LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

Gerhard Gröschl, Miran Mizani

Sicherheitsaspekte beim Deployment virtueller Netzinfrastrukturen

Abschlusspräsentation im Bachelorseminar

„Trends in Mobilen und Verteilten Systemen“

München, Oettingenstr. 67, Raum 027

16. Februar 2017

Motivation

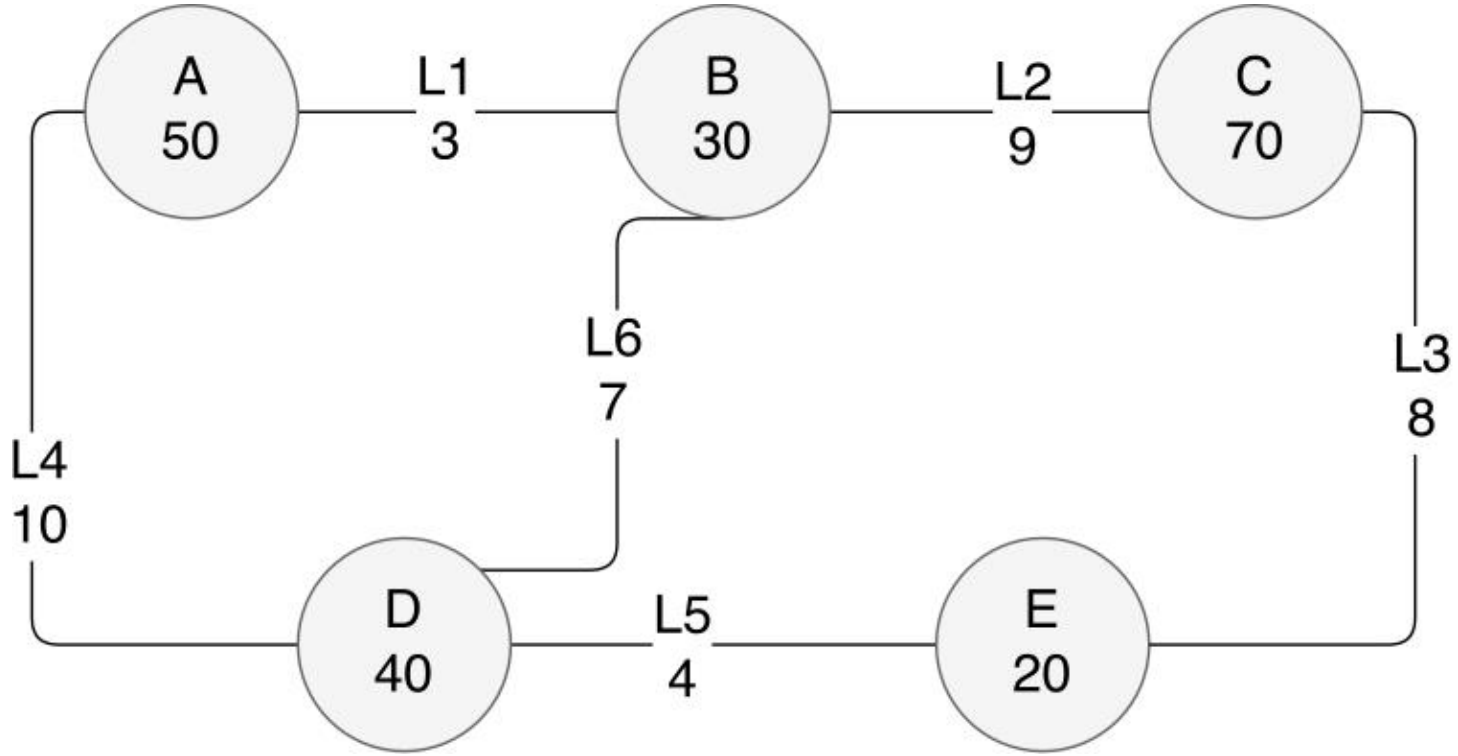
- Anforderungen an Netzstrukturen ändern sich häufig

- Netzvirtualisierung bietet Möglichkeit zur Abstraktion von der eingesetzten Hardware → Aufbau logischer Netze

