Technische Universität München
Lehrstuhl für Netzarchitekturen und Netzdienste
Prof. Dr. Georg Carle

15.11.201

Bachelorarbeit
Masterarbeit

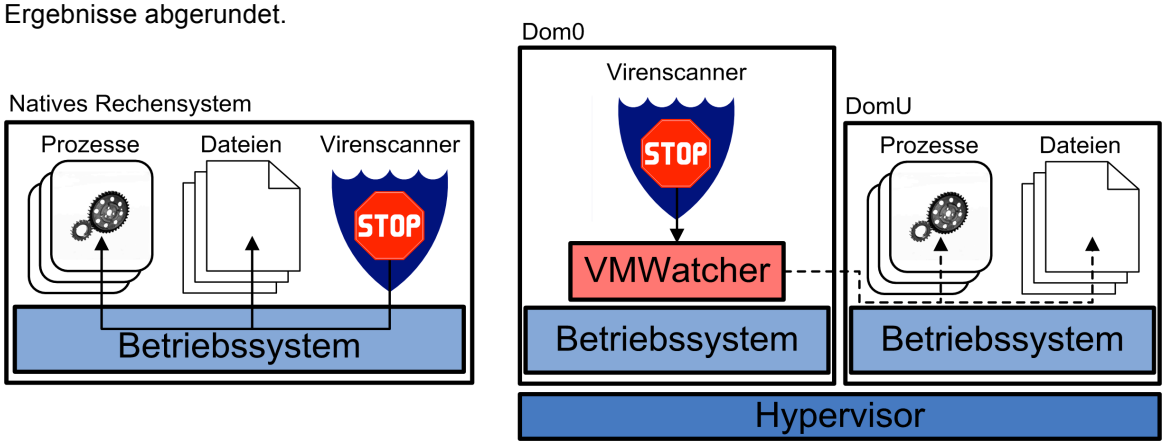
Erkennungsmechanismen für VM-basierte Intrusion Detection Systeme

Motivation

Ein Großteil der heutigen Computersysteme ist miteinander vernetzt – teils sogar über das öffentliche Internet. Dies bringt eine Reihe von Vorteilen (z.B. Fernwartung) aber auch große Nachteile: Angreifer können z.B. von überall aus Rechensysteme angreifen und Schadsoftware kann sich über die Netzwerke verbreiten. Vor allem dann, wenn Rechensysteme sensitive Daten verarbeiten oder sicherheitskritische Aufgaben durchführen, müssen umfassende Schutzmechanismen die *Integrität* der Systeme sicher stellen. In professionell administrierten Umgebungen werden hierfür unter anderem sog. *Hostbasierte Intrusion Detection Systeme* (HIDS) eingesetzt. HIDS kombinieren vielfältige Mechanismen, z.B. Fingerprinting von Binärdateien, Verfahren zur Erkennung von Rootkits, Analysetools für Logdateien oder von Virenscannern bekannte Mechanismen zur Erkennung und automatischen Vereitelung von Angriffen oder Kompromittierung des Systems. Da aber HIDSe direkt auf dem überwachten, d.h. potentiell kompromittierten System laufen, können HIDSe selbst angegriffen und somit manipuliert werden. Durch Virtualisierung kann aber das überwachte System vom überwachenden HIDS wirkungsvoll isoliert werden. Dies macht es dem Angreifer bzw. der Malware schwer das sog. *Virtual Machine Introspection*-basierte IDS (VMI-IDS) zu kompromittieren.

Aufgabenstellung

Leider können Erkennungsmechanismen von HIDSen nicht 1:1 auf eine virtualisierte Umgebung übertragen werden. Ein erster in dieser BA durchzuführende Schritt ist daher die Analyse von Erkennungsmechanismen gängiger HIDS, eine Bewertung deren Möglichkeiten und Grenzen und Überlegungen wie derartige Mechanismen auf virtualisierte Systeme angewendet werden können. Ein Anwendungsfall des zu entwickelnden Systems könnten VMs sein, die Komponenten des am Lehrstuhl entwickelten Sicherheitsframeworks (Authentisierung/Autorisierung in Smart Building Umgebungen) enthalten. Die speziellen Eigenschaften dieses Anwendungsfalls müssen ebenfalls analysiert und geeignet berücksichtigt werden. In einem zweiten Schritt ist ein Prototyp zu Implementieren. Dieser kann auf dem auf VMI beruhenden IDS *VMWatcher* basieren und in der Arbeit erweitert werden. Die Arbeit wird im dritten Schritt von einer umfassenden Bewertung der Ergebnisse abgerundet.

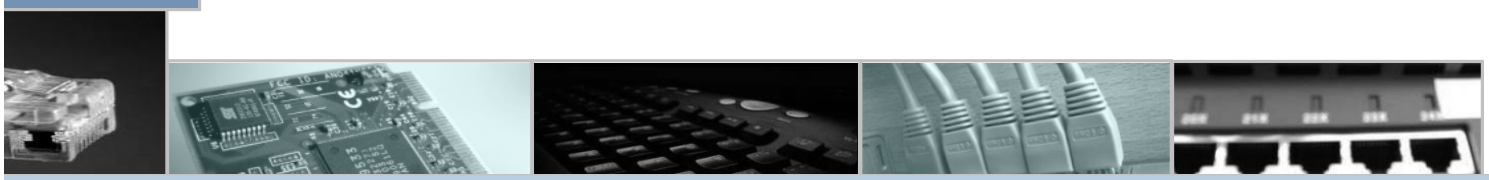


Voraussetzungen

Grundlagen von Virtualisierungtechnologien (Xen), Betriebssystemen (Linux), Kenntnisse in C/C++, Spaß am Ausprobieren und Tüfteln an neuen Technologien.

Stichworte

Hostbased Intrusion Detection Mechanisms (HIDS), Virtualisierung, Virtual Machine Introspection (VMI).



Mehr Informationen am Lehrstuhl für Netzarchitekturen und Netzdienste
Holger Kinkelin, Simon Stauber, Dr. Heiko Niedermayer -- [kinkelin | stauber | niedermayer]@net.in.tum.de