Computer Networks 104 (2016) 55–65

Contents lists available at ScienceDirect

Computer Networks

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

Towards a secured network virtualization

Yang Wang [a,*], Phanvu Chau [a], Fuyu Chen [b]

[a] Department of Math and Computer Science, La Salle University, PA, 19141, United States
[b] Department of Electrical Engineering, SUNY, University at Buffalo, NY, 14260, United States

ARTICLE INFO

Article history:
Received 18 September 2015
Revised 10 March 2016
Accepted 29 April 2016
Available online 6 May 2016

Keywords:
SVNE
Security-awareness
Network Virtualization

ABSTRACT

Network virtualization promises to fulfill the demand for an agile Internet that is friendly to technological innovation. In the past, tremendous efforts have been dedicated to studying the fundamental problem in network virtualization, namely Virtual Network Embedding (VNE). However, until recently, very limited work has addressed the security issues and implications of VNE or network virtualization as a whole, despite their importance. On one hand, the literature lacks a systematic overview of security issues in network virtualization (e.g., which can be VNE-relevant or VNE-irrelevant). On the other hand, existing studies on security-aware VNE share common limitations. This paper aims to present a timely study to fill the above needs with the following contributions: First, we present a classified comprehensive overview of security issues that arise in the context of network virtualization based on multiple criteria. Second, based on the review of existing approaches in Security-aware Virtual Network Embedding (SVNE), a novel framework is presented to address VNE-relevant security issues in network virtualization. Third, our extensive evaluation uncovers a few important implications and shows that the proposed framework can address the SVNE problem with reduced time (compared to that of the regular VNE approach).

1. Introduction

Network virtualization introduces a logical layer of abstraction to allow for a flexible and agile deployment of revolutionary technologies, which is considered a promising solution to address the Internet impasse [1–9]. In network virtualization, service provision is decoupled into two phases: logical representation, in which a service is expressed as a virtual network; and physical mapping, which instantiates each virtual network. These two phases are separately maintained by the Service Provider (SP) and the Infrastructure Provider (InP), respectively. Given the freedom of independent technology decisions by both parties, the inherence resistance (of the current Internet) to technological revolutions is removed in network virtualization. This separation, however, calls for a holistic bridging process that projects the logical network onto the physical network, which is referred to as the *Virtual Network Embedding* (VNE) problem.

Fundamentally, network virtualization builds upon node virtualization (e.g., Xen [10]) in combination with link virtualization (e.g., OpenFlow [11]). As a result, the VNE process contains two corresponding modules: node assignment, and link mapping, respectively. The former decides the physical host for each virtual node (by the creation of virtual machine instance), while the latter allocates bandwidth along substrate paths to connect instances of virtual nodes. Given the NP-Completeness of the VNE problem [12], existing approaches can be classified into three categories: *(i)* Optimal solutions based on Integer Linear Programming (ILP) formulations (e.g., link-based ILP model in [13] and path-based model in [6]); *(ii)* Relaxation approaches based on the LP-relaxation of the ILP formulations (e.g., relaxation and rounding in [13], and decomposition approach in [14]); and *(iii)* Heuristic or meta-heuristic algorithms (e.g., [15]).

Given the essence of *virtualization*, outsourcing computation, storage, content, and network to the third party (i.e., InPs) gives rise to inherent Confidentiality, Integrity and Availability (C.I.A) vulnerabilities [16,17]. As a result, security plays a critical rule in network virtualization. Despite the extensive studies in network virtualization (particulary in VNE), only limited work, however, has addressed the resulting security issues and implications [7–9,18,19]. On one hand, the existing literature lacks a systematic overview of security issues in network virtualization. Note that although it is commonly believed that security factors should be integrated into the VNE process to ensure a robust mapping [1], not all of them should or can be addressed in the VNE process. On the other hand, as to be further discussed, existing studies on security-aware VNE share a few limitations. First, they only address particular aspects of security, e.g., support for data integrity with encryption in [7]. Second, the security requirements (e.g., the

* Corresponding author.
E-mail address: wang@lasalle.edu (Y. Wang).