Motivation

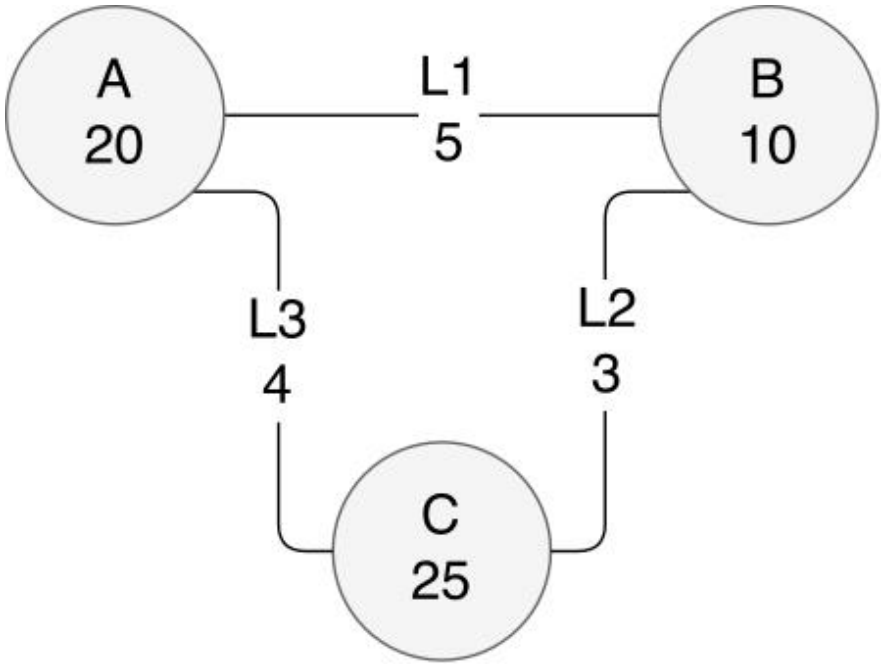
- Anforderungen an Netzstrukturen ändern sich häufig
- Netzvirtualisierung bietet Möglichkeit zur Abstraktion von der eingesetzten Hardware → Aufbau logischer Netze
- Virtual Network Embedding (VNE) bislang nur hinsichtlich Performance optimiert
- Sicherheitsaspekte meist außer Acht gelassen
  => Integration solcher in den VNE-Prozess (SecureVNE)

Virtual Network Embedding



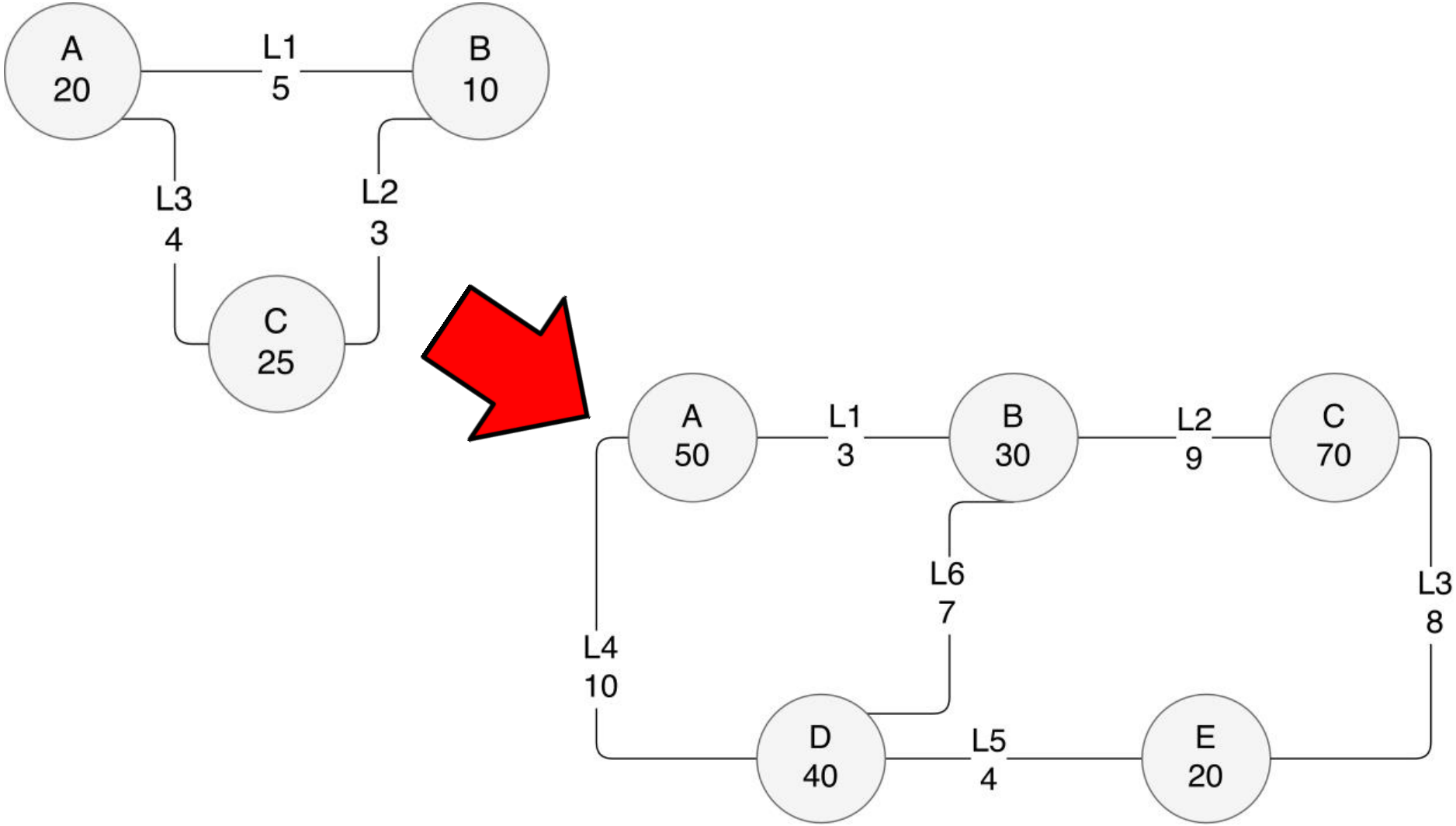
Substratnetz mit Quantifizierung von Merkmalen

