Einleitung

- Problem: Anforderungen an die Netzstruktur ändern sich häufig. Beispiel Webhosting. Neuer Kunde möchte vier Maschinen, die zueinander auf bestimmte Weise verlinkt sind. Anbieter kann nicht täglich neue Kabel verlegen oder für jeden Kunden eigene Rechner aufstellen, deren Kapazitäten nicht vollständig ausgelastet werden.
- Vorteile der NV:
    - Abstraktion von der eingesetzten Hardware; Logisches Netzwerk
    - Flexibilität in der Konfiguration des Netzwerks
    - Testumgebungen
    - Automatisierbarkeit; Dynamisches Skalieren
- Herausforderung ist die Zuordnung von virtuellen zu physischen Knoten und Links -> VNE
- VNE wurde bislang nur hinsichtlich Performance optimiert
- Sicherheitsaspekte dabei meist außer Acht gelassen, obwohl durch geschicktes Design einige Verwundbarkeiten bereits in der Planungsphase vermieden werden können. („Security by design“)
- Gliederung dieses Vortrags:
    - Klassifizierung von Sicherheitsrisiken; einigen derer kann bereits im VNE-Alg. begegnet werden
    - Zwei SVNE-Algorithmen vorstellen, die Sicherheitsaspekte integrieren
    - Dazu beginnen wir mit einer kurzen allg. Darstellung des VNE-Prozesses

Klassifizierung von Sicherheitsrisiken

- In virtuellen Netzinfrastrukturen tun sich neue Verwundbarkeiten gegenüber herkömmlicher Netze auf.
- Zur Klassifizierung orientierten wir uns an der drei Schichten Architektur des NV
- <BILD: Drei Schichtenarchitektur> + Erklärung:
    - Trennung von ISP in InP und SP
    - Substratnetz zweier InPs hostet zwei virtuelle Netze eines SPs
    - Neun Angriffsrichtungen. Einige eröffnen keine neuen Gefahren
- Unsere Klassifizierung:
- <BILD: Klassifizierung>

Von NI gegen VN/VM und User

- Physische Hosts bieten ihren VMs Ressourcen an. Alle Dienste und Anwendungen der VMs werden letztlich auf dem physischen Host ausgeführt und auch alle Daten auf ihm gespeichert.
- Dies ermöglicht dem Host ein Monitoring aller VM-Aktivitäten und vertraulichkeitsverletzendes Sniffing und Spoofing.
- Einschleusen konstruierter Nachrichten, gezieltes Löschen empfangener

Von VN/VM gegen NI

- Bereitstellen von Ressourcen ist auch für den Host nicht ungefährlich.
- VM kann Verwundbarkeiten ihres Hosts durch zugeteilte Ressourcen angreifen.
- Ohne hinreichende Restriktionen:
    - Über ihr Kontingent hinaus Speicherbereiche manipulieren
    - DoS durch Reservierung von CPU-Zeiten
    - Übernahme des Hostes „break of isolation“
        - Alle Angriffe aus der vorherigen Kategorie „Von NI gegen VN/VM und User“

Von VN/VM gegen VN/VM

- Gemeinsame Nutzung von Ressourcen erleichtert den Zugang zu Verwundbarkeiten von VMs auf demselben physischen Host. Z.B. durch benachbarte Speicherbereiche auf der Festplatte des Hosts
- Nur virtuelle Netzwerkkarten -> Monitoring
- VNs aus der Ferne programmierbar -> Einschleusen von Nachrichten des Managementprotokolls.

Von VN/VM gegen User

- Monitoring, Abbruch von P2P-Verbinungen

Vom User gegen NI

- Da sich die virtuelle Netztopologie im VNE-Prozess laufend ändert, müssen Netzwerkkomponenten wie Switches und Router dynamisch umprogrammierbar sein.
- Dies jedoch ermächtigt Angreifer solche ggfs. mit Codeexpliots wie Bufferoverflows o. Ä. zu kompromittieren und für ihre Zwecke zu nutzen oder einen Denail of Service herbeizuführen.
- Daneben besteht die Chance auch Netzwerkknoten anzugreifen. Gelingt es z.B. mit
- einem Rootkit wie BluePill [RT08] – als Vorbereitung für weitere Angriffe – einen Hypervisor zu übernehmen, wird so gleichzeitig die Kontrolle über alle gehosteten VMs erlangt. Auch eine VM lässt sich als Rootkit instrumentalisieren.

Vom User gegen VN/VM

- Während der Migration im Livebetrieb eines VNs ist eine Man-in-the-Middle-Attacke möglich, mit der Informationen über und Inhalte des migrierenden VNs erlangt werden können. [NW]
- Auch die Manipulation von Speicherbereichen der VMs ist während der Migration umsetzbar und lässt sich sogar automatisieren.
- Virtuelle Netzwerkstruktur aus der Ferne umkonfigurieren zu können, erschließt weitere Angriffsziele: Attacken auf die VN-Managementtools

VNE-relavant

- „Security by design“ als Überleitung
- Nicht alle der genannten Verwundbarkeiten lassen sich durch den VNE-Prozess beeinflussen.
- Als „VNE-relevant“ bezeichneten wir in unserer Arbeit solche Sicherheitsrisiken, die durch entsprechende Wahl der Abbildungen von virtuellen auf physische Knoten und Links vermindert oder vermieden werden können.
- Dies trifft hauptsächlich auf solche zu, die auf Isolationsverletzungen basieren oder durch Nutzung gemeinsamer Ressourcen entstehen.
- Zwei Algorithmen, die solche Sicherheitsaspekte bereits in der Planungsphase berücksichtigen, wird Gerhard nun vorstellen.

Schluss

- Wir haben gesehen,
  - dass sich durch NV neue Verwundbarkeiten ergeben
  - dass automatisierte Ansätze zum VNE existieren
  - und dass sich Sicherheitsaspekte in die VNE-Algorithmen lassen.
- In unserer Seminararbeit haben wir uns noch etwas tiefer mit den entsprechenden Themen beschäftigt. Worüber wir jetzt im Anschluss gern noch etwas eingehender sprechen können.
- Damit schließen wir unseren Vortrag. Für die nächsten paar Minuten hätten wir noch Diskussionsthemen vorbereitet und stehen für inhaltliche Fragen zur Verfügung.
- Vielen Dank.