WORLD ACADEMIC FRONTIERS
世界学术研究前沿丛书

Computer Network Security

计算机网络安全

“世界学术研究前沿丛书”编委会
THE EDITORIAL BOARD OF
WORLD ACADEMIC FRONTIERS

世界图书出版公司

WORLD ACADEMIC FRONTIERS
世界学术研究前沿丛书

Computer Network Security

计算机网络安全

“世界学术研究前沿丛书”编委会
THE EDITORIAL BOARD OF
WORLD ACADEMIC FRONTIERS

中国出版集团公司
世界图书出版公司
广州·上海·西安·北京

图书在版编目（CIP）数据

计算机网络安全：英文 / “世界学术研究前沿丛书”编委会编. —广州：世界图书出版广东有限公司，2017.8
ISBN 978-7-5192-2462-2

Ⅰ. ①计… Ⅱ. ①世… Ⅲ. ①计算机网络－网络安全－英文 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2017)第 040988 号

书　　名：计算机网络安全
Jisuanji Wangluo Anquan
编　　者：“世界学术研究前沿丛书”编委会
责任编辑：康琬娟
出版发行：世界图书出版广东有限公司
地　　址：广州市海珠区新港西路大江冲25号
邮　　编：510300
电　　话：（020）84460408
网　　址：http：//www.gdst.com.cn/
邮　　箱：wpc_gdst@163.com
经　　销：新华书店
印　　刷：广州市德佳彩色印刷有限公司
开　　本：787 mm×1092 mm　1/16
印　　张：55.75
插　　页：4
字　　数：1060千
版　　次：2017年8月第1版　　2017年8月第1次印刷
国际书号：ISBN 978-7-5192-2462-2
定　　价：598.00元

Preface

Computer network security consists of the policies adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done.[1]

In the present book, thirty literatures about computer network security published on international authoritative journals were selected to introduce the worldwide newest progress, which contains reviews or original researches on network security, cloud computing, wireless sensor network, network confidentiality and so on. We hope this book can demonstrate advances in computer network security as well as give references to the researchers, students and other related people.

March 9, 2017

[1]From Wikipedia: https://en.wikipedia.org/wiki/Network_security.

Selected Authors

Christian Senk, University of Regensburg, Regensburg, Germany.

Kristin Glass, Systems Analysis, New Mexico Institute of Mining and Technology, Socorro, USA.

Alvaro Araujo, Electronic Engineering Department, Universidad Politécnica de Madrid, Avda/Complutense 30, Madrid, Spain.

Roland Schwarzkopf, Department of Mathematics and Computer Science, University of Marburg, Hans-Meerwein-Str. 3, D-35032 Marburg, Germany.

Thomas E. Carroll, Pacific Northwest National Laboratory, P.O. Box 999, Richland, Washington, USA.

Paul Ormerod, Software Development, University College London, London, UK.

David M. Laverty, School of Electronics, Electrical Engineering and Computer Science, Queen's University Belfast, 125 Stransmillis Road, Belfast BT9 5AH, UK.

Jingwei Huang, Information Trust Institute, University of Illinois at Urbana-Champaign 1308 West Main Street, Urbana, Illinois 61801, USA.

Paul Watson, School of Computing Science, Newcastle University, Newcastle-upon-Tyne, UK.

Geumhwan Cho, Department of Computer Science and Engineering, Sungkyunkwan University, Seobu-ro 2066, Suwon, Republic of Korea.

Contents

Chapter 1

Virtual Network Security: Threats, Countermeasures, and Challenges

Leonardo Richter Bays[1], Rodrigo Ruas Oliveira[1], Marinho Pilla Barcellos[1], Luciano Paschoal Gaspary[1], Edmundo Roberto Mauro Madeira[2]

[1]Institute of Informatics, Federal University of Rio Grande do Sul, Porto Alegre, Brazil
[2]Institute of Computing, University of Campinas, Campinas, Brazil

Abstract: Network virtualization has become increasingly prominent in recent years. It enables the creation of network infrastructures that are specifically tailored to the needs of distinct network applications and supports the instantiation of favorable environments for the development and evaluation of new architectures and protocols. Despite the wide applicability of network virtualization, the shared use of routing devices and communication channels leads to a series of security-related concerns. It is necessary to provide protection to virtual network infrastructures in order to enable their use in real, large scale environments. In this paper, we present an overview of the state of the art concerning virtual network security. We discuss the main challenges related to this kind of environment, some of the major threats, as well as solutions proposed in the literature that aim to deal with different security aspects.