Virtual Network Embedding



Virtual Network Request

Virtual Network Embedding



Virtual Network Embedding

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

Virtual Network Embedding

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

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

Virtual Network Embedding

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

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

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

Virtual Network Embedding

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

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

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

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

Virtual Network Embedding

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

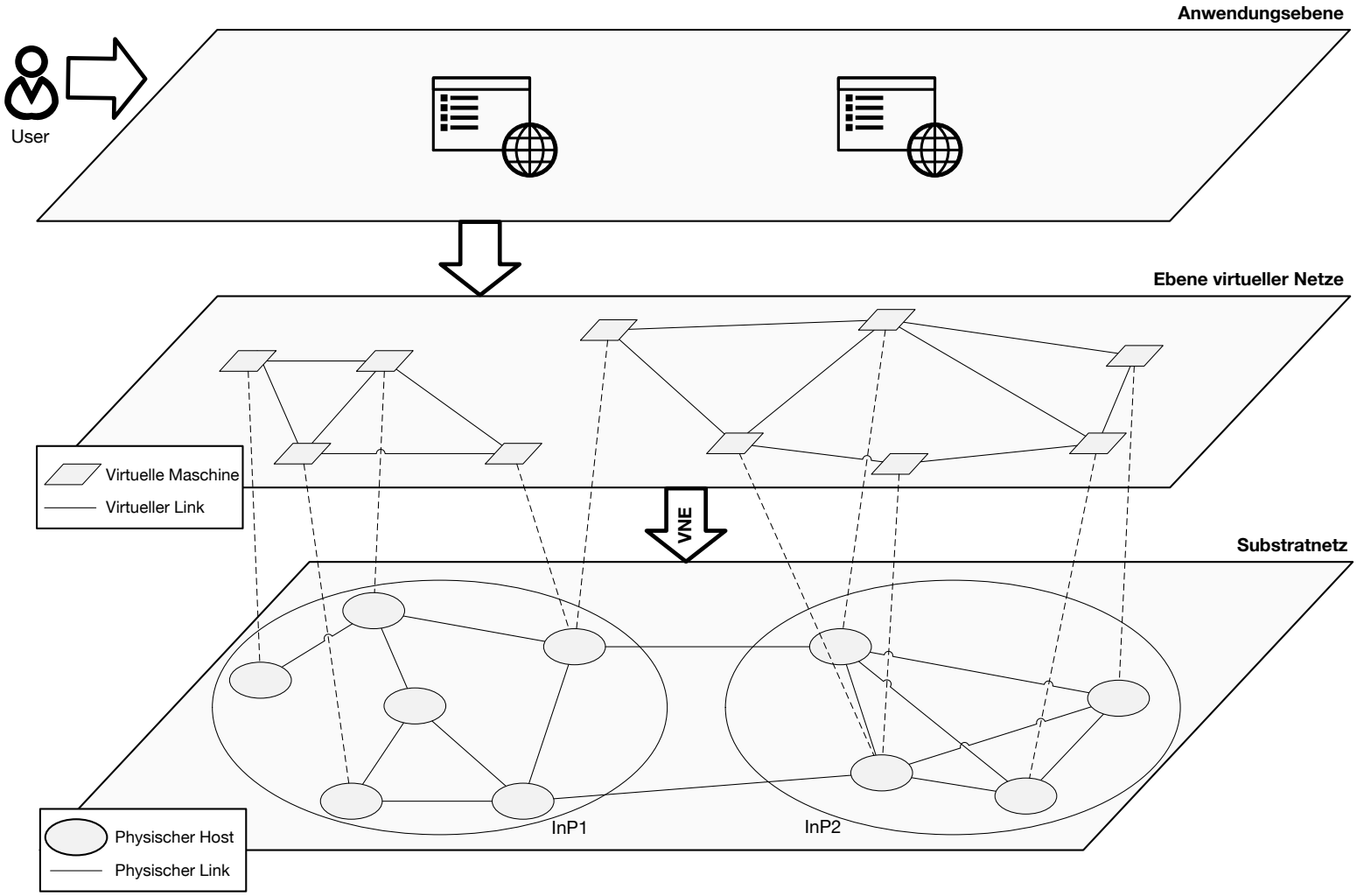
$$G^S = \{\{ (A^S,50),(B^S,30),(C^S,70), (D^S,40),(E^S,20)\},$$
$$\{ (L1^S,3),(L2^S,9),(L3^S,8), (L4^S,10),(L5^S,4),(L6^S,7)\}\}$$