http://dx.doi.org/10.1016/j.comnet.2016.04.023
1389-1286/

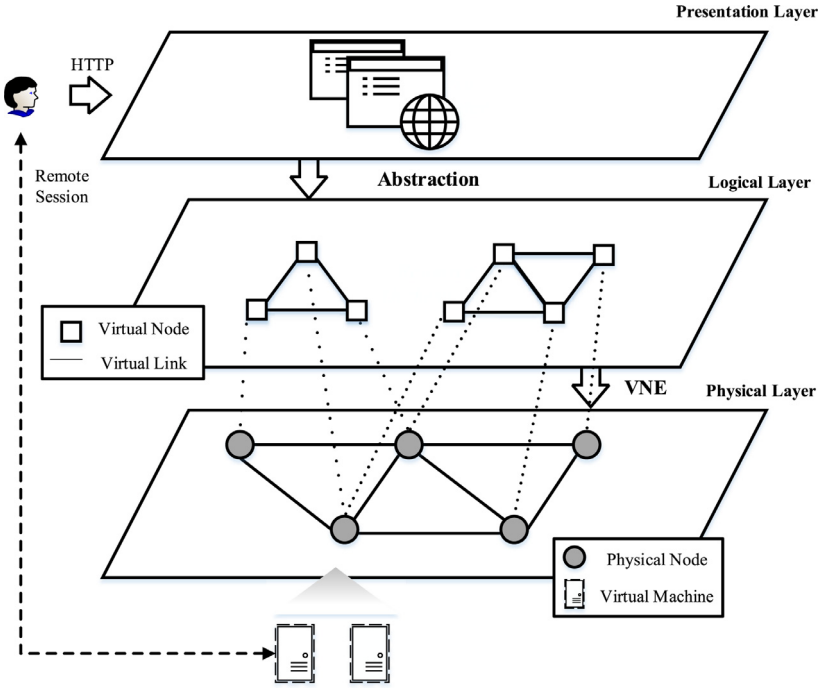

Fig. 1. Three-layer architecture of network virtualization.

security level [8]) are not explicitly defined in an *Open Design* [20] format that can be interpreted by SPs/end users and implemented by the InPs. In this work, we aim to present a timely study to fill the above gaps. We present a classified overview of security issues that arise in the context of network virtualization according to various criteria and hierarchies. Based on the discussion of existing approaches in Security-aware Virtual Network Embedding (SVNE), we propose a new SVNE approach that employs flexible and fine-granular security plans.

The remainder of this work is organized as follows. In Section 2, we overview security issues in network virtualization, which are classified according to multiple criteria such as their VNE-relevance. In Section 3, we define the SVNE problem, and present security plans that can be incorporated in the SVNE problem. In Section 4, we present a security framework that addresses the VNE-relevant security issues by resolving the SVNE problem. Section 5 presents the evaluation of the proposed framework. We discuss other security issues in Section 6, and conclude this work in Section 7.

2. A classified overview of security issues in network virtualization

In this section, we present a classified overview of security issues in network virtualization depending on various criteria including: holistic view from the layer perspective, end users's view, InPs' view, and VNE-relevance.

2.1. Layer perspective: holistic view

In network virtualization, the traditional ISP is decomposed into two new parties: the Service Provider and the Infrastructure Provider. The former offers end-to-end logical services to the end user, while the latter physically deploys and manages the substrate network infrastructure. From the security perspective, we view network virtualization as a three layer architecture as shown in Fig. 1. The *Presentation Layer* provides interfaces (e.g, Web, RESTful API) to end users in which the service feature can be specified. Each service request is abstracted as a virtual network at the *Logical Layer* that consists of virtual nodes and virtual links. Finally, each virtual network is instantiated at the substrate network of the *Physical Layer* via the VNE process.

Depending on the layer where the attack is originated, we can classify the attacks in network virtualization as in Table 1. At the physical layer, when virtual instances co-reside at the same physical host, the shared hypervisor or hardware can be exploited to construct cross-virtual-machine attacks [17,21]. Likewise, classic physical attacks and Denial of Service attacks can also lead to service disruption of the hosted instances [23–25]. At the logical layer, attackers can masquerade as a SP to probe the topology and determine the locations as well as attributes of possible victim instances in the physical network [18]. At the presentation layer, a web-based interface can be exploited with classic SQL injection, and Cross-Site Scripting attacks [17,22]. It is worth noting that the work flow (e.g., VNE process), control flow (e.g., remote access session), and data flow (e.g., computation results) among layers could be hijacked by attacks such as *man-in-the-middle*. In addition, InPs may not deliver the agreed computing/bandwidth resources to the subscriber, which could be hard to verify in scenarios such as Big Data Computation [26].

2.2. Service goals: end users' view

We next look at the security issues from the end users' viewpoint by answering an important question: what do general security goals specifically entail in network virtualization? This leads to a classification shown in Table 2 based on the goals of C.I.A and Assurance. Different from classic network environment, network virtualization implies the outsourcing of data/computation to the third-party away from the end users. The *Confidentiality/Integrity* of user data/computation should prevent access/modification from un-authorized parties including the InPs, and SPs. The *Availability* and *Assurance* goals require the InPs/SPs to deliver the service in an uninterrupted manner, and with the agreed resources, respectively. Given the hosting vantage of SPs, it is challenging to achieve