Keywords: Network Virtualization, Security, Threats, Countermeasures

1. Introduction

Virtualization is a well established concept, with applications spanning several areas of computing. This technique enables the creation of multiple virtual platforms over a single physical infrastructure, allowing heterogeneous architectures to run on the same hardware. Additionally, it may be used to optimize the usage of physical resources, as an administrator is able to dynamically instantiate and remove virtual nodes in order to satisfy varying levels of demand.

In recent years, there has been a growing demand for adaptive network services with increasingly distinct requirements. Driven by such demands, and stimulated by the successful employment of virtualization for hosting custom-built servers, researchers have started to explore the use of this technique in network infrastructures. Network virtualization allows the creation of multiple independent virtual network instances on top of a single physical substrate[1]. This is made possible by instantiating one or more virtual routers on physical devices and establishing virtual links between these routers, forming topologies that are not limited by the structure of the physical network.

In addition to the ability to create different topological structures, virtual networks are also not bound by other characteristics of the physical network, such as its protocol stack. Thus, it is possible to instantiate virtual network infrastructures that are specifically tailored to the needs of different network applications[2]. These features also enable the creation of virtual testbeds that are similar to real infrastructures, a valuable asset for evaluating newly developed architectures and protocols without interfering with production traffic. [3]For these reasons, network virtualization has attracted the interest of a number of researchers worldwide, especially in the context of Future Internet research. Network virtualization has been embraced by the Industry as well. Major Industry players—such as Cisco and Juniper—nowadays offer devices that support virtualization, and this new functionality allowed infrastructure providers to offer new services.

In contrast to the benefits brought by network virtualization, the shared use of routing devices and communication channels introduces a series of security-related concerns. Without adequate protection, users from a virtual network might be able to access or even interfere with traffic that belongs to other virtual net-

works, violating security properties such as confidentiality and integrity[4][5]. Additionally, the infrastructure could be a target for denial of service attacks, causing availability issues for virtual networks instantiated on top of it[6][7]. Therefore, it is of great importance that network virtualization architectures offer protection against these and other types of threats that might compromise security.

Recently, attention has been drawn to security concerns in network infrastructures due to the discovery of pervasive electronic surveillance around the globe. Although all kinds of networks are potentially affected, the shared use of physical resources in virtual network environments exacerbates these concerns. As such, these recent circumstances highlight the need for a comprehensive analysis of current developments in the area of virtual network security.

In this paper, we characterize the current state of the art regarding security in network virtualization. We identify the main threats to network virtualization environments, as well as efforts aiming to secure such environments. For this study, an extensive literature search has been conducted. Major publications from the literature have been studied and grouped according to well known classifications in the area of network security, as well as subcategories proposed by the authors of this paper. This organization allows the analysis and discussion of multiple aspects of virtual network security.

The remainder of this paper is organized as follows. Section 2 presents a brief background on the area of network virtualization as well as a review of related literature. Section 3 introduces the taxonomy used to classify the selected publications. Section 4 exposes the security vulnerabilities and threats found in the literature, while Section 5 presents the security countermeasures provided by solutions found in previous proposals. In Section 6, we discuss the results of this study, and in Section 7 we summarize the main current research challenges in the area of virtual network security. Last, in Section 8 we present our conclusions.

2. Background and Literature Review

In this section, we first provide a brief background on the area of network virtualization, highlighting its most relevant concepts. Next, we present a review of literature closely related to virtual network security.