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

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

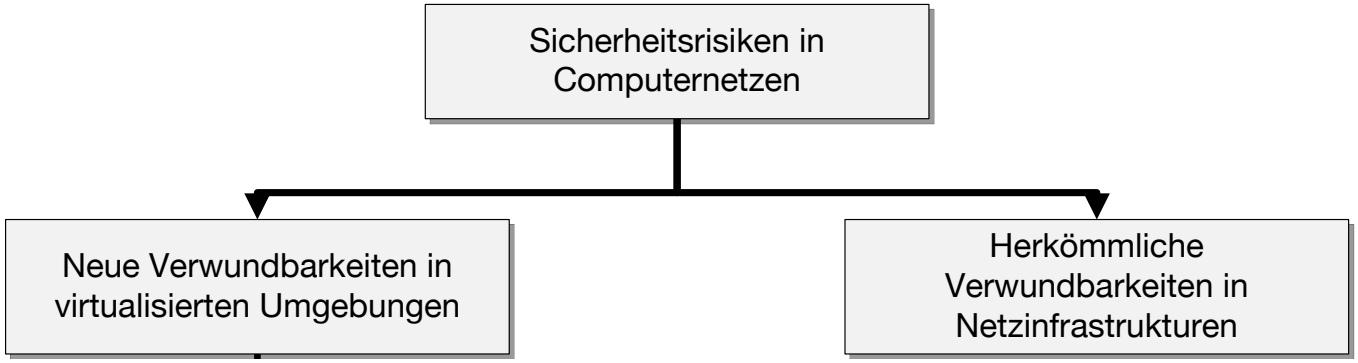
$$\mathbf{f : G^V \rightarrow G^S}$$

Klassifizierung von Sicherheitsrisiken

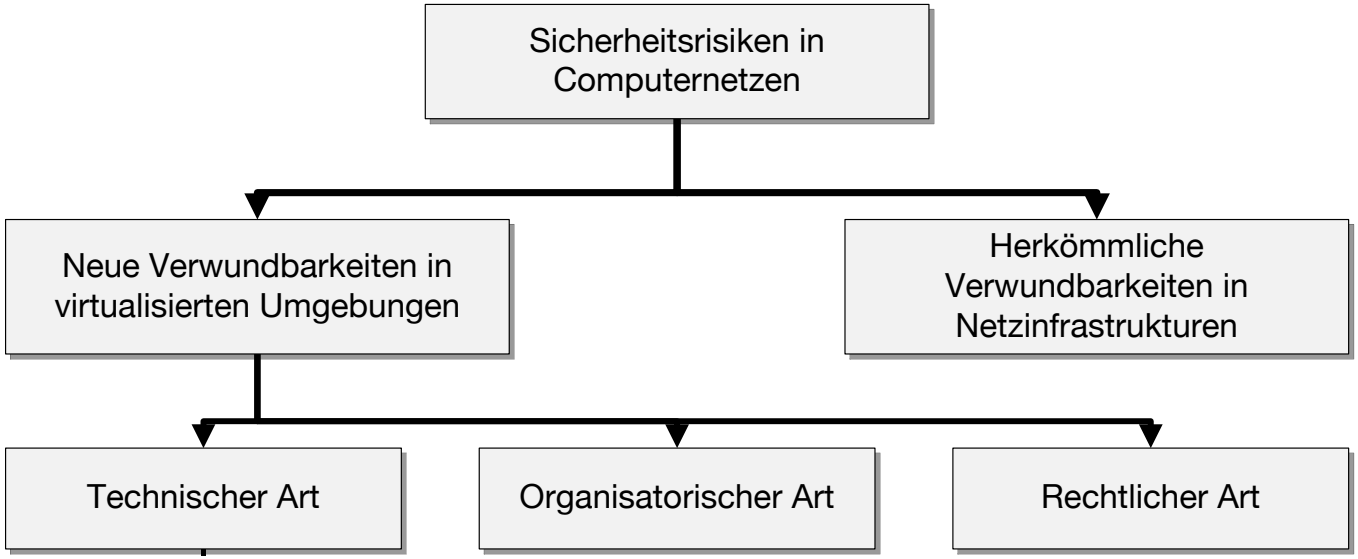


Drei-Schichten-Architektur. Die Substratnetze zweier Infrastructure Provider hosten zwei virtuelle Netze eines Service Providers.

