

# **Sicherheitsaspekte bei Deployment virtueller Netzwerkinfrastrukturen**

Gerhard Gröschl, Miran Mizani  
{gerhard.groeschl, miran.mizani}@campus.lmu.de

Seminar: Trends in Mobilen und Verteilten Systemen  
Wintersemester 2016/2017

Lehrstuhl für Mobile und Verteilte Systeme  
Institut für Informatik  
Ludwig-Maximilians-Universität München

Betreuer: Michael T. Beck  
*eingereicht am 18. Dezember 2016*

**Abstract:** Durch die äußerst effiziente Nutzung von Hardware mittels Virtualisierung steigt die Nachfrage nach virtualisierten Infrastrukturen enorm. Serviceprovider müssen die Hardwarebasis für ihre Dienste nicht mehr selbst unterhalten und geben ihre dahingehende Verantwortung an Infrastrukturanbieter weiter. Um die Sicherheit dieser Strukturen nicht zu vernachlässigen, arbeiten viele Forscher in diesem Bereich und versuchen effiziente Algorithmen mit integrierter Beachtung der Sicherheitsaspekte zu finden. Diese Arbeit soll einen Überblick und eine Klassifizierung der Gefahren, die solche Konstrukte betreffen, sowie eine Analyse zweier unterschiedlicher Ansätze zur Vermeidung möglichst vieler Risiken zum Zeitpunkt der Planung übermitteln.

## **Inhaltsverzeichnis**

<b>1</b>	<b>Einleitung</b>	<b>3</b>
<b>2</b>	<b>Sicherheitsaspekte bei virtuellen Netzwerk-Infrastrukturen</b>	<b>3</b>
2.1	Herkömmliche Gefahren . . . . .	3
2.2	Spezielle Gefahren bei virtualisierten Umgebungen . . . . .	3
2.3	VNE-Relevante Gefahren . . . . .	3
<b>3</b>	<b>Vermeidung von Gefahren via Secure VNE</b>	<b>3</b>
3.1	Modell 1 . . . . .	5
3.2	Modell 2 . . . . .	5
3.3	Vergleich . . . . .	5
<b>4</b>	<b>Ungelöste Probleme</b>	<b>5</b>
<b>5</b>	<b>Schlussfolgerung und Ausblick</b>	<b>5</b>

## 1 Einleitung

## 2 Sicherheitsaspekte bei virtuellen Netzwerk-Infrastrukturen

### 2.1 Herkömmliche Gefahren

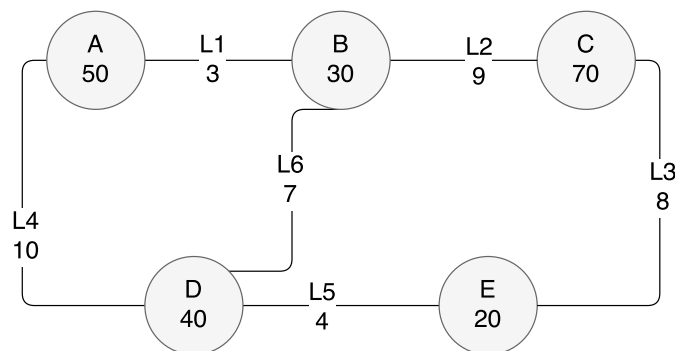
### 2.2 Spezielle Gefahren bei virtualisierten Umgebungen

### 2.3 VNE-Relevante Gefahren

## 3 Vermeidung von Gefahren via Secure VNE

Um den Anforderungen der heutigen Gefahren zu genügen, ist es unumgänglich sämtliche Grundsätze der IT-Sicherheit möglichst früh in die Planung der gewünschten Infrastruktur miteinzubeziehen. Nicht nur, weil das nachträgliche Schließen von Sicherheitslücken und Hinzufügen von Sicherheitskomponenten in finanzieller und zeitlicher Hinsicht zehnmal so teuer ist wie die initiale Beachtung dieser Aspekte, sondern weil die vollständige Sicherheit eines nachgerüsteten Systems kaum gewährleistet werden kann [Col11]. „Security-by-Design“ ist einer der wichtigsten Begriffe bei der Planung öffentlich zugänglicher Netzwerkstrukturen. Dementsprechend groß ist die Nachfrage nach VNE-Algorithmen, die bereits beim Prozess des Mappings möglichst viele Sicherheitsaspekte beachten und abdecken. Die vorausgehende Klassifizierung der bekannten Gefahren in „VNE-relevant“ und „nicht-VNE-relevant“ bildet die Grundlage für unsere weiteren Untersuchungen. Um zuvor noch einen genaueren Einblick in die Problematik von VNE zu gewähren, beginnen wir zunächst mit der Erläuterung des VNE-Problems sowie einem Überblick über die verschiedenen erfolgreichen Strategien bestehender VNE-Algorithmen, welche die Sicherheitsaspekte noch nicht beachten.

