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