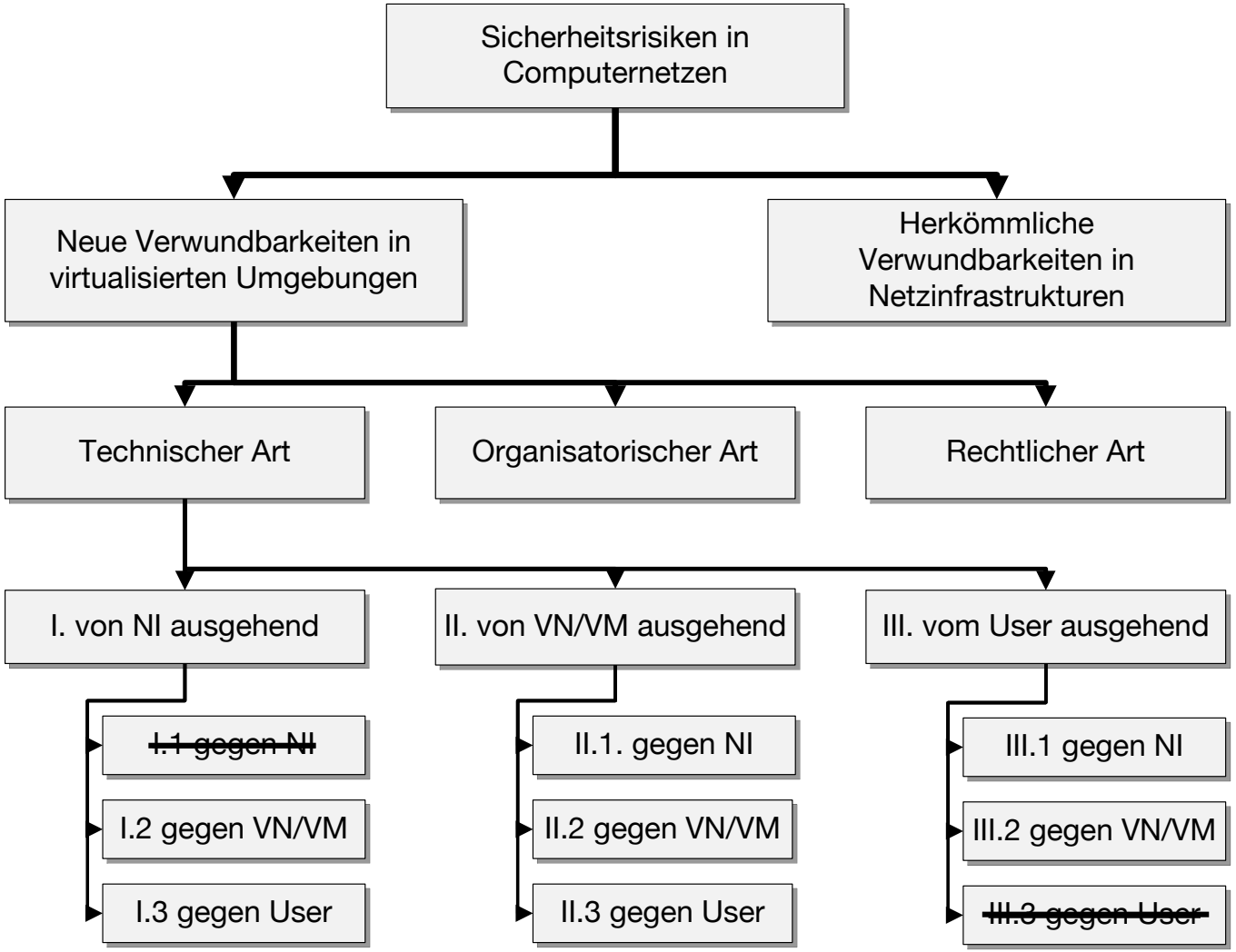
Klassifizierung von Sicherheitsrisiken



Klassifizierung von Sicherheitsrisiken



Klassifizierung von Sicherheitsrisiken

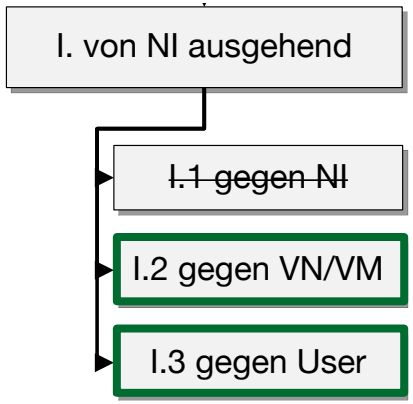


Sicherheitsrisiken technischer Art

Von NI ausgehend...

... gegen VN/VM und User

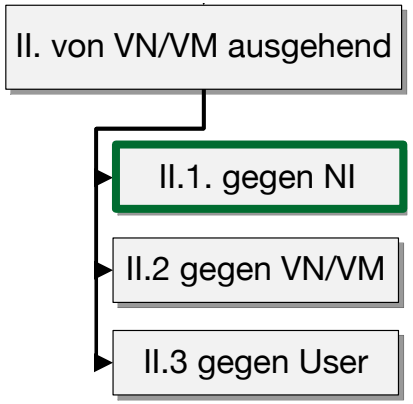
- Monitoring der VM-Aktivitäten
- Sniffing, Spoofing
- Manipulation des legitimen Datenverkehrs



Sicherheitsrisiken technischer Art

Von VN/VM ausgehend…

… gegen NI / ihren physischen Host

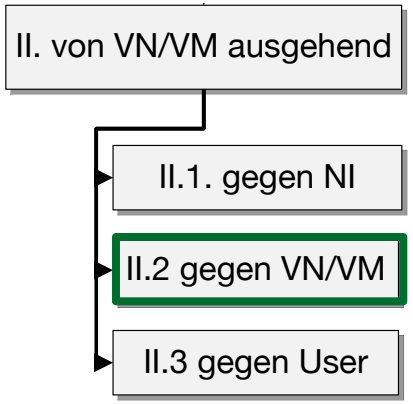


- Verwundbarkeiten des Hosts über zur Verfügung gestellte Ressourcen ausnutzen
- DoS
- „break of isolation“