Betrachtet man das zugrundeliegende physische System als einen ungerichteten Graphen



und extrahiert die vorhandenen Elemente sowie deren Werte, erhält man die Basismenge

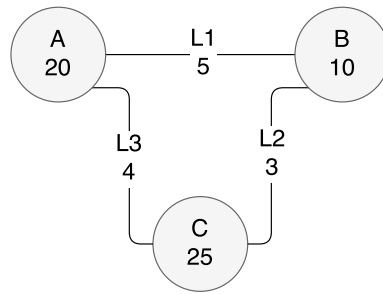
$$G^S = \{N^S, L^S\}$$

(N steht für die Menge der physischen Knoten, L für die Menge der physischen Links)

$$G^S = \{ \{ (A^S, 50), (B^S, 30), (C^S, 70), (D^S, 40), (E^S, 20) \}, \\ \{ (L1^S, 3), (L2^S, 9), (L3^S, 8), (L4^S, 10), (L5^S, 4), (L6^S, 7) \} \}$$

in welche die virtuellen Strukturen eingebettet werden sollen.

Ein „virtual network request“ (in Folge „VNR“ genannt) kann hierbei ebenfalls als ein ungerichteter Graph gesehen



und genauso in eine Menge übersetzt werden.

$$G^V = \{N^V, L^V\}$$

(N steht für die Menge der virtuellen Knoten, L für die Menge der virtuellen Links)

$$G^V = \{ \{ (A^V, 20), (B^V, 10), (C^V, 25) \}, \{ (L1^V, 5), (L2^V, 3), (L3^V, 4) \} \}$$

Gesucht ist nun eine Abbildungsfunktion  $f : G^V \rightarrow G^S$

In der Regel ist es üblich, nicht nur eine einzelne VNRs auf ein physisches System abzubilden, sondern gleich mehrere auf einmal. Ebenso wäre es theoretisch möglich, dass ein Infrastruktur-Provider gleich mehrere getrennte unabhängige physische Strukturen betreibt, und somit mittels VNE das beste System für die Abbildung der Menge von VNRs eroiren möchte. Dies könnte beispielsweise der Fall sein, wenn ein Serviceprovider ein VNR mit der Bedingung „alle Elemente mögen sich am selben Standort befinden, egal

an welchem“ in Auftrag gibt, und der Infrastruktur-Provider über mehrere Hardware-Standorte verfügt.

Die Attributmenge bei den grundlegenden VNE-Algorithmen beschränkt sich zumeist auf Rechnerleistung und Bandbreite. Lokalität, GPU-Leistung und RAM-Menge wären einige weitere mögliche Standard-Attribute. Ein großes Problem bei der Berechnung des optimalen Mappings findet sich bei der Berechnungszeit. Die endliche Beschränkung der Knoten- sowie Link-Ressourcen und die „on-line nature“ von VNRs stellen zusätzliche Hindernisse dar. Da selbst Lösungen für einfache Anfragen (geringe Anzahl von Knoten und Links), welche wenige Attribute beinhalten, exponentiellen Rechenaufwand benötigen, steigt der Aufwand sowohl mit der Anzahl der abzubildenden Knoten und Links, als auch mit steigender Attributanzahl dementsprechend. Teilweise gilt das Problem als rechnerisch unlösbar, grundsätzlich aber befinden wir uns im Komplexitätsbereich der NP-Vollständigkeit [MRR13]. Da die Erhöhung der Attributmenge - wie bereits genannt - grundsätzlich nicht positiv zur Laufzeit der existierenden Algorithmen beiträgt, werden wir den Komplexitätsbereich beim Hinzufügen von Sicherheitsanforderungen nicht verlassen. Dennoch gibt es Möglichkeiten, die den Rechenaufwand reduzieren können. Mit den folgenden beiden Modellen werden wir sowohl diese Möglichkeiten, als auch andere Vor- und Nach-Teile, genauer untersuchen.

### **3.1 Modell 1**

### **3.2 Modell 2**

### **3.3 Vergleich**

## **4 Ungelöste Probleme**

## **5 Schlussfolgerung und Ausblick**

Frage: Auf welcher Ebene wird virtualisiert? Auf IP-Ebene? Was ist dann aber mit IP-Support-Protokollen (ARP)? Oder nicht-IP-Protokollen? Will ich ein Netzwerk virtualisieren, oder nur den IP-Verkehr? Verkapselung führt zu Leistungseinbußen. [CDRS07]

## **Literatur**

[CDRS07] Serdar Cabuk, Chris I Dalton, HariGovind Ramasamy und Matthias Schunter. Towards automated provisioning of secure virtualized networks. In *Proceedings of the 14th ACM conference on Computer and communications security*, Seiten 235–245. ACM, 2007.

[Col11] Eric Cole. Network Security Bible: Edition 2, 2011.

- [MRR13] Raouf Boutaba Muntasir Raihan Rahman. Surviveable Virtual Network Embedding Algorithms for Network Virtualization, 2013.