Sicherheitsaspekte bei Deployment virtueller Netzwerkinfrastrukturen

Miran Mizani, Gerhard Gröschl

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

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

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.
Hier folgt eine kurze Zusammenfassung des Themas sowie der wichtigsten Erkenntnisse und Ergebnisse. Länge: ca. 200 Wörter.

1 Einleitung

Die Ausarbeitung zum Seminar soll dem Layout der *GI-Edition Lecture Notes in Informatics (LNI)* entsprechen. Die verwendete Literatur wird in der beiliegenden Datei `literatur.bib` verwaltet. Eine Referenz kann mittels des `\cite{}`–Kommandos eingefügt werden, z.B.

1.1 Hinweise für Abbildungen

Abbildungen müssen als `.pdf`, `.png`, oder `.jpg` eingebunden werden. Beispiel:

Abbildung 1: Das Logo der GI

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 10 mal 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 Strukturen. Dementsprechend groß ist die Nachfrage nach VNE-Algorithmen die bereits beim Prozess des Mappings möglichst viele Sicherheitsaspekte beachten und abdecken. Die folgenden zwei Algorithmen wurden ausgewählt, um dieses Feature zu untersuchen und zu beurteilen.

3.1 Algorithmus 1

3.2 Algorithmus 2

3.3 Vergleich

4 Ungelöste Probleme

5 Schlussfolgerung und Ausblick

Literatur

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