Sicherheitsrisiken technischer Art

Von VN/VM ausgehend…

… gegen VN/VM

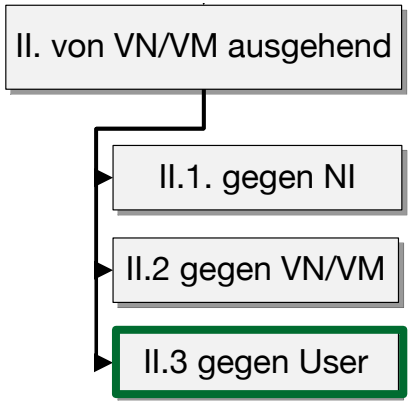


- Erleichterter Zugang zu Verwundbarkeiten durch gemeinsam genutzte Ressourcen
- Virtuelle Netzwerkkarten => Monitoring anderer VNs/VMs
- Einschleusen von Nachrichten des Netzwerkmanagement-protokolls

Sicherheitsrisiken technischer Art

Von VN/VM ausgehend...

... gegen User

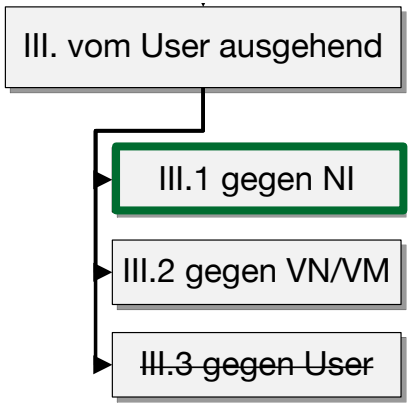


- Monitoring
- Einschleusen konstruierter Nachrichten zum Abbruch von Peer-to-Peer-Verbindungen
- etc.

Sicherheitsrisiken technischer Art

Vom User ausgehend...

... gegen NI



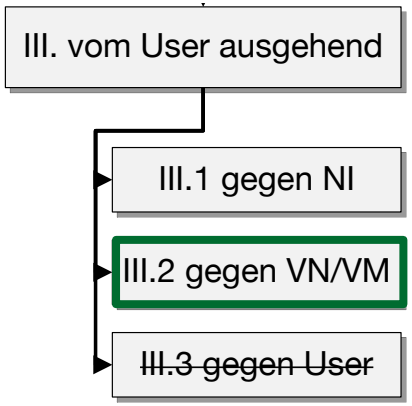
- Angriffe gegen dynamisch umprogrammierbare Router und Switches
- VM als Rootkit
- BluePill[1]

[1] Joanna Rutkowska und Alexander Tereshkin. Bluepilling the xen hypervisor. *Black Hat USA*, 2008.

Sicherheitsrisiken technischer Art

Vom User ausgehend...

... gegen VN/VM



- Man-in-the-Middle während Migration des VNs im Livebetrieb[1]
- Angriffe gegen das VN-Managementtool (XSS, CRSF, SQL-Injection etc.)

[1] Sriram Natarajan und Tilman Wolf. Security Issues in Network Virtualization for the Future Internet.

VNE-relevante Gefahren

- „VNE-relevant“ → im VNE-Prozess beeinflussbar

- Neue Verwundbarkeiten v.a. durch Nutzung gemeinsamer Ressourcen
- Isolationsverletzungen
- => entsprechende Wahl der Abbildung von VMs auf physische Hosts

SVNE-Algorithmen:
Strikte Trennung und Preprocessing[1]

SVNE-Ansatz 1:

- Starre Sicherheitslevels
- Leistungsoptimierendes Preprocessing

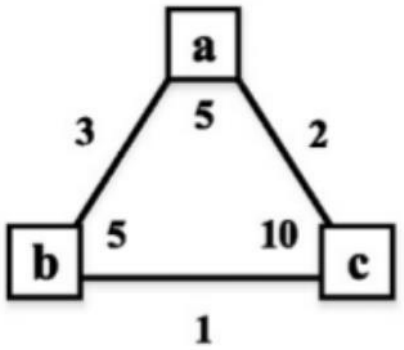
[1] Yang Wang, Phanvu Chau und Fuyu Chen. Towards a secured network virtualization. *Computer Networks*, 104:55–65, 2016.

SVNE-Algorithmen:
Strikte Trennung und Preprocessing[1]

SVNE-Ansatz 1:

- Starre Sicherheitslevels
- Leistungsoptimierendes Preprocessing

Network: *None*
Node: {a,b,c}:*High*
Link: {*a-c*}: *E2E*



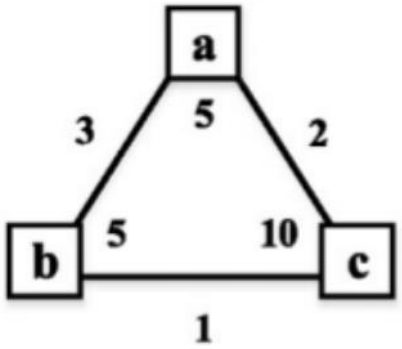
[1] Yang Wang, Phanvu Chau und Fuyu Chen. Towards a secured network virtualization. *Computer Networks*, 104:55–65, 2016.