2.1. Background

Network virtualization consists of sharing resources from physical network devices (routers, switches, etc.) among different virtual networks. It allows the coexistence of multiple, possibly heterogeneous networks, on top of a single physical infrastructure. The basic elements of a network virtualization environment are shown in **Figure 1**. At the physical network level, a number of autonomous systems are represented by interconnected network substrates (e.g., substrates A, B, and C). Physical network devices are represented by nodes supporting virtualization technologies. Virtual network topologies (e.g., virtual networks 1 and 2), in turn, are mapped to a subset of nodes from one or more substrates. These topologies are composed of virtual routers, which use a portion of the resources available in physical ones, and virtual links, which are mapped to physical paths composed of one or more physical links and their respective intermediate routers.

From the point of view of a virtual network, virtual routers and links are seen as dedicated physical devices. However, in practice, they share physical resources with routers and links from other virtual networks. For this reason, the virtualization technology used to create this environment must provide an adequate level of isolation in order to enable the use of network virtualization in real, large scale environments.

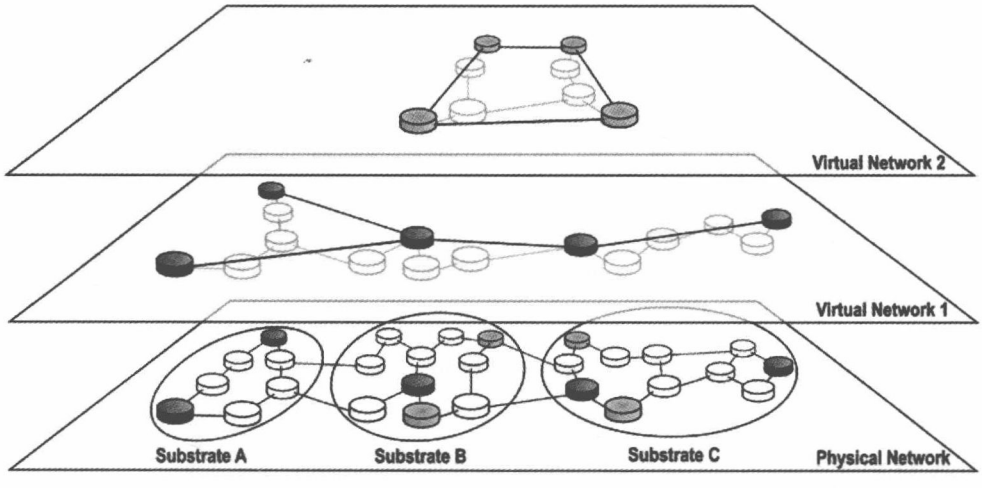

Figure 1. Network virtualizationmodel, denoting a scenario with multiple physical substrates (Substrate A, B, and C) and virtual networks (Virtual Network 1 and 2).

Over the years, different methods for instantiating virtual networks have been used. Typical approaches include VLANs (Virtual Local Area Networks) and VPNs (Virtual Private Networks). Recently, Virtual Machine Monitors and programmable networks have been employed to create virtual routers and links over physical devices and communication channels. These approaches are briefly revisited next.

2.1.1. Protocol-Based Approaches

Protocol-based approaches consist of implementing a network protocol that enables the distinction of virtual networks through techniques such as tagging or tunneling. The only requirement of this kind of approach is that physical devices (or a subset of them) support the selected protocol.

One example of protocol-based network virtualization are VLANs. VLANs consist of logical partitions of a single underlying network. Devices in a VLAN communicate with each other as if they were on the same Local Area Network, regardless of physical location or connectivity. All frames sent through a network are tagged with their corresponding VLAN ID, processed by VLAN-enabled routers and forwarded as necessary[8]. Since isolation is typically based only on packet tagging, this approach is susceptible to eavesdropping attacks.

Another commonly used approach is the creation of Virtual Private Networks. VPNs are typically used to provide a secure communication channel between geographically distributed nodes. Cryptographic tunneling protocols enable data confidentiality and user authentication, providing a higher level of security in comparison with VLANs. VPNs can be provided in the physical, data link, or network layers according to the protocols being employed[9].

