networks, databases, information systems, and storage that interconnect and support entities in the system/space. Interaction encompasses activities and interdependencies among system/cyberspace entities via the interconnecting infrastructure and the information within concerning communication, policy, business, and management [15]. Information or cybersecurity can be considered systems, tools, processes, practices, concepts, and strategies to prevent and protect the cyberspace from unauthorized interaction by agents with elements of the space to maintain and preserve the confidentiality, integrity, availability, and other properties of the space and its protected resources [15].

Essentially, cybersecurity is concerned with identifying vulnerabilities of cyberspace, assessing the risk associated with threats that exploit the vulnerability, and providing security solutions. A security vulnerability is a weakness in a system (component/product/system/cyberspace) that could allow an attacker to compromise the confidentiality, integrity, availability, authenticity, or accountability of that system. Threats and risks are closely related, but they are not equivalent. A threat is any entity, action, or condition that results in harm, loss, damage, and/or a deterioration of existing conditions. The risk associated with a threat is a

characteristic that embraces three components: *the impact or importance of a threat incident*, *the likelihood or potential of a future threat incident*, and *the potential loss due to a threat incident*. Evaluating the risk associated with a threat provides the impetus for going forward with security solutions and the requirements for those solutions [36].

### 1.3.2 NFV Security Challenges

Because network components are virtualized, NFV networks contain a level of abstraction that does not appear in traditional networks. Securing this complex and dynamic environment, that encompasses the virtual/physical resources, the controls/protocols, and the boundaries between the virtual and physical networks, is challenging for many reasons according to CSA [18]:

- *Hypervisor dependencies* Hypervisors are available from many vendors. They must address security vulnerabilities in their software. Understanding the underlying architecture, deploying appropriate types of encryption, and applying patching diligently are all critical for the security of the hypervisors.
- *Elastic network boundaries* In NFV, the network fabric accommodates multiple functions. Physical and virtual boundaries are blurred or nonexistent in NFV architecture, which makes it difficult the design of security systems.
- *Dynamic workloads* While NFV is about agility and dynamic capabilities, traditional security models are static and unable to evolve as network topology changes in response to demand.
- *Service insertion* NFV promises elastic, transparent networks since the fabric intelligently routes packets that meet configurable criteria. Traditional security controls are deployed logically and physically in-line. With NFV, there is often no simple insertion point for security services that are not already layered into the hypervisor.
- *Stateful versus stateless inspection* Security operations during the last decade have been based on the premise that stateful inspection is more advanced and superior to stateless access controls. NFV may add complexity where security controls cannot deal with the asymmetry flows created by multiple, redundant network paths and devices.
- *Scalability of available resources* Deeper inspection technologies—next-generation firewalls and Transport Layer Security decryption, for example—are resource intensive and do not always scale without offload capability.

The ETSI Security Expert Group focuses on the security of the software architecture. It identified potential security vulnerabilities of NFV and established whether they are new problems or just existing problems in different guises [32]. The identified new security concerns resulting from NFV are as shown in Table 1.1.