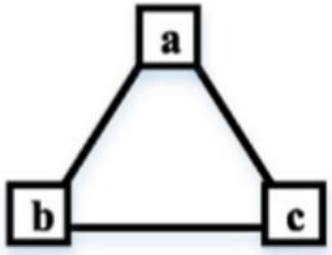
SVNE-Algorithmen:
Strikte Trennung und Preprocessing[1]

SVNE-Ansatz 1:

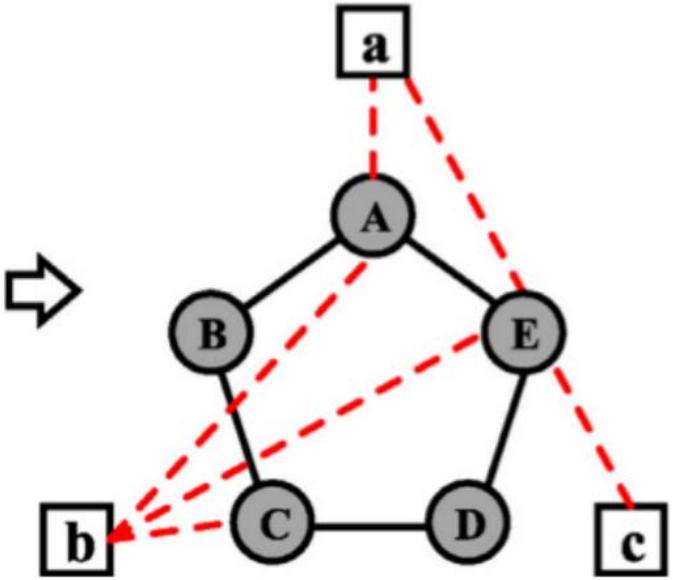
- Starre Sicherheitslevels
- Leistungsoptimierendes Preprocessing

Network: *None*
Node: {a,b,c}:*High*
Link: {a-c}: *E2E*





$C_a = \{A,E\}$
$C_b = \{A,C,E\}$
$C_c = \{E\}$



[1] Yang Wang, Phanvu Chau und Fuyu Chen. Towards a secured network virtualization. *Computer Networks*, 104:55–65, 2016.

SVNE-Algorithmen:
Sicherheitsvektoren und doppelte Berechnung[1]

SVNE-Ansatz 2:

- Flexible Sicherheitsvektoren
- 4 Grundregeln
- 2 Algorithmen

[1] Hong Xu Ming Xu Shuhao Liu, Zhiping Cai. Towards Security-aware Virtual Network Embedding, 2015.

SVNE-Algorithmen:
Sicherheitsvektoren und doppelte Berechnung[1]

SVNE-Ansatz 2:

- Flexible Sicherheitsvektoren
- 4 Grundregeln
- 2 Algorithmen

$$\text{Sicherheitsvektor} = \begin{pmatrix} \dots \\ \dots \\ 7 \\ 3 \\ 9 \\ 1 \\ \dots \\ \dots \end{pmatrix}$$

[1] Hong Xu Ming Xu Shuhao Liu, Zhiping Cai. Towards Security-aware Virtual Network Embedding, 2015.

SVNE-Algorithmen:
Sicherheitsvektoren und doppelte Berechnung[1]

SVNE-Ansatz 2:

- Flexible Sicherheitsvektoren
- 4 Grundregeln
- 2 Algorithmen

$$\text{Sicherheitslevel}(K^S) >= \text{Anforderungslevel}(K^V)$$
$$\text{Sicherheitslevel}(K^V) >= \text{Anforderungslevel}(K^S)$$

$$\forall\ K_i^V \text{ auf } K^S: \text{Sicherheitslevel}(K_i^V) \approx \text{Sicherheitslevel}(K_j^V)$$
$$\text{Sicherheitslevel}(L^S) >= \text{Anforderungslevel}(L^V)$$

[1] Hong Xu Ming Xu Shuhao Liu, Zhiping Cai. Towards Security-aware Virtual Network Embedding, 2015.

SVNE-Algorithmen:
Sicherheitsvektoren und doppelte Berechnung[1]

SVNE-Ansatz 2:

- Flexible Sicherheitsvektoren
- 4 Grundregeln
- 2 Algorithmen

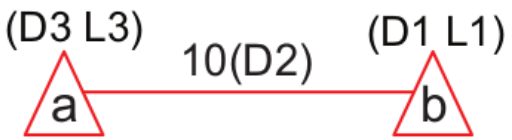
	uSAV (unkoordiniert)	cSAV (koordiniert)
Phasen	zwei	eine
Betrachtung von Knoten und Links	getrennt	gemeinsam
Schwerpunkt	Knotenmapping	Gesamtstruktur
Laufzeit	kurz	lang

[1] Hong Xu Ming Xu Shuhao Liu, Zhiping Cai. Towards Security-aware Virtual Network Embedding, 2015.