2.1.2. Machine Virtualization-Based Approaches

Machine virtualization-based approaches consist of creating virtual networks by means of groups of interconnected virtual machines. Virtual Machine Monitors are used to instantiate virtual routers, and virtual links are established between them, regardless of physical network topology. **Table 1** shows different

Table 1. Virtualization techniques.

Technique	Description	Examples
Full virtualization	The Virtual Machine Monitor emulates a complete machine, based on the underlying hardware architecture. The guest Operating System runs without any modification.	VMware Workstation, VirtualBox
Paravirtualization	The Virtual Machine monitor emulates a machine which is similar to the underlying hardware, with the addition of a hypervisor. The hypervisor allows the guest Operating System to run complex tasks directly on non-virtualized hardware. The guest OS must be modified in order to take advantage of this feature.	VMware ESX, Xen
Container-based virtualization	Instead of running a full Virtual Machine, this technique provides Operating System-level containers, based on separate userspaces. In each container, the hardware, as well as the Operating System and its kernel, are identical to the underlying ones.	OpenVZ, Linux VServer

machine virtualization-based techniques that can be used to create virtual networks, as well as a brief explanation and an example of each.

This alternative is remarkably flexible and relatively cheap, as it allows the use of customized software and does not require the use of specific hardware[1]. However, it is more demanding in terms of resource usage in comparison to previously described protocol-based approaches. Additionally, it may introduce security concerns associated with server virtualization, some of which are mentioned in Sections 4 and 5. A general study on the security issues that arise from the use of machine virtualization was performed by van Cleeff *et al.*[10].

2.1.3. Programmable Networks

Programmable routers have been used to enable the creation of virtual networks. Although this is not a new concept, research in this area has been recently stimulated by the inception of Software-Defined Networking (SDN). This paradigm consists of decoupling the data plane and the control plane in network devices. More specifically, devices such as routers and links retain only the data plane, and a separated control plane manages such devices based on an overview of the entire network.

OpenFlow[11], one of the most promising techniques for implementing this paradigm, defines a protocol that allows a centralized controller to act as the control plane, managing the behavior of network devices in a dynamic manner. The controller communicates with network devices through a secure connection, creating and managing flow rules. Flow rules instruct network devices on how to properly process and route network traffics with distinct characteristics. Through

the establishment of specific flow rules, it is possible to logically partition physical networks and achieve data plane isolation. This isolation enables the creation of virtual networks on top of an SDN environment. OpenFlow gave rise to the Open Networking Foundation, an organization ran by major companies within the area of computer networks that aims to disseminate this type of technology.

2.2. Literature Review

To the best of our knowledge, there have been no previous attempts at characterizing the state of the art regarding security in network virtualization. However, there have been a number of similar studies in other, closely related fields of research. We now proceed to a review of some of the main such studies.

Chowdhury *et al.*[1] provide a general survey in the area of network virtualization. The authors analyze the main projects in this area (both past projects and, at the time of publication, current ones) and discuss a number of key directions for future research. The authors touch upon the issues of security and privacy both while reviewing projects and discussing open challenges; however, as this is not the main focus of this survey, there is no in-depth analysis of security issues found in the literature.

Bari *et al.*[12] present a survey that focuses on data center network virtualization. Similarly to the aforementioned study, the authors survey a number of key projects and discuss potential directions for future work. When analyzing such projects, the authors provide insights on the fault-tolerance capabilities of each one, in addition to a brief discussion on security issues as one of the potential opportunities for future research.

In addition to the general studies on network virtualization presented so far, a number of surveys on cloud computing security have also been carried out. Cloud computing environments tend to make use of both machine and network virtualization, making this a highly relevant related topic for our study. However, while there is some overlap between cloud computing security and virtual network security, we emphasize that cloud computing represents a very specific use case of network virtualization and, therefore, poses a significantly distinct set of security challenges. Zhou *et al.*[13] provide an investigation on security and privacy issues