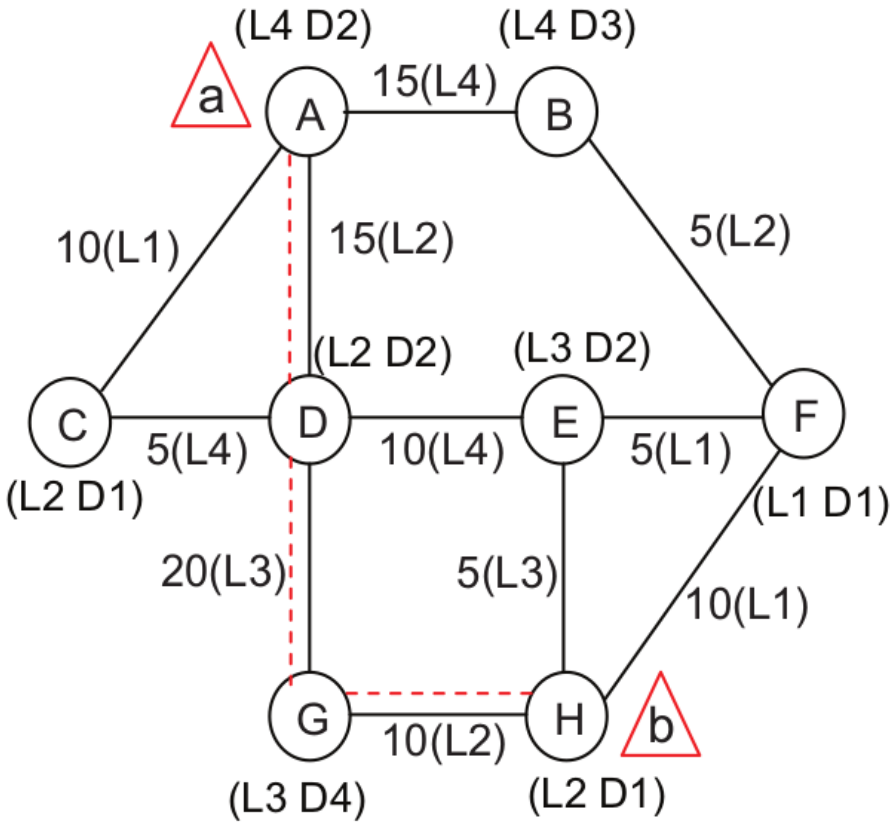
SVNE-Algorithmen:
Sicherheitsvektoren und doppelte Berechnung[1]

SVNE-Ansatz 2:

- Flexible Sicherheitsvektoren
- 4 Grundregeln
- 2 Algorithmen



Virtual Network Request
with
Security Constraints



Substrate Network

[1] Hong Xu Ming Xu Shuhao Liu, Zhiping Cai. Towards Security-aware Virtual Network Embedding, 2015.

Zusammenfassung

- Durch Netzvirtualisierung ergeben sich neue Verwundbarkeiten
- Automatisierte Ansätze zum Embedding virtueller Netze
- verschiedene Verfahren mit integrierten Sicherheitsaspekten beim Embedding

Diskussion

- Kriterien zur Wahl des Verfahrens?
- Mögliche Entwicklungsrichtungen?
- Welchen der Sicherheitsrisiken kann mit Ansatz 1, welchen mit Ansatz 2 begegnet werden?
- Sicherheit nur durch Isolation?
- Gewählte Art der Klassifizierung sinnvoll?

Empfehlenswerte Literatur

Sicherheitsaspekte virtueller Netzinfrastrukturen

- Kamal Dahbur, Bassil Mohammad und Ahmad Bisher Tarakji. A survey of risks, threats and vulnerabilities in cloud computing. In *Proceedings of the 2011 International conference on intelligent semantic Web-services and applications*, Seite 12. ACM, 2011.
- Andreas Fischer, Juan Felipe Botero, Michael Till Beck, Hermann De Meer und Xavier Hesselbach. Virtual network embedding: A survey. *IEEE Communications Surveys & Tutorials*, 15(4):1888–1906, 2013.
- Shuiqing Gong, Jing Chen, Conghui Huang, Qingchao Zhu und Siyi Zhao. Virtual Network Embedding through Security Risk Awareness and Optimization. *KSII Transactions on Internet & Information Systems*, 10(7), 2016.

Untersuchte Algorithmen

- Hong Xu Ming Xu Shuhao Liu, Zhiping Cai. Towards Security-aware Virtual Network Embedding, 2015.
- Yang Wang, Phanvu Chau und Fuyu Chen. Towards a secured network virtualization. *Computer Networks*, 104:55–65, 2016.

Vielen Dank für Ihre Aufmerksamkeit!

{gerhard.groeschl, miran.mizani}@campus.